



User Guide

Avigilon™ Access Control Manager™

© 2016, Avigilon Corporation. Portions All rights reserved. AVIGILON, the AVIGILON logo, ACCESS CONTROL MANAGER and ACM are trademarks of Avigilon Corporation. HID, VertX, V100, V200 and V300 are registered trademarks of HID Global Corporation. Other product names mentioned herein may be the trademarks of their respective owners.

The absence of the symbols ™ and ® in proximity to each trademark in this document 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. 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 covering the latest product descriptions and specifications. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Neither Avigilon Corporation nor any of its affiliated companies guarantees the completeness or accuracy of the information contained in this document and is not responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
<http://www.avigilon.com>

PDF-ACM-UG5.6.4

Revision: 1 - EN

20160628

Table of Contents

Avigilon™ Access Control Manager Fundamentals	1
The Avigilon™ Access Control Manager System	1
Logging into the Avigilon Access Control Manager Application	2
Navigating the Application	3
Logging Out of the Avigilon Access Control Manager Application	4
Help in Avigilon Access Control Manager	4
Using a Pop-Up Calendar	4
Setting Personal Preferences	5
Changing the Password in My Account	6
My Account Screen - Profile Page	6
My Account Screen - Batch Jobs	7
My Account Screen - Job Specification	8
Scheduling Batch Jobs	8
Generating a Batch Report	8
Applying Identity Profile to Groups	10
Scheduling a Global Action	11
Setting Batch Door Modes	12
Contacting Your Support Representative	13
For More Information	13
The Avigilon Training Center	14
Support	14
Upgrades	14
Feedback	14
Initial Setup	14
Accepting the End User License Agreement	14
Changing the Administrator Password	14
Creating a Super Admin Identity	15
Managing Appliances	16
Appliances - Changes	16
Adding Extra Appliances	16
Editing Appliances	16
Deleting an Appliance	17
Configuring Replication and Failover	17
Recommended System Architecture	18
System Architecture for Replication	18
System Architecture for Failover	19

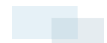
Replication and Failover Requirements	20
1. Preparing Appliances for Replication and Failover	21
Setting Up the Primary Appliance	22
Setting Up the Secondary or Standby Appliances	22
2. Setting Up Replication Between Appliances	22
Enabling Replication on the Primary Appliance	23
Enabling Replication on the Secondary or Standby Appliance	23
3. Adding a Replication Subscription	23
Testing Replication	25
Checking the Appliance Replication Status	25
Testing Two-Way Replication	25
4. Setting Up Failover	25
Removing Replication and Failover	26
Failing Over and Failing Back	26
Automatic Failover	26
Manual Failover	27
Failback	27
Configuring Network Connections	27
Configuring Ethernet Ports	27
Appliances - Virtual Port Add Page	28
Adding Ethernet Routes	28
Enabling Serial Ports	29
Appliances - Serial Port Edit Page	29
Backups	30
Backing Up System Data	30
Manually Backing Up Data	30
Restoring Backups	30
Logs	31
Accessing Appliance Logs	31
Software Updates	31
Updating the Appliance Software	31
Appliances - About	32
Applying License Upgrades	32
Viewing the End User License Agreement	33
Accepting the End User License Agreement	33
Reviewing the Appliance Status	33
Appliances - Listing Page	33
Appliances - Add Page	34

Appliances - Appliance Page	36
Appliances - Access Page	39
Appliances - Port Listing Page	40
Appliances - Ethernet Ports Page	40
Appliances - Ethernet Virtual Listing page	41
Appliances - Virtual Port Edit Page	41
Appliances - Routes Listing Page	42
Appliances - Route Add Page	42
Appliances - Route Edit Page	43
Appliances - Serial Port Edit Page	43
Appliances - Replication Page	44
Replication Page	44
Appliances - Backups Listing Page	46
Appliances - Backups Add Page	47
Appliances - Backups Edit Page	48
Appliances - Backup File List	49
Appliances - Logs Listing Page	50
Appliances - Logs Page	51
Appliances - Software Updates Page	51
Appliances - Software Update Add Page	51
Appliances - About Page	52
Physical Access - Main Page	54
Output Modes	54
Operating Mode	54
Offline Mode	55
Outputs	55
Inputs	56
Outputs	56
Configuring Doors	57
Adding Doors	57
Adding Simple Macros	58
Editing Doors	59
Doors - Editing HID™ Doors	59
Doors - Editing Mercury Security Doors	59
Searching for Existing Doors	60
Controlling Doors	60
Deleting Doors	61
Door Modes	61



Access Types	62
Anti-Passback	62
Anti-Passback Modes	63
Setting Up Anti-Passback	64
Granting a Free Pass	64
Global Anti-Passback	65
Global Anti-Passback Modes	65
Interlocks	66
Accessing Interlocks through Doors	66
Accessing Interlocks from Subpanel Inputs	67
Accessing Interlocks from Subpanel Outputs	67
Adding Interlocks	67
Editing Interlocks	67
Doors - Listing Page	67
Doors - Add Page	68
Doors - HID™ New Parameters Page	69
Doors - Mercury Security New Parameters Page	71
Doors - Edit Screen	74
Doors - HID VertX® Edit Screen	74
Doors - HID™ Parameters Page	74
Doors - HID™ Operations Page	76
Doors - HID™ Hardware Page	79
Doors - HID™ Subpanel Reader Edit Page	81
Doors - HID™ Subpanel Input Edit Page	82
Doors - HID™ Subpanel Output Edit Page	83
Doors - HID™ Cameras Page	83
Doors - HID™ Events Page	84
Doors - Creating Local Events for HID™ Doors	86
Doors - HID™ Access Page	87
Doors - HID™ Transactions Page	87
Doors - Mercury Security Edit Screen	88
Doors - Mercury Security Parameters Page	88
Mercury Security Operations Page	91
Doors - Mercury Security Hardware Page	93
Doors - Subpanel Reader Edit Page	96
Doors - Subpanel Input Edit Page	98
Doors - Subpanel Output Edit Page	99
Doors - Mercury Security Elev Page	99
Doors - Mercury Security Cameras Page	99

Live Video Window	102
Doors - Mercury Security Interlocks Page	102
Interlocks - Add Page	104
Interlocks - Door Edit Page	106
Doors - Mercury Security Events Page	107
Doors - Creating Local Events for Mercury Doors	109
Doors - Mercury Security Access Page	110
Doors - Mercury Security Transactions Page	110
Doors - Access Page	111
Configuring Panels	111
Searching for Panels	111
Adding Panels	111
Adding HID VertX® Panels	112
Adding Mercury Security Panels	112
Editing Panels	112
Editing HID VertX® Panels	112
Editing Mercury Security	113
Resetting Anti-Passback from the Panel	113
Downloading Parameters	114
Downloading Tokens	114
Lenel™ Panel Support	114
Resetting Doors/Subpanels	114
Updating Firmware	115
Updating Panel Time	115
Deleting Panels	116
Subpanels	116
Adding Subpanels	116
Editing Subpanels	117
Deleting Subpanels	117
Macros	117
Adding Macros	118
Editing Macros	118
Deleting Macros	119
Assigning Macros	119
Assigning a Macro to a Trigger	119
Assigning a Macro to a Macro	119
Assigning a Macro to a Door	119
Sorting Macros	119



Triggers	120
Adding Triggers	120
Editing Triggers	120
Deleting Triggers	120
Panels - Listing Page	120
Panels - Panel Add Page	121
HID	122
Mercury Security	122
Panels - Batch Add HID Subpanels Page	123
Panels - Batch Add Mercury Subpanels Page	123
HID VertX® Panel Pages	124
Panels - HID VertX® Status Page	124
Subpanels - HID VertX® Status Listing Page	125
Panels - HID™ Firmware Listing Page	126
Panels - HID™ Firmware Upload Page	126
Panels - HID VertX® Configure Page	126
Panels - HID VertX® Host Page	127
Panels - HID VertX® Subpanels Page	128
Subpanels - HID™ Subpanel Add Page	129
Subpanels - HID™ Subpanel Edit Page	129
Subpanels - HID™ Input Listing Page	130
Subpanels - HID™ Input Edit Page	130
Subpanels - HID™ Outputs Listing Page	131
Subpanels - HID™ Outputs Edit Page	132
Subpanels - HID™ Readers Listing Page	132
Subpanels - HID™ Reader Edit Page	133
Panels - HID VertX® Events Page	133
Panels - Create Local Events for HID™ Panels	135
Subpanels - HID VertX® Events Page	136
Subpanels - Create Local Events for HID™ Subpanels	138
Inputs - HID VertX® Events Page	139
Inputs - Create Local Events for HID™ Inputs	141
Outputs - HID VertX® Events Page	142
Outputs - Create Local Events for HID™ Outputs	144
Mercury Security Panel Pages	145
Panels - Mercury Security Status Page	146
Subpanels - Mercury Security Status Listing Page	147
Panels - Mercury Firmware Listing Page	148
Panels - Mercury Firmware Upload Page	148
Panels - Mercury Security Configure Page	148
Panels - Mercury Security Host Page	149
Panels - Mercury Security Subpanels Page	150
Subpanels - Mercury Subpanel Add Page	151
Subpanels - Subpanel Edit Page	152

Subpanels - Mercury Input Listing Page	152
Subpanels - Mercury Input Edit Page	154
Interlocks - Input Listing Page	156
Interlocks - Input Add Page	157
Interlocks - Input Edit Page	159
Subpanels - Mercury Outputs Listing Page	160
Subpanels - Mercury Outputs Edit Page	161
Interlocks - Output Listing Page	162
Interlocks - Output Add page	163
Interlocks - Output Edit Page	165
Subpanels - Mercury Readers Listing Page	166
Subpanels - Mercury Reader Edit Page	167
Panels - Mercury Security Macros	168
Macros - Macro Command Listing Page	168
Macros - Macro Command Add Page	169
Macros - Macro Command Edit Page	169
Triggers - Listing page	170
Triggers - Add Page	170
Triggers - Edit Page	172
Panels - Mercury Security Access Levels Page	173
Panels - Mercury Security Events Page	173
Panels - Create Local Events for Mercury Panels	175
Subpanels - Mercury Security Events Page	176
Subpanels - Create Local Events for Mercury Subpanels	178
Inputs - Mercury Security Events Page	179
Inputs - Create Local Events for Mercury Inputs	181
Outputs - Mercury Security Events Page	182
Outputs - Create Local Events for Mercury Outputs	184
Areas	186
Areas - Adding	186
Areas - Editing	187
Areas - Deleting	187
Areas - Listing Page	187
Areas - Add Page	187
Areas - Edit Page	188
EOL Resistance	189
Adding EOL Resistance for Mercury Input Points	189
Adding EOL Resistance to HID Input Points	189
Editing EOL Resistance for Mercury Input Points	190

Editing EOL Resistance for HID Input Points	190
EOL Resistance - HID Listing Page	190
EOL Resistance - Add Page	190
EOL Resistance - Edit Page	191
EOL Resistance - Mercury Listing Page	191
EOL Resistance - Add Normal Page	192
EOL Resistance - Add Advanced Page	192
EOL Resistance - Edit Page	193
Normal Edit Page	193
Advanced Edit Page	194
Card Formats	194
Adding Card Formats	195
Editing Card Formats	195
Deleting Card Formats	195
Card Formats - Listing Page	195
Card Formats - Add Page	195
Card Formats - Edit Page	196
Events - Introduction	197
Events - Searching	198
Events - Editing	198
Events - Assigning Priority Colors	198
Events - Listing Page	199
Events - Edit Page	200
Events - Colors Listing Page	202
Events - Color Add Page	202
Events - Color Edit Page	202
Global Actions	202
Global Actions - Adding	203
Global Actions - Editing	203
Global Actions - Action Types	203
Global Actions - Deleting	204
Global Actions Listing Page	204
Global Actions - Add Page	204
Global Actions - Edit Page	208
Global Linkages - Introduction	211
Global Linkages - Adding	212
Global Linkages - Editing	212
Global Linkages - Listing Page	212

Global Linkages - Add Page	213
Global Linkages - Edit Screen	214
Global Linkages - Linkage Page	214
Global Linkages - Devices Page	215
Global Linkages - Events Page	216
Global Linkages - Tokens Page	217
Global Linkages - Actions Page	219
Mustering - Introduction	220
Mustering - Requirements	220
Mustering - Creating a Dashboard	221
Mustering - Using the Dashboard	221
Mustering - Manually Moving Identities	223
Settings - Main Page	224
Schedules and Holidays - Introduction	224
Schedules	224
Holidays	224
Adding Schedules	225
Editing Schedules	225
Deleting Schedules	225
Holidays - Adding	226
Holidays - Editing	226
Holidays - Deleting	226
Schedules - Listing Page	226
Schedules - Add New Page	227
Schedules - Edit Page	228
Holidays - Listing Page	229
Holidays - Add New Page	230
Holidays - Edit Page	230
Event Types - Introduction	231
Adding Event Types	231
Editing Event Types	232
Deleting Event Types	232
Event Types - Listing Page	232
Event Types - Add New Page	233
Event Types - Edit Page	234
User Defined Fields - Introduction	234
User Defined Fields - Adding a Field	235
User Defined Fields - Adding User Defined Tabs	235

User Defined Fields - Editing User Defined Tabs	236
User Defined Fields - Deleting Fields	236
User Defined Tabs - Deleting	236
User Defined Fields - Listing Page	237
User-Defined Fields - Add New Page	237
User Defined Tabs - Listing Page	238
User Defined Tabs - Add Page	238
User Defined Tabs - Edit Page	238
User Lists - Introduction	239
User Lists - Adding Items to a List	239
User Lists - Editing Items	239
User Lists - Deleting Items	239
User Lists - User-Defined Lists	240
User Lists - User List Edit Screen	240
System Settings	240
System Settings - General Page	240
Remote Authentication from External Domains	242
System Settings - Configuring Remote Authentication	242
System Settings - Remote Authentication	243
System Settings - External Domains Listing Page	244
System Settings - External Domains Add Page	244
System Settings - External Domains Edit Page	245
System Settings - Certificates Listing Page	245
Certificate Upload Page	246
Badge Templates - Introduction	246
Using Badge Templates	246
Adding a Badge Template	247
Editing a Badge Template	248
Duplicating a Badge Template	248
Deleting a Badge Template	248
Badge Designer - Changing the Badge Background Color	248
Color Palette	249
Badge Templates - Listing Page	251
Badge Designer - Add and Edit Page	251
Badge Designer - Add Picture	253
Badge Designer - Add DB Field	253
Badge Designer - Add Text	255
Badge Designer - Add Graphic	256

Badge Designer - Barcodes	257
Badge Designer - Layer Ordering	257
External Systems - Introduction	257
Supported External Systems	258
External Systems - Avigilon™ Server Listing Page	258
External Systems - Avigilon™ Server Add Page	258
External Systems - Avigilon™ Server Edit Page	259
External Systems - Dedicated Micros™ Listing Page	260
External Systems - Dedicated Micros™ Add Page	260
External Systems - Dedicated Micros™ Edit Page	261
External Systems - Exacq™ Servers Listing Page	261
External Systems - Exacq™ Server Add Page	262
External Systems - Exacq™ Server Edit Page	262
External Systems - Motion Smoothing	263
External Systems - IP-Based Camera Listing Page	264
External Systems - IP-Based Camera Add Page	264
External Systems - IP-Based Camera Edit Page	265
External Systems- Enabling RTSP	265
External Systems - LifeSafety Power™ Listing Page	266
External Systems - LifeSafety Power™ Add Page	266
External Systems - LifeSafety Power™ Supply Edit Page	266
External Systems - Milestone™ Servers Listing Page	267
External Systems - Milestone™ Server Add Page	267
External Systems - Milestone™ Server Edit Page	268
External Systems - Salient™ Servers Listing Page	269
External Systems - Salient™ Server Add Page	269
External Systems - Salient™ Server Edit Page	270
External Systems - Adding	271
External Systems - Editing	271
External Systems - Deleting	271
External Systems - Defining the Badge Camera for the System	272
Maps - Introduction	272
Maps - Creating and Editing a Map	272
Maps - Linking Maps	273
Using a Map	274
Map Templates (Settings) - Listing Page	277
Maps - Add Page	277
Maps - Edit Page	278



Map Properties	278
Map Details	279
Identities	281
Identities Overview	281
Adding an Identity	281
Searching for an Identity	282
Editing an Identity	283
Identities - Assigning Roles	283
Identities - Assigning Tokens	284
Identities - Assigning Groups	284
Capturing an Image of an Identity	285
Identities - Creating Badges	286
Creating an Identity Report	287
To generate an identity report:	287
To generate an event report:	288
Uploading a Photo of an Identity	288
Deleting an Identity	289
Destroy Batch feature	289
Identities - Identity Search Page	289
Identities - Add Page	290
Identities - Identity Page	292
Identities - Roles Page	293
Identities - Tokens Listing Page	294
Identities - Token: Add New Page	295
Identities - Token Edit Page	296
Identities - Groups Page	298
Identities - Access Page	299
Capturing an Image of an Identity	299
Identities - Photos Page	300
Identities - Transactions Page	301
Identities - Badge Page	301
Identities - Audit Page	301
Identity Profiles	302
Adding an Identity Profile	302
Editing an Identity Profile	303
Identity Profiles - Assigning Roles	303
Identity Profiles - Defining Token Settings	304
Identity Profiles - Assigning Groups	304

Identity Profiles - Batch Update	305
Deleting an Identity Profile	305
Identity Profiles - Listing Page	305
Identity Profiles - Add Page	306
Identity Profiles - Identity Page	307
Identity Profiles - Roles Page	309
Identity Profiles - Token Profile: Edit Page	310
Identity Profiles - Groups Page	311
Identity Profiles - Access Page	311
Collaboration - Introduction	313
Collaborations - Adding	313
Collaborations - Adding Events XML Collaboration	314
Collaborations - Events XML Definitions	315
Collaborations - Events XML Example	318
Collaboration - Editing	319
Collaboration - Types	319
Collaboration - Running	320
Collaboration - Deleting	320
Collaboration - Assigning Events to a Collaboration	321
Collaboration - Listing Page	321
Collaboration - Add Page	322
Collaboration - Edit Screen	324
Collaboration - ArcSight™ CEF Edit Screen	325
Collaboration - CSV One-time Edit screen	325
Short Format	325
Long Format	326
Collaboration - Preparing CSV files	326
Avoiding Duplicate Identities and Errors	326
Collaboration - Fields	326
Mandatory Identity Fields	326
Optional Identity Fields	327
Token Fields	328
Collaboration - CSV Upload	329
Collaboration - CSV Upload Template	329
CSV One Time Short Format Collaboration	330
CSV One Time Long Format Collaboration	330
CSV Recurring Collaborations	331
Collaboration - LDAP Pull Edit Screen	333
Collaboration - Milestone™ Edit Screen	333



Collaboration - Oracle™ RDBMS Pull Edit Screen	333
Collaboration - SQL Server Pull Edit Screen	334
Collaboration - Syslog Edit Screen	334
Collaboration - XML Edit Screen	335
Collaboration - Identity CSV Export Edit Screen	335
Collaboration - Identity CSV Recurring Edit Screen	336
Collaboration - Source Page	339
Collaboration - Schedule Page	339
Collaboration - Identity CSV Export Schedule Page	340
Collaboration - Identity CSV Recurring Schedule Page	340
Collaboration - Identities Page	341
Collaboration - Tokens Page	341
Collaboration - Blob Page	342
Collaboration - User Defined Page	342
Collaboration - Roles Page	343
Collaboration - Events Page	343
Roles - Main Screen	345
Configuring Roles	345
Adding a Role	345
Editing a Role	346
Assigning an Access Group to a Role	346
Roles - Assigning Delegations	347
Roles - Assigning Routing Groups	347
Roles - Assign Roles	348
Deleting a Role	348
Roles - Listing Page	348
Roles - Default Roles Page	349
Roles - Add New Page	349
Roles - Role Edit Page	350
Roles - Access Groups Page	351
Roles - Delegate Page	351
Roles - Routing Page	352
Roles - Assign Roles Page	352
Roles - Access Page	353
Roles - Audit Page	353
Managing Policies	354
Adding a Policy	354
Editing a Policy	354

Deleting a Policy	355
Policies - Listing Page	355
Policies - Policy Add Page	355
Policies - Policy Page	356
Policies - Mercury page	357
Policies - Input Page	359
Policies - Output Page	360
Policies - Audit Page	360
Configuring Groups	361
Adding a Group	361
Editing a Group	361
Assigning Policies to Groups	362
Assigning Components to Groups	362
Creating a Hardware Group for Routing	363
Using Policies to Override Hardware Settings	364
Performing an Identity Batch Update	364
Scheduling an Identity Batch Update	365
Deleting a Group	366
Groups - Listing Page	367
Groups - Group Add Page	367
Groups - Group Edit page	367
Groups - Policies Page	368
Groups - Members page	368
Groups - Audit Page	368
Managing Door Access	369
Adding an Access Group	369
Editing an Access Group	370
Deleting an Access Group	370
Access Groups - Example	370
Assigning an Access Group to a Role	371
Access Groups - Listing Page	371
Access Groups - Access Group Add page	372
Access Groups - Edit Page	373
Access Groups - Access Page	373
Access Groups - Audit Page	374
Managing Access in the Application	374
Adding a Delegation	374
Editing a Delegation	375



Adding a Delegation to a Role	375
Deleting a Delegation	376
Delegations Listing Page	376
Delegations - Edit Page	376
Partitioning the System	377
Adding a Partition	377
Editing a Partition	378
Configuring Partitions	378
Deleting a Partition	379
Partitions - Listing Page	379
Partitions - Partition Edit Page	379
Routing Events to the Monitor Screen	380
Adding a Routing Group	380
Editing a Routing Group	381
Assigning a Routing Group to a Role	381
Deleting a Routing Group	382
Routing Groups - Listing Page	382
Routing Groups - Add Page	382
Routing Groups - Schedule Page	383
Routing Groups - Event Types Page	383
Routing Groups - Groups Page	384
Managing Elevator Access	384
Adding an Elevator Access Level	385
Editing an Elevator Access Level	385
Assigning an Elevator Access Level to an Access Group	385
Deleting an Elevator Access Level	385
Elevator Access Levels - Listing Page	386
Elevator Access Levels - Add Page	386
Elevator Access Levels - Edit Page	387
Monitor - Introduction	388
Monitoring Events	388
Pause/Resume Events	389
Clear Events	389
View Live Video	389
View Recorded Video	390
Create Event Notes	390
View Event Notes	390
View Event Instructions	391

View Event Identity Details	391
View Event History	391
Change Events List Settings	392
Reconnect to Events List	392
Searching for Events and Alarms	392
View Camera (Search)	394
View Recorded Video (Search)	394
Create Event Notes (Search)	394
View Event Notes (Search)	395
View Event Instructions (Search)	395
View Event Identity Details (Search)	395
View Event History (Search)	395
Change Transactions List Settings	396
Monitor Alarms	396
Acknowledge Alarms	397
View Live Video (Alarms)	398
View Recorded Video (Alarms)	398
Create Event Notes (Alarms)	398
View Event Notes (Alarms)	399
View Event Instructions (Alarms)	399
View Event Identity Details (Alarms)	399
View Event History (Alarms)	400
Change Alarms List Settings	400
Monitor Screen - Verification	401
Verifying Cardholders at Doors	401
Verification Events List	401
Monitor Page - Hardware Status	402
System Status	403
Door Actions	404
Door Status	404
Panel Status	405
Subpanel Details	406
Input / Output Details	407
LifeSafety Panels	407
Controlling System Hardware	408
Status Colors	409
Monitor Screen - Map Templates Page	409
Using a Map	410



Add Map	412
Monitor Screen - Events	412
Monitor Screen - Live Video Window	413
Monitor Screen - Recorded Video Window	414
Monitor Screen - Notes Window	415
Monitor Screen - Instructions Window	416
Monitor Screen - Identity Window	416
Monitor Screen - History Window	416
Monitor Screen - Viewing Camera Video	417
Monitor Screen - Search	417
Wildcard Characters	419
Monitor Screen - Alarms	419
Maps - Add Page	420
Generating Reports	421
Reports - Generating Reports	421
Reports - Report Preview	421
Reports - Editing	422
Reports - Editing Audit Log and Transaction Reports	423
Reports - Listing Page	423
Reports - Access Grant via Operator	424
Reports - Access Groups	425
Reports - Action Audit	425
Reports - Alarm	426
Reports - Appliance	428
Reports - Area Identity	428
Reports - Area	429
Reports - Audit Log	430
Reports - Cameras	431
Reports - Collaboration	431
Reports - Delegation Comparison	432
Reports - Delegation	433
Reports - Door Configuration	433
Reports - Door/Identities with Access	434
Reports - Event	435
Reports - Event Type	436
Reports - Group	436
Reports - Holiday	437
Reports - Identity Photo Gallery	438

Reports - Identity Summary	438
Reports - Identity/Doors with Access	440
Reports - Panel	440
Reports - Policy	441
Reports - Role	442
Reports - Schedule	442
Reports - Token	443
Reports - Tokens Pending Expiration Date	444
Reports - Transaction	445
Reports - Creating Custom Reports	447
Reports - Creating Custom Transaction Reports	448
Reports - Custom Reports Listing Page	448
Reports - Custom Report Preview	448

Avigilon™ Access Control Manager Fundamentals

The Avigilon Access Control Manager software gives you the ability to configure and control your local access control security system through a web browser. Once all of your access control components are connected to the Avigilon Access Control Manager appliance, you can configure your system with ease.

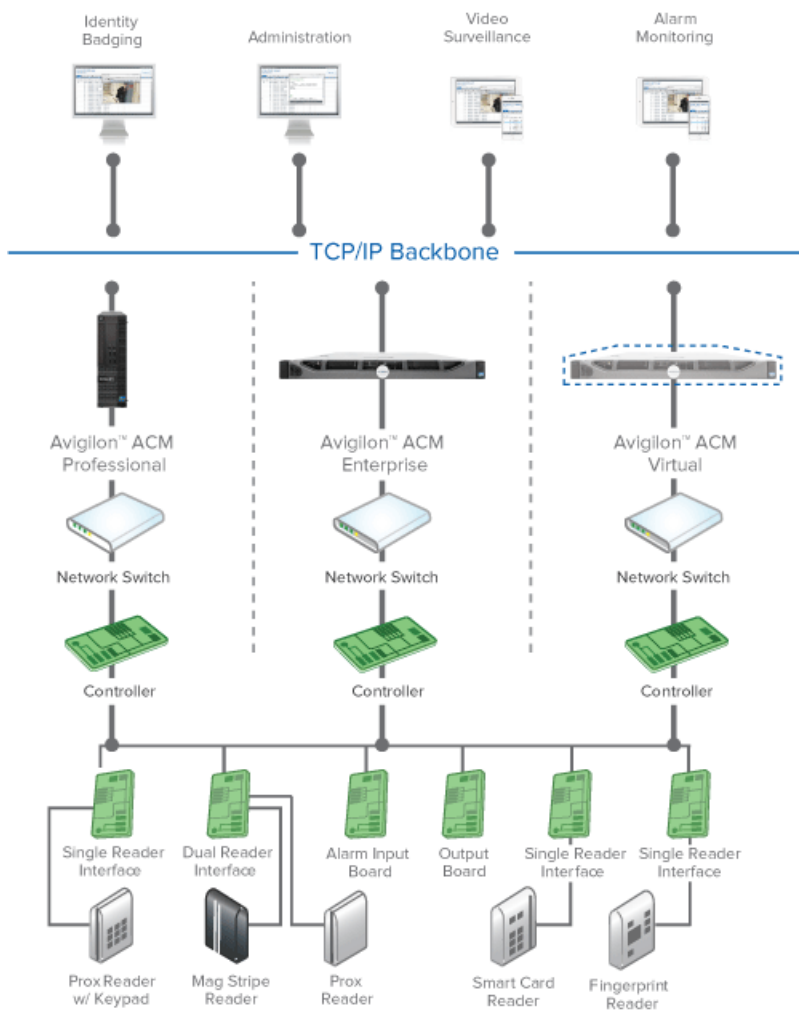
The Avigilon Access Control Manager software allows you to:

- Configure your access control system hardware and software
- Design and assign badges
- Monitor events
- Generate access control reports
- Perform required administrative tasks

To begin using the Avigilon Access Control Manager application, refer to these pages:

The Avigilon™ Access Control Manager System

The Avigilon Access Control Manager system can be organized like this:



To begin using the AvigilonAccess Control Manager application, refer to these pages:

Logging into the Avigilon Access Control Manager Application

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

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

If this is the your first time logging into the Avigilon Access Control Manager application, the default username is `admin`.

4. Enter your password in the **Password** field.

If this is your first time logging in to the application, the default password is `admin`.

5. Click the **Sign in** button.

The application's Home page is displayed.

Navigating the Application

After you log in to the Avigilon™ Access Control Manager, the Home page is displayed.

The home page may look different depending on your system preferences and the permissions you have. The key features of the application window are:

The screenshot shows the Avigilon Access Control Manager interface. At the top, there is a navigation bar with user links (1) and setup links (2). Below this is a main menu bar with icons for Monitor, Identities, Reports, Physical Access, and Roles (3). Below this is a secondary menu bar with icons for Roles, Policies, Groups, Access Groups, Delegations, Partitions, Routing Groups, and Elevator Access Levels (4). The main content area is titled 'Roles' and features an 'Add New Role' button. A table lists various roles with columns for Name, Parent, Child Roles, Installed status, Start Date, Stop Date, and Delete. A '5' callout points to the table. At the bottom, there are buttons for 'Add New Role' and 'Create New Report'.

Name	Parent	Child Roles	Installed	Start Date	Stop Date	Delete
Admin		0	✓	09/10/2008	31/12/2020	✖
Enrollment Operator		0	✓	09/10/2008	31/12/2020	✖
Identities View Only		0	✓	09/10/2008	31/12/2020	✖
Identities View/Edit		0	✓	09/10/2008	31/12/2020	✖
Monitoring Operator		0	✓	09/10/2008	31/12/2020	✖
Monitoring Supervisor		0	✓	09/10/2008	31/12/2020	✖
Super Admin		0	✓	01/01/2007	31/12/2025	

Figure 1: Typical features of the Access Control Manager application window.

Feature	Description
1. User links area	
My Account	Click on this link to view your account page.
Support	Click this link to display information on how to obtain support for your Access Control Manager system.
Help	Click this link to view context-sensitive help for the current feature.
Log Out	Click this button to log out of the application.
2. Setup links area	
Appliance	Click this link to define the Access Control Manager devices that mediate network traffic between the application and its connected security system.
Settings	Click this link to define the building blocks of the Access Control Manager — such as Schedules, Holidays, Event Types and Badge Designer.

Feature	Description
Collaboration	Click this link to configure the Access Control Manager system to share information with supported database and directory structure protocols, such as Oracle RDBMS, SQL Server or LDAP directory structures.
3. Icon task bar	
Monitor	The application's oversight feature that enable the qualified operator to track events, alarms, and other system functions either by table or map.
Identities	Users are defined as operators or cardholders of this system. This includes badges and related access groups that allow access to the Access Control Manager monitored facility.
Reports	Generate and customize status reports of the Access Control Manager system.
Physical Access	Define the access control field hardware, including doors, that are connected to the Access Control Manager appliance. You can also configure anti-passback areas, card formats, events and EOL resistance values.
Roles	Roles limit or regulate the number of tasks that a specific user can perform within the Access Control Manager system.
4. Sub-options task bar	
	When you select one of the icon task bar options, the available sub-options for that task appear. This section changes depending on the icon task bar option that is selected.
5. Feature pages and fields	
	When you select a link or an option from a Task Bar, the feature is opened in this area. This is the workspace where you will be performing most of the tasks available in the Access Control Manager system.

Logging Out of the Avigilon Access Control Manager Application

From top left User links area, click **Log Out**.

The Sign In screen is displayed.

Help in Avigilon Access Control Manager

To use this help, click the **Help** link in the User links section from any page in the Avigilon Access Control Manager application.

This online help appears.

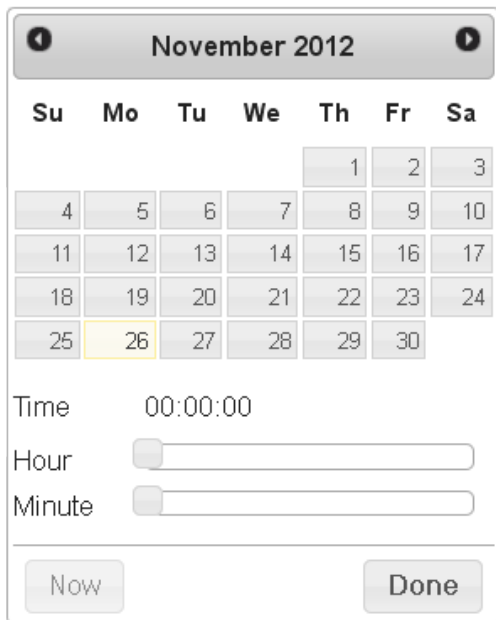
Use the navigation tools in your browser to go from topic to topic, just as you would with any browser. You can also use the options, links, and navigation tools built into the application itself.

Using a Pop-Up Calendar



When you click a **Date** field, a calendar will pop up:



Date and time calendars have additional fields:



To use the calendar:

1. Click  or  to find the month/year.
2. Click the date.
3. If you are using a date and time calendar, adjust the **Hour** and **Minute** bars until the correct time appears in the **Time** field.

If you want to select the current time, click **Now**.

4. When you're finished, click Done.

The date and time appears in the Date field.

Setting Personal Preferences

To set up your personal preferences, click **My Account** from the top left User links area. 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-left User links area, click **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.

My Account Screen - Profile Page

This is the first page you see after you click **My Account** in the User links area.


Feature	Description
Name	Displays your name as it is configured in the system.
Login	Displays your login name.
Old Password	If you need to change your password, you must first enter your current password in this field.
Password	<p>If you need to change your current password, first enter your old password in the Old Password field, then enter the new password you want to use to access your account information.</p> <p>The strength of the password you use is important. The more combinations of numbers, letters, and characters you use the more difficult it is for unauthorized individuals to break into the system. To enforce more stringent passwords, select Password Strength Enforced in the General tab of the System Settings screen.</p> <p>The password must be at least four characters long.</p>
Confirm	If you need to change your current password, enter the new password again to confirm your choice.
Defaults:	
Items/Page	<p>Enter the maximum number of items to be listed in standard tables.</p> <p>NOTE: This does not apply to non-standard tables (e.g. the Monitor Events page).</p>
Monitor dflt rows	Select the initial number of rows you can see on the Monitor screen.

Feature	Description
Badge Camera	Select the camera you want to use to capture images for this system. Only those devices previously installed and configured for this computer or network appear in the drop down window.
Photo Size	Enter the format size you want for photos captured with the camera specified above. This size is in pixels with the length and width separated by a comma (no spaces required).
Locale	Select your preferred system language. This setting overrides the default system language setting. NOTE: If you are using the Easy Lobby Integration plug-in, this requires the locale to be set as English (United States).
Home Page	From the drop down pick list, select the page you would like to appear when you first open this application. The available options are: <ul style="list-style-type: none"> • Alarms • Doors • HW Status • Identities • Monitor • Panels • Reports
Default Badge Template	Select the default badge template to use from the drop down list.
Show Timezone Offset?	Check this box to enable local time fields in Reports and Monitoring to report time with the time zone offset from the UTC time.
Do Not Log REST Command	Check this box to exclude internal system details from the transaction logs.
Clear Custom Layouts	Click this button to clear any previously configured custom layouts and return to the factory default settings.
	Click this button to save your changes.

My Account Screen - Batch Jobs

When you click the **Batch Jobs** tab from the My Account screen, a list of all the batch jobs that have been run from this user account is displayed.

Batch jobs are created on the Job Specification page.

Feature	Description
	Click this button with one or more of the batch jobs highlighted and the selected batch job(s) will be deleted.




Feature	Description
Name	The name of this batch job.
Status	The current status of this batch job (completed, in progress, or halted).
Type	The type of this batch job.
Results	The results of this job indicated by an icon.
Started At	Date and time when the job was begun.
Completed At	Date and time when the job was completed.

In addition to these read-only columns, there are a group of navigation fields and buttons at the bottom of this screen. These enable you to scroll through the batch jobs list, specify a particular page of the list, go to the beginning or end of the list, and refresh the list.

My Account Screen - Job Specification

When you click the **Job Specification** tab, a list of all the batch jobs that have been defined for this system is displayed.

You can add, delete, edit, or immediately activate an existing batch by selecting the batch from the list and click the corresponding button.

Feature	Description
Add	Click this button to schedule a new batch job.
	Click this button to delete a highlighted batch job.
	Click this button to edit a highlighted batch job. The batch job wizard appears.
	Click this button to toggle between activating or deactivating a highlighted batch job.
Name	The name of the batch job.
Author	The person who defined the batch job.
Type	The type of batch job being run.
Script	Any script that was created for this batch job.
Schedule	When this job is scheduled to be performed.
Activated On	The date/time when this job was first activated.

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

Perform this procedure to generate a custom report on a schedule.

1. Open the My Account screen and click the Job Specification tab.

The Job Specification page is displayed.

2. Click the  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... 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.

Applying Identity Profile to Groups

When you choose to create an Identity Update job, you have the option to apply a new, updated or temporary identity profile to a group.

After you make changes to an identity profile, the identities created from the identity profile are not automatically updated, you need to perform this job to apply the changes.

You can apply a temporary identity profile to a group by using the Off Identity Profile option. Once the new identity profile expires, the original identity profile is applied.

1. Open the My Account screen and click the Job Specification tab.

The Job Specification page appears.

2. Click the  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, additional 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.
 - From the **Off Identity Profile** drop down list, you have the option to select to an alternative identity profile when the first identity profile 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:

If you selected an Off Identity Profile, you will have the option to enter when the Off profile 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... 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.

Scheduling a Global Action

Perform this procedure to schedule global actions.

1. Open the My Account screen and click the Job Specification tab.

The Job Specification page appears.

2. Click the  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:

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.

- **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... 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.

Setting Batch Door Modes

Perform this procedure to change the door mode for a set of doors.

1. Open the My Account screen and click the Job Specification tab.

The Job Specification page appears.

2. Click the  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:

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.

- **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... 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.

Contacting Your Support Representative

When you click **Support** from the top left User links area, the Support page displays information on how to contact your Avigilon support representative. The system displays the following message by default:

Support

Thank you for choosing Avigilon.

For quickest support please contact your account representative xxxxx at xxxxx.

To customize this message, see *System Support* on page 241.

For More Information

Visit Avigilon at <http://www.avigilon.com> for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon software. Register online at the Avigilon Partner Portal site to begin: <http://avigilon.force.com/login>.

Support

For additional support information, visit <http://avigilon.com/support-and-downloads/>. The Avigilon Partner Portal also provides self-directed support resources — register and login at <http://avigilon.force.com/login>.

To call Avigilon Technical Support, go to <http://avigilon.com/contact-us/> to find the phone number for your country.

To email Technical Support, send your messages to support@avigilon.com.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check <http://avigilon.com/support-and-downloads/> for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to feedback@avigilon.com.

Initial Setup

After installing your Access Control Manager appliance, complete the following recommended set up procedures:

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.

Changing the Administrator Password




After you login for the first time, it is recommended that you change the default "admin" identity password.

1. From the icon task bar, click **Identities**.
2. On the Identities Listing Page, click **A**.
3. Select the **Administrator, System** identity.
4. In the Account Information area, enter a new password in the **Password** and **Confirm** field.
5. Click .

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

Creating a Super Admin Identity

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

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

These are the only settings required to create a Super Admin identity. You can add and configure more details for the account. For more information about the available Identity settings, see *Identities* on page 281.

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 system 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 Setup links area, click **Appliance**.

The Appliance Listing page is displayed. For more information, see *Appliances - Listing Page* on page 33.

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

The Appliance Add page is displayed. For more information, see *Appliances - Add Page* on page 34.

3. Enter a new hostname for the appliance.

By default, the hostname for all appliances is ACM. 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. But if you want to customize your appliance further, you can edit the system's default settings and set up the appliances backup and redundancy features.

1. In the top-right Setup links area, click **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. For more information, see *Appliances - Listing Page* on page 33.
 - **Access:** Use this page to specify and enable the controller panel types. For more information, see *Appliances - Access Page* on page 39.
 - **Ports:** Use this page to specify how the appliance Ethernet ports are used to communicate with access control devices. For more information, see *Appliances - Port Listing Page* on page 40.
 - **Replication:** Use this page to set up system replication and redundancy. For more information, see *Appliances - Replication Page* on page 44.
 - **Backups:** Use this page to set up scheduled backups for this appliance. For more information, see *Appliances - Backups Listing Page* on page 46.
 - **Logs:** Use this page to access the system logs. For more information, see *Appliances - Logs Listing Page* on page 50.
 - **Software Updates:** Use this page to update the appliance software. For more information, see *Appliances - Software Updates Page* on page 51.
 - **About:** Use this page to see the current licenses, version numbers, and status of this appliance. For more information, see *Appliances - About Page* on page 52.
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 Setup links area, click **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 appliance Replication tab allows you to set up data replication and failover so that data is not lost even if an appliance fails.

Tip: It is recommended that you set up replication before you add panels, other hardware or user details to the system. Once replication is configured, you will be able to configure the system from one location on the network rather than have to connect directly to each individual appliance.

The replication feature allows you to set up two or more appliances to copy configuration data to each other. The appliances would be able to share identities, events and other system details. Any change made to one appliance would automatically be copied to the other. You can set up appliances to replicate to each other like a Site in the Avigilon ACM 5.6.4 software, or from a primary appliance directly to a standby appliance.

The failover, or redundancy, feature allows you to set up a standby appliance to take over when the primary appliance used in daily operations fails. To use the failover feature, the standby appliance must receive replication data from each appliance it could potentially replace. The standby appliance does not have its own hardware or collaborations.

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.

The following types of failover are supported:

- Automatic failover
- Manual failover
- Manual failback

Automatic failover occurs by monitoring the health of the primary appliances. If a primary appliance is found to be unresponsive within a set period of time, the standby appliance will automatically replace the primary appliance.

Also, you can manually initiate a failover through the Access Control Manager software. 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 manually set the standby appliance to failback, or restore regular operations to the primary appliance.

Read through all of the following procedures before you configure replication and redundancy. If any detail is unclear to you, 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 in a peer-to-peer system. Changes made in one database are automatically replicated to the other. Replication can occur between two or more appliances, or it can occur between an appliance and a standby appliance.

If you only have one appliance in your system, replication is not possible. In this situation, performing periodic backups is the recommended alternative.

When you have two appliances, you 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.

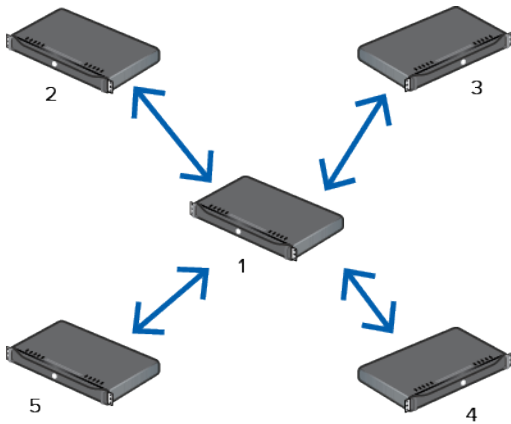


Once replication is set up, any details added to one appliance is automatically copied to the other.

When you have more than two appliances, it is recommended that you set up replication in a star formation. This allow you to perform your system configuration from one appliance and have the details automatically replicated to all the other appliances.

NOTE: You can have up to nine appliances connected together for peer-to-peer replication, including any standby appliances configured for redundancy.

Be aware that each appliance would be responsible for their connected panels, readers and other hardware. You will be able to see all system hardware from any appliance, but you will not be able to see the hardware status or change the hardware configuration outside the installed appliance.

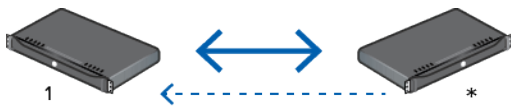


System Architecture for Failover

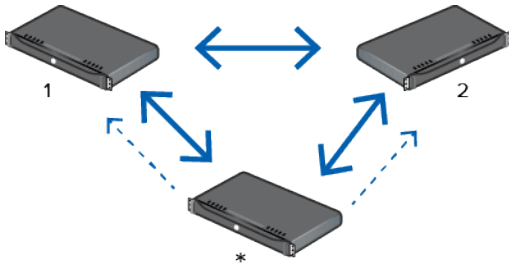
Failover works by having a configured standby appliance automatically or manually replace a failed appliance. Failover must be configured with replication or it will not function correctly.

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 user or hardware data except for the details replicated from the primary appliance. 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. Instead, the applications running on the standby appliance begin to service the records (including doors, panels, video servers, collaborations and so on) controlled by the primary appliance.

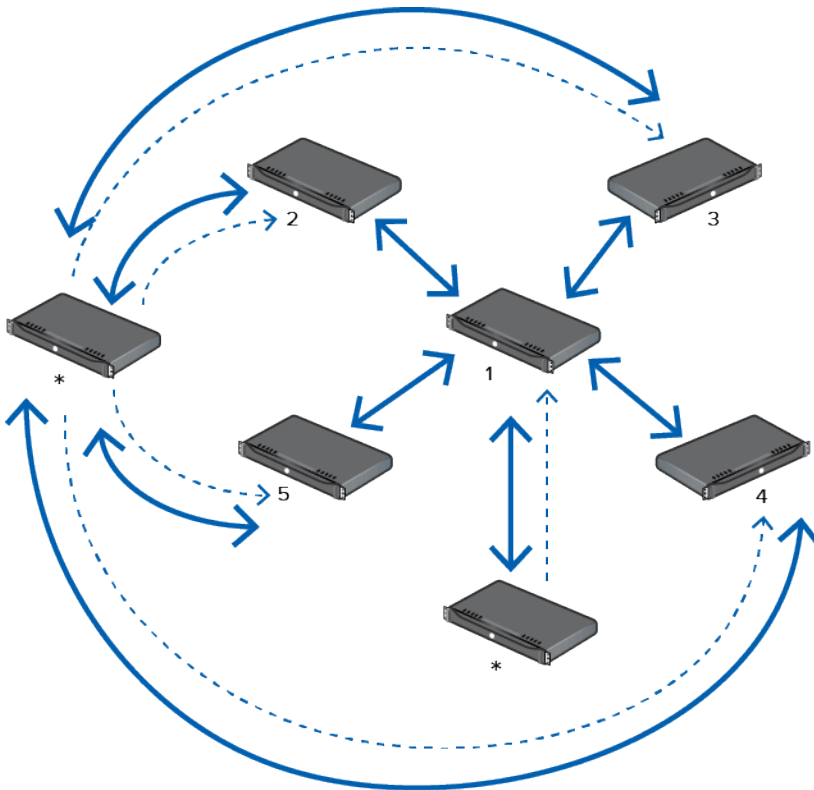
If you have one primary appliance (1) for everyday operations and one standby appliance (*), you need to set up the standby appliance to receive replicated data from the primary appliance. If the primary appliance fails, the standby can automatically step-in and maintain daily operations.



If you have more than one appliance, the standby appliance remains separate from daily operations but must receive replicated data from all appliances it is configured to failover for. Be aware that the standby appliance can only step-in for one failed appliance at a time.



If the system is configured in a star formation for replication, it is recommended that the main appliance that the other appliances replicate to have its own standby appliance. In the event of a failure, the main appliance is guaranteed to have a standby available even if more than one appliance fails.



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. A license must be separately installed on both the primary and standby appliance. 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 other appliances by host name. Each appliance must have a named server configured for this purpose.
 - Time Server IP address or host name – All appliances must be synchronized for time and date. This is absolutely crucial for proper replication processing. Each must utilize a time server for this purpose. Open LDAP multi-master replication synchronizes a 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.
- Defined and open TCP ports:
 - Web Service Port / Replication Subscriptions Port (default 443) – Certain replication options require each appliance to contact each other through the web service port.
 - LDAP Connect 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, each appliance will automatically transfer event transactions between each appliance. Connectivity is required 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.
 - 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 to 9.


NOTE: You can have up to nine 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 database updates (adding deleting system records, massaging of data) is only completed on the appliance with Address 1 as these changes are replicated to the other appliances.
- 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.

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 the previous page.

Setting Up the Primary Appliance

Whether you are configuring two or more appliances to replicate to each other, or configuring a redundant failover system, designate one appliance as the primary appliance that you will perform the majority of your system configurations on. If you are connecting your appliances into a star formation, this will be the appliance that replicates data to all the other appliances in the system.

1. Log in to the primary appliance.
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 of the DNS server used to resolve the appliance identity.
 - **Time Server** – enter the address of a time server that is accessible on the network. The time on all connected appliances must be in sync.
 - **Web Server Port** – enter the port number used for accessing the appliance web service.
 - **LDAP Connect Port** – enter the same port number on the standby appliance.
3. Click  to save your changes.


The appliance will automatically restart.

Setting Up the Secondary or Standby Appliances

Complete this procedure for all the other appliances in your system. Besides the name and hostname, it is recommended that all other settings be the same as the primary appliance.

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 of the DNS server used to resolve the appliance identity.
 - **Time Server** – enter the address of a time server that is accessible on the network. The time on all connected appliances must be in sync.
 - **Web Server Port** – enter the port number used for accessing the appliance web service.
 - **LDAP Connect Port** – enter the same port as the primary appliance.
3. If this is a standby appliance, select the **Hot Standby** check box.

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.

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 primary appliance.
2. In the top-right Setup links area, click **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:** enter 1 for the primary appliance. If you have multiple appliances in your system, you must enter a unique single digit number but one appliance must be set to "1".
 - d. **Identity Password:** enter a password for allowing data replication. It is recommended that you use the same password as the "admin" identity.
 - e. **Event Replication Port:** enter a port number that will be used by the primary appliance to replicate data to the other appliances.
4. Click  to save your changes.

Enabling Replication on the Secondary or Standby Appliance

Perform this procedure for all other appliances in the system.

1. Log in to the appliance.
2. In the top-right Setup links area, click **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 9. You cannot enter the same number twice.

NOTE: You can only have up to nine appliances 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.
4. Click  to save your changes.


3. Adding a Replication Subscription

Before you add a replication subscription between the 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.
- The appliances are able to connect to each other by their host name.
- Each appliance has a time server and a name server configured for them.
- A Web Service 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 secondary or standby appliance. After an appliance first subscribes and receives replicated data from the primary appliance, the existing LDAP database on the receiving appliance is overwritten by the replicated data. This is why it is recommended that replication and redundancy is set up before you add hardware, user identities or system configurations.

Do not add a replication subscription to a primary appliance or all configured data will be deleted.

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 Setup links area, click **Appliance**.
3. In the Replication tab, click **New** in the Replication Subscriptions area.
4. Complete the following fields:
 - a. **Host** – enter the primary appliance host name.
 - b. **Web Port** – enter the primary appliance web port number.
 - c. **Ldap Port** – enter the primary appliance LDAP port number. Should be the same as the LDAP port number on the standby appliance.
 - d. **Login** – enter `admin` for the default administrator identity. You can enter a different identity, but it must be an identity with a Super Admin role.
 - e. **Password** – enter the password for the login identity.
5. Click  to save your changes.

The Replication Setup Process Log is automatically displayed if this is the first replication subscription. Click the **Continue** button that is displayed.

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.

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.

1. Log in to the primary appliance. This procedure can only be performed on the primary appliance.
2. In the top-right Setup links area, click **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 standby appliance should check the health of the primary appliance. Do not leave the setting at 0.
- e. **Heartbeat Count:** If the standby appliance is unable to communicate with the primary appliance, enter a number of communication attempts before the standby appliance takes over for the primary appliance.

5. Click  to save your changes.

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 appliance's Failover Settings area, the 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 standby appliance assumes 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 standby will not step-in unless it is manually set to do so.

To check if a primary appliance has failed-over to a 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 standby appliance, you see that the standby has started logging hardware events on the Monitor screen.

Standby appliances do not have any connected panels or other hardware, so there should not be any events listed on the Monitor screen unless the standby appliance has replaced a primary appliance.

- When you access the **Appliance > Replication** page, the standby appliance is listed as *Active: Yes* beside the name of the inactive 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, you may want to turn-off the Monitor On failover option so that an appliance does not failover until you want it to.

To manually failover an appliance, complete the following:

1. Log in to the standby appliance.
2. Access the **Appliances > Replication** page.
3. In the Failover Settings area, click the **Take Over** button beside the appliance you want to manually failover.

After a few moments, the Active status will change to Yes beside the appliance the 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, you cannot set it to take over another appliance until after it has failed-back.

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 standby appliance.
2. Access the **Appliances > Replication** page.
3. In the Failover Settings area, click the **Fail Back** button.

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. For more information, see *Appliances - Virtual Port Add Page* on the facing page.

To enable and configure an Ethernet port:

1. From the Appliance Edit page, select the **Ports** tab.

The Port Listing page is displayed. For more information, see *Appliances - Port Listing Page* on page 40.

2. Click the name or port number from the Ethernet Ports list.

The Port: Edit page is displayed. For more information, see *Appliances - Ethernet Ports Page* on page 40.

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.

Appliances - Virtual Port Add Page

When you click **Add New Virtual Port** from the Virtual Ports Listing page, the Virtual Port Add page is displayed.

Note that the port and appliance of this virtual port is listed above the fields. Click on the relevant link to return to the main appliance or port page.

Feature	Description
Name	Enter a name for this virtual port.
IP Address	Enter the IP address for this virtual port.
Netmask	Select an address for the netmask of this virtual address. Only the netmasks currently recognized by the system are listed.
Installed	Check this box to indicate that the virtual port is enabled and communicating with the appliance.
	Click this button to save your changes.
	Click this button to discard your changes.

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. For more information, see *Appliances -*

Route Add Page on page 42.

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. For more information, see *Appliances - Serial Port Edit Page* below.

4. Select the **Enable** check box.
5. Complete the remaining fields as required to define the serial connection.
6. Click  .

Appliances - Serial Port Edit Page

When you select a serial port from the Appliance Ports Listing page, the Serial Port Edit page is displayed. This page allows you to enable and configure the serial port.

Note that the port and appliance of this serial port is listed above the fields. Click on the relevant link to return to the main appliance or port page.

Feature	Description
Type	Select the type of serial connection this is: <ul style="list-style-type: none">• Panel — this serial port is connected to a panel.• Subpanel — this serial port is connected to a subpanel.• Shell — this port is connected to a shell.
Baud rate	Select the baud rate this serial connection will run.
Flow control	Select the flow control for this connection.
Enable	Check this box to enable the serial connection.
Parameters	Select the serial values for this connection.
	Click this button to save your changes.
	Click this button to discard your changes.

Backups

Backups can be used to restore information if an appliance's configuration or transaction data ever becomes corrupted. Backups can either be scheduled or manually initiated .

Backing Up System Data

You can set up the appliance to automatically backup system configuration settings and transaction event details. More than one backup event can be created, and each backup can be stored in a different location.

NOTE: Configuration data (including tokens) and transactions data must be backed up separately.


When you configure the backup settings, you can also assign a schedule for when backups automatically occur each week.

1. From the Appliance Edit page, select the **Backups** tab.
2. Click **Add New Appliance Backup**.

The Appliance Backup: Add New page is displayed. For more information, see *Appliances - Backups Add Page* on page 47.

3. Enter a name for the back up.
4. Select the preferred **Backup Type**.

Some of the other settings change to match the selected option. Complete the new settings as required to use the preferred Backup Type.

5. From the **Data Type** drop down list, select the type of data that is in this backup.
6. Click **Browse** to select where the back up files will be stored.
7. 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.
8. Click  .

Manually Backing Up Data

After you've set up a backup event, you can manually initiate a system backup outside the configured schedule.

1. From the Appliance Edit page, select the **Backups** tab.

The Appliance Backup Listing page displays. For more information, see *Appliances - Backups Listing Page* on page 46.

2. Click **Backup Now** for the backup event that you want to initiate.

The backup for this operation is initiated.

Restoring Backups

If the appliance's configuration or transaction data ever becomes corrupted, you can restore a backup.

NOTE: You cannot restore configuration or transaction data if no backups exist.



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.

The Backup File List is displayed. For more information, see *Appliances - Backup File List* on page 49.

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.

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. For more information, see *Appliances - Logs Listing Page* on page 50.

2. Click the log you want to view.

The Appliances Log page displays. For more information, see *Appliances - Logs Page* on page 51.

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:

<http://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* below. When the update is complete, the appliance will automatically reboot. You will need to log in to the appliance again.

Appliances - About

The About section for appliances provides access to:

- review the appliance status
- the end user licence agreement, and
- licence and licence 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 Setup links area, click **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 409.

You can also review the appliance hardware status from the Monitor Screen. For more information, see *Monitor Page - Hardware Status* on page 402.

Appliances - Listing Page

The listing page only appears if there is more than one appliance in the system, otherwise the Appliance: Edit screen is displayed instead. The Appliance Listing page displays the following details about each appliance.

NOTE: An appliance can be connected to more than one panel type if the appliance license supports more than one panel manufacturer.

Feature	Description
Name	The name of the appliance. Click the name to edit the appliance details.
Host Name	The host name for this appliance. This is the name you entered in the 'Host Name' field when you added this appliance.
Log Count	The number of logs enabled for this appliance. To view the available logs or create new logs, click on this number. The log listing page appears.
Mercury Security	If this appliance is connected to Mercury Security panels, this field is marked Yes . If this appliance is not currently connected to Mercury Security panels, this field is marked No .
HID	If this appliance is connected to HID panels, this field is marked Yes . If this appliance is not currently connected to HID panels, this field is marked as No .
ISONAS	If this appliance is connected to Isonas panels and is licensed for use, this field is marked Yes . If this appliance is not currently connected to Isonas panels, this field is marked as No .
Kaba	If this appliance is connected to Kaba panels and is licensed for use, this field is marked Yes . If this appliance is not currently connected to Kaba panels, this field is marked as No .
CoreStreet	If this appliance is connected to CoreStreet panels, this field is marked Yes . If this appliance is not currently connected to CoreStreet panels, this field is marked No .
Delete	Click  to delete the specified appliance.
Add New Appliance	Click this button to add a new appliance to the available list.
Create New Report	Click this button to generate a standard report on the appliance list.



Appliances - Add Page

When you click the **Add New Appliance** button from the Appliances Listing page, the Appliance Add page is displayed. Enter the required appliance details.

Feature	Description
Name	Enter a name for this appliance.
System Name	This read-only field gives the name of the entire Access Control Manager system.
Host Name	This is the DNS name for the appliance and is used under the 'Host Name' field on the Appliance Listing page.

Feature	Description
Domain Name	The domain name where this appliance resides.
Name Server	The name of the domain server.
Time zone	From the drop down list, select the timezone of the appliance.
Time Server	Enter the address of the Network Time Protocol (NTP) server used to keep time for this appliance.
Hot Standby	<p>Check this box to indicate that this appliance is the hot standby (backup) for the master appliance.</p> <p>If the master appliance fails, this appliance will take over. For more information, see <i>Configuring Replication and Failover</i> on page 17.</p>
Enable Remote TCP/IP Management	<p>Check this box to allow this appliance to use remote TCP/IP management.</p> <p>For security this feature is disabled (i.e. unchecked) by default. The functionality will also be reset to disabled automatically following a software update.</p>
Stored Transactions	<p>Enter the maximum number of transactions that can be stored on the appliance.</p> <p>When the number of transactions exceeds this limit, new transactions will start overwriting previously stored transactions.</p> <p>The default is 1,000,000 transactions.</p>
Hardware Type	From the drop down list, select which Access Control Manager appliance this is.
Web Server Port	Specify the port number that is used to connect the web server to this appliance.
Service Port	Specify the port number that is used to access diagnostics and service for this appliance.
Edge Listen Port	<p>Specify the port number that accesses the listening feature on this appliance for HID Edge panel communication.</p> <p>This field only applies to HID Edge devices.</p>
Ldap Connect Port	<p>Specify the port number that enables communications between this appliance and other IP network-attached entities using LDAP information service protocol.</p> <p>This field is only applicable for LDAP devices.</p>
Transactions Connect Port	Specify the port number used for connecting to the Postgres ¹ transaction database for ODBC connections.
Mercury Client Port	<p>Specify the port number used to set the port you wish this appliance to use in order to listen for IP client panel connections.</p> <p>NOTE: This must be the same port configured on all of the IP Client panels that will connect to this appliance.</p>
Mercury-Require TLS	Check this box, if required, to encrypt connections between the appliance and the Mercury Panel.

¹An object-relational database management system (ORDBMS) available for many platforms including Linux, FreeBSD, Solaris, Microsoft Windows and Mac OS X. Also called PostgreSQL

Feature	Description
	NOTE: All IP client panels connecting to this appliance must be configured for ' TLS ¹ Required' if this option is checked
SMTP Server	Enter the mailbox server for this system. This is the name of the server that handles the transfer of email. This field and the next four are required before email alerts can be sent automatically in case of an alarm or event occurs.
SMTP Port	Enter the name of the port that the Host uses to connect to the SMTP ² Server.
SMTP Host Name	Enter the name of the host used for SMTP traffic.
Use Start TLS	Check this box to indicate that this appliance uses Start TLS cryptography to communicate with the SMTP server.
Use TLS	Check this box to indicate that this appliance uses generic TLS cryptography to communicate with the SMTP server.
SMTP From	Enter the email address of the person or organization that email will be from.
SMTP User	Enter the email addresses of persons or organizations to which email alerts are sent in case of alarms.
SMTP Password	Enter the password required to use the email server.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Appliance Page

The **Appliance** tab on the Appliance Edit screen allows you to edit and define the appliance identity and port settings.

Feature	Description
Appliance Name	Enter a name for this appliance.
System Name	This read-only field designates the name of the entire Access Control Manager system.

¹Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which are designed to provide communication security over the Internet.

²Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Feature	Description
Host Name	This is the DNS name for this appliance and is identified as such under the 'DNS Name' field on the Appliance Listing page.
Domain Name	Enter the domain name where this appliance resides.
Name Server	Enter the name of the domain server.
Time Server	Enter the time server connected to this appliance.
Time Zone	From the drop down pick list, specify the time zone where this appliance resides.
Time Server	Enter the name of the server used as the de facto time keeper for this appliance.
Hot Standby	<p>Check this box to indicate that this appliance is the hot standby (backup) for a primary appliance.</p> <p>If the primary appliance fails, this appliance will take over. For more on this, refer to <i>Appliances - Replication Page</i> on page 44.</p>
Enable Remote TCP/IP Management	<p>Check this box to indicate that this appliance can use remote TCP/IP management.</p> <p>For security this feature is disabled (i.e. unchecked) by default. The functionality will also be reset to disabled automatically following a software update.</p>
Splunk URL	URL for the Splunk collaboration. Splunk is a log aggregation product.
APB Reset	Click this button to reset all of the APB ¹ settings on this appliance.
Reboot Appliance	<p>Click this button to reboot the appliance. This will automatically restart the appliance.</p> <p>This button can be used when the appliance has frozen or experienced other problems.</p>
Shutdown Appliance	<p>Click this button to shut down the appliance.</p> <p>This button can be used when you need to turn off the appliance for maintenance or re-configuration.</p>
Date/Time	This read-only field displays the current date and time set for this appliance. To reset this field, click the Set Date/Time button.
Set Date/Time	Click this button to reset the date and time for this appliance then enter a new date and time in the field to the right.
Stored Transactions	<p>Enter the maximum number of transactions that can be stored in this appliance.</p> <p>When the number of transactions exceeds this limit, new transactions will start overwriting previously stored transactions.</p> <p>The default is 1,000,000 transactions.</p>
Hardware Type	From the drop down pick list, select which Access Control Manager appliance is being used for this appliance.
Web Server Port	<p>Specify the port number that is used to connect the web server to this appliance.</p> <p>The default port value is 443. (If 80 is specified, the application automatically redirects the value to 443.)</p>
Service Port	Specify the port number that is used to access diagnostics and service for this appliance.

¹See Anti-Passback.



Feature	Description
	The default port value is 6050 .
Edge Listen Port	Specify the port number that accesses the listening feature on this appliance for HID Edge panel communication. NOTE: This field only applies to HID Edge devices.
LDAP Connect Port	Specify the port number that enables communications between this appliance and other IP network-attached entities using LDAP information service protocol. This field is only applicable for LDAP devices.
Transactions Connect Port	Specify the port number used for connecting to the Postgres ¹ transaction database for ODBC connections.
Mercury Client Port	Specify the port number used to set the port you wish this appliance to use in order to listen for IP client panel connections. NOTE: This must be the same port configured on all of the IP Client panels that will connect to this appliance.
Mercury Require TLS	Check this box, if required, to encrypt connections between the appliance and the Mercury Panel. All IP client panels connecting to this appliance must be configured for 'TLS Required' if this option is checked.
SMTP Server	Enter the mailbox server for this system. This is the name of the server that handles the transfer of email. This field and the next four are required before email alerts can be sent automatically in case of an alarm or event occurs.
SMTP Port	Enter the name of the port that the Host uses to connect to the SMTP ² Server.
SMTP Host Name	Enter the name of the host used for SMTP traffic.
Use Start TLS	Check this box to indicate that this appliance uses Start TLS ³ cryptography to communicate with the SMTP server.
Use TLS	Check this box to indicate that this appliance uses generic TLS ⁴ cryptography to communicate with the SMTP server.
SMTP Mail From	Enter the email address of the person or organization that email will be from.
SMTP User	Enter the email addresses of persons or organizations to which email alerts are sent in case of alarms.
SMTP Password	Enter the password required to use the email server.

¹An object-relational database management system (ORDBMS) available for many platforms including Linux, FreeBSD, Solaris, Microsoft Windows and Mac OS X. Also called PostgreSQL

²Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

³Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which are designed to provide communication security over the Internet.

⁴Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which are designed to provide communication security over the Internet.

Feature	Description
Send Test Email	Click to send a test email to the 'SMTP Mail from' email address.
Partitions	If partitions are defined for this system, this window appears. From the window, click to highlight one or more partitions that are assigned to this appliance. Only those partitions previously defined for this system appear in this window. If no partitions are defined for this system, this field does not appear.
Tactical Settings:	
Tactical Master	From the drop down list, select the tactical master this appliance is using. Only those tactical masters configured for this system appear in the list. If no tactical masters are configured for this system, this field is blank.
Manage Hardware	Check this box to indicate that the tactical master specified above should manage this appliance and its connected hardware.
Transfer Events	Check this box to indicate that the tactical master is enabled to exchange events with the appliance.
	Click this button to save your changes.
	Click this button to discard your changes.



Appliances - Access Page

The **Access** tab on the Appliance Edit screen allows you to identify which door panel manufacturers are installed in the system.

NOTE: Only the manufacturers supported by the system license is listed on the Access page. For example, if your system license only supports Mercury Security, only Mercury Security is listed as an option.

Be careful to select all the manufacturers that are installed in the system. The selected options will determine the properties and pages that are available when you configure panels and doors.

If your system uses a panel manufacturer that is not listed on the Access page, you may need to upgrade your system license. Contact your support representative for more information.

Feature	Description
Installed	Check this box to indicate that there are panels from the manufacturer installed.
Debug	Check this box to indicate that the appliance can be used to debug the panels from the manufacturer.
Vendor	This is the list of all the manufacturers supported by the Access Control Manager system license.
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Port Listing Page

When you select the **Ports** tab from the Appliance Edit screen, a list of all the appliance's Ethernet ports and serial ports is displayed.

The Port Listing page displays the following details about each Ethernet and serial port.



Feature	Description
Ethernet Ports	
Port	The number of the Ethernet port. Up to eight Ethernet ports may appear on the list. To edit an Ethernet port, click on the port name or number.
Name	The name of the Ethernet port. To edit an Ethernet port, click on the port name or number.
Virtual	The number of virtual ports associated with this Ethernet port. To add or edit a virtual port, click Virtual in the far right column.
IP Address	The IP address for the port.
Gateway	The gateway that is used by the port.
Netmask	The netmask for the port.
Virtual/Routes	Click Virtual to access the Virtual Ports List page. From that page, you can add and edit the available virtual ports. Click Routes to access the Routes Listing page. From that page, you can add and edit the communication route used between the appliance and panel.
Serial Ports	
Port	The name of the available serial port. To edit and enable this port, click the port name.
Enable	Indicates if the serial port is enabled. Yes or No.
Baud	Indicates the baud rate currently defined for this port.
Parameters	Indicates the parameter values currently defined for this port.
Flow	Indicates the flow control values currently defined for this port.

Appliances - Ethernet Ports Page

When you select an Ethernet port from the Appliance Port Listing page, the Ethernet Ports page is displayed.

This page allows you to define the current Ethernet connection between the appliance and the panels it controls.


Feature	Description
Name	This field contains the name of the Ethernet port. Initially, the name that appears is the current or default name of the port; however, you can enter a new name if you require.
Link Status	This read-only field indicates whether the connection is currently up or down.

Feature	Description
IP Address	Enter the IP address for this port. If you aren't sure what the address is, consult your IT administrator. NOTE: If you assign or change an IP address, make sure that any switches or routers on the appliance's network recognize the changed address. To do this, either: <ul style="list-style-type: none"> reboot the appliance, or unplug the Ethernet cable, wait a few seconds, then plug it back in
Netmask	Select the netmask required for addressing this connection. The values are 0 - 32 bits where a 24 -bit netmask is the default value.
Network Gateway	Enter the network gateway address this appliance will use.
MAC Address	This read-only field displays the MAC address for this appliance.
Installed	Check this box to indicate that this Ethernet port is already connected to a panel.
Data rate	This read-only field specifies the current data rate detected for this connection.
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Ethernet Virtual Listing page

When you click a **Virtual** link from Appliance Ports Listing page, the Ethernet Virtual Listing page is displayed.



This page contains a list of the virtual ports for this physical Ethernet port. You can choose to add new virtual ports as needed.

Feature	Description
Virtual Port	The name of this virtual port. You can edit the details of this port by clicking its name.
Installed	Indicates that the virtual port is enabled (Yes) or disabled (No).
State	The IP address for this virtual port.
Netmask	The size, in bits, of the netmask for this virtual address. The default value is 24 bits.
Delete	Click  to delete the selected virtual port.
Add New Virtual Port	Click this button to add a new virtual port for this appliance.

Appliances - Virtual Port Edit Page

When you select an existing Virtual Port name from the Virtual Port Listing page, the Virtual Port Edit page is displayed. This page allows you to edit the details of the virtual port.


Note that the port and appliance of this virtual port is listed above the fields. Click on the relevant link to return to the main appliance or port page.

Feature	Description
Name	Enter or modify the name of this virtual port.
IP Address	Enter or modify the IP address for this virtual port.
Netmask	Select an address for the netmask of this virtual address. Only the netmasks currently recognized by the system are listed.
Installed	Check this box to indicate that this virtual port is enabled and communicating with the appliance.
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Routes Listing Page

When you click the **Routes** link from Appliance Ports Listing page, the Routes Listing page is displayed.

This page displays the communication routes used by the appliance and the destination panel. Only the routes currently defined for this system are listed.



Feature	Description
Appliance	Appliance for this destination panel.
Port	Port for this destination panel.
Destination IP	The IP address for the destination panel you want. To change the destination IP address, click this address and the Edit Routes page appears.
Destination Netmask	The netmask address for this destination panel.
Gateway	Gateway address for this destination panel.
Metric	The metric interface specified for this destination panel.
Enabled	Indicates whether this destination panel is connected and functional (Yes) or not (No).
Delete	Click  to delete the selected Ethernet route.
Add New Route	Click this button to add another route to this list.

Appliances - Route Add Page

When you click **Add New Route** from the Appliance Routes Listing page, the Route Add page is displayed. This page allows you to add a new communication route between the appliance and the destination panel.

Note that the port and appliance of this virtual port is listed above the fields. Click on the relevant link to return to the main appliance or port page.



Feature	Description
Destination IP Address	Enter the IP address for the destination panel.
Destination Netmask	Enter the netmask for this destination panel.
Gateway	Enter the gateway address for this destination panel.

Feature	Description
Metric	Enter the metric required for this destination panel.
Enabled	Check this box to indicate that this destination panel is connected and functional.
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Route Edit Page

When you click the Destination IP of a route from the Appliance Route Listing page, the Route: Edit page is displayed. This page allows you to edit the communication route between the appliance and the destination panel.

Note that the port and appliance of this virtual port is listed above the fields. Click on the relevant link to return to the main appliance or port page.



Feature	Description
Destination IP Address	Enter the IP address for the destination panel.
Destination Netmask	Enter the netmask for this destination panel.
Gateway	Enter the gateway address for this destination panel.
Metric	Enter the metric required for this destination panel.
Enabled	Check this box to indicate that this destination panel is connected and functional.
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Serial Port Edit Page

When you select a serial port from the Appliance Ports Listing page, the Serial Port: Edit page is displayed. This page allows you to enable and configure the serial port.

Note that the port and appliance of this serial port is listed above the fields. Click on the relevant link to return to the main appliance or port page.

Feature	Description
Type	Select the type of serial connection this is: <ul style="list-style-type: none"> • Panel — this serial port is connected to a panel. • Subpanel — this serial port is connected to a subpanel. • Shell — this port is connected to a shell.
Baud	Select the baud rate this serial connection will run.
Flow	Select the flow control for this connection.
Enable	Check this box to enable the serial connection.
Parameters	Select the serial values for this connection.

Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Replication Page

When you select the **Replication** tab from the Appliance: Edit page, the Replication Settings page is displayed.

This page allows the administrator to configure data replication and system redundancy.

NOTE: Only the "admin" identity is allowed to modify these settings.

- Replication allows all configuration and system data to be continuously copied between appliances so that details and configurations can be shared.
- Redundancy allows a standby appliance to be configured to replace or failover an active appliance in the event of a system failure.

If you require assistance in setting up replication and redundancy, contact Avigilon Technical Support.

Replication Page

When you select the **Replication** tab from the Appliance: Edit page, the Replication Settings page is displayed.

Only the "admin" identity is allowed to modify these settings.


NOTE: DO NOT make any changes to this page until after you've read all the details about replication and redundancy. To begin, see *Configuring Replication and Failover* on page 17.

Feature	Description
Replication¹ Settings — In this area, enable replication and set how frequently the appliance will connect with other appliances and synchronize data.	
Enable Replication	Check this box to enable replication for this appliance.
Enable Encryption	Check this box to enable encryption of all communications between peers used to replicate data.
Address	Enter an address for this appliance that is unique across this enterprise network. The address must be a number between 1-255. One of the appliances must be set to address 1.
Identity Password	Enter the password that enables this appliance to enter and use the designated peer.
Event Replication Port	Enter the replication port for this appliance.
Initial Retry Time	Enter the number of seconds the appliance will wait after requesting access to the designated peer before it times out.

¹The process of copying and synchronizing the LDAP database between two or more appliances so that they share the same configuration information.

Feature	Description
Initial Retry Count	Enter the number of times the appliance can request access to the designated peer before issuing an alarm.
Last Retry Time	Enter the number of seconds the appliance will wait after requesting access to the designated peer before it times out.
Last Retry Count	Enter the number of times the appliance can request access to the designated peer before issuing an alarm. A value of 0 indicates that there is an unlimited count.
Timeout	Enter the number of seconds allowed before the replication process times out. An alarm is issued and you are queried to retry.
Network Timeout	Enter the number of seconds allowed for the appliance replication program and the network target to sync up before the process times out. An alarm is issued and you are queried to retry.
Keep Alive	Enter how often you want to test the connection between the primary appliance and the secondary appliance. <i>(##:##:##) = ## seconds the system must be idle before the connection is tested: # probes the system sends to test the connection : ## seconds between each probe.</i>



Replication Subscriptions — In this area, configure appliances to receive replicated data.

New	Click this button to begin the subscription process. The following fields appear: <ul style="list-style-type: none"> • Host — Enter the primary appliance hostname. • Web Port — Enter the primary appliance web service port number. The default port number is 443. • Ldap Port — Enter the LDAP port number on the primary appliance. • Login — Enter the username for a Super Admin identity on the primary appliance. • Password — Enter the password for the Super Admin identity.
	Click this icon to delete this subscription account information.
RID	The Replication Subscriber ID. Typically 1 is the primary appliance, 2 is the standby appliance.
CSN	Change Sequence Number. Displays the date and time when the last replication occurred.
Name	The subscribed appliance in name from the LDAP database.

Transaction Replication Status — this area displays the current status of all transactions that have occurred between the primary appliance and the secondary appliance.

Failover¹ Settings — For the primary appliance, select the standby appliance that the system will failover, or

¹When an appliance fails, a configured standby appliance is able to automatically, or manually, take its place so that the system can continue to run.

Feature	Description
	<p>use as a hot standby, if the primary appliance fails.</p> <p>For secondary appliances, this area will display the appliances it will stand-in for in the event of a system failure.</p>
Standby Appliance	From the drop down list, select the standby appliance to be used for redundancy.
TCP Port	Enter the primary appliance's TCP port to communicate its health status to the secondary appliance.
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.
Heartbeat Count	Enter the number of failures in a row before the secondary appliance takes over for the primary appliance. If you leave the setting at 0, the system defaults to 5.
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 loses network connectivity unexpectedly.
Active	<p>Indicates if the appliance you are logged in to is active.</p> <p>In a primary appliance, this read-only setting is displayed as a check box. If it is checked, the primary appliance is active.</p> <p>In a standby appliance, this read-only setting is displayed as "Yes" or "No" under the Active column:</p> <ul style="list-style-type: none"> • Yes – the standby appliance is currently active and is replacing the appliance listed under the Appliance column. • No – the standby appliance is not currently active and is on standby.
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Backups Listing Page


When you select the **Backups** tab from the Appliance: Edit page, the Appliance Backup Listing page is displayed.

This page displays all the backup events that have been configured for the appliance.

The difference between replicating data and backing up data is:

- In replication, all relevant data is copied from the primary appliance to a secondary appliance in anticipation of primary appliance failure (replication); in the event that the primary appliance fails, control of the system is automatically shifted to the second appliance (redundancy). See *Appliances - Replication Page* on page 44 for more information.
- In backup, data on the primary appliance is copied to a host computer where it is stored. In the event that

the information in the primary appliance becomes corrupted, this backup data can be transferred to the primary and replace the corrupted data.



Feature	Description
Name	The name of the backup. Click the name to open the Backup Edit page.
Backup Type	The type of location the backup files are stored in.
Data Type	Displays if the backup is for configuration data or transaction data.
	Click this button to delete the backup.
Backup Now	Click this button to initiate a backup outside the configured schedule.
File List	Click this button to display a list of the backup files that have been generated from the appliance.
USB state	Indicates the current state of the USB connection between the backup device and the appliance. This read-only field is only relevant if this backup is a USB backup type.
Mount USB	Click this button to mount (connect) the relevant backup device to the appliance.
Un-Mount USB	Click this button to unmount (disconnect) the relevant backup device to the appliance.
Add New Appliance Backup	Click this button to create a new backup event.

Appliances - Backups Add Page

When you click the **Add New Appliance Backup** button on the Appliance Backups Listing page, the Appliance Backup: Add New page is displayed. This page allows you to set up a new backup schedule for the appliance.

Feature	Description
Name	Enter the name of this backup. It is recommended that the name does not use spaces, like <i>Avgilon_Corp</i> .
Host	If you are using Windows Share , enter the IP address of backup network location and the directory separated by a forward slash (/). If you are using SCP , enter the host name (which can be just the IP address) without the directory.
Port	Enter the port for the backup.
Host Login	Enter the username required to log into the backup location.
Host Password	Enter the password required to log into the backup location.
Backup Type	From the drop down list, select the backup type. There are three types available: <ul style="list-style-type: none"> SCP¹ — Secure Copy. Securely transfer backup data from the appliance to a remote host

¹Secure Copy Protocol is the most basic backup protocol and does not require much adjustment before it can work properly. It can work effectively on Linux and other Unix-like systems. To start work, its enough to install the SCP program on the server and establish the connection.



Feature	Description
	<p>location.</p> <ul style="list-style-type: none"> • USB — Transfer backup data to a device connected to the appliance via a USB cable. • Windows Share — Transfer backup data to a Windows network location. <p>The page refreshes to display different options depending on the selected backup type.</p>
Data Type	<p>Select the backup data type:</p> <ul style="list-style-type: none"> • Configuration — back up all configuration data from the appliance. • Transactions — back up all event data that occur within the system.
Location	<p>Enter the name of the subdirectory where the backup files are stored.</p> <p>If the file is to be located in a subdirectory of the share, use this format:</p> <p><i>directory_name/</i></p> <p>Notice that the directory name needs both a leading slash and a trailing slash.</p> <p>If the file is to be located in the top level of the share (no subdirectory), use this format:</p> <p><i>/directory_name</i></p> <p>Notice that there is only one leading slash required.</p> <p>There must be an entry in the Location field for the backup to work.</p>
Use Encryption	<p>Check this box to encrypt the backup data using AES 256-bit encryption. By default, the password (key) for the encrypted file is the name of the appliance.</p>
Schedule	<p>Select the days of the week when the backup should occur.</p>
Start Time	<p>Enter the time when the backup should occur. This field uses a 24-hour clock.</p>
	<p>Click this button to save your changes.</p>
	<p>Click this button to discard your changes.</p>

Appliances - Backups Edit Page

When you click the name of a backup schedule on the Appliance Backups Listing page, the Backup Edit page is displayed.

Make the changes that are required.

Feature	Description
Name	<p>Name of this backup. It is recommended that the name does not use spaces. For example: <i>Avigilon_Corp.</i></p>
Host	<p>If you are using Windows Share, enter the IP address of backup network location and the directory separated by a forward slash (/).</p> <p>If you are using SCP, enter the host name (which can be just the IP address) without the directory.</p>
Port	<p>Port for the backup.</p>

Feature	Description
Host Login	Enter the username required to log into the backup location.
Host Password	Enter the password required to log into the backup location.
Backup Type	From the drop down list, select the backup type. There are three types available: <ul style="list-style-type: none"> • SCP¹ — Secure Copy. Securely transfer backup data from the appliance to a remote host location. • USB — Transfer backup data to a device connected to the appliance via a USB cable. • Windows Share — Transfer backup data to a Windows network location.
Data Type	You cannot edit the set data type. To change the data type, you will need to create a new backup. <ul style="list-style-type: none"> • Configuration — back up all configuration data from the appliance. • Transactions — back up all event data that occur within the system.
Location	Enter the name of the subdirectory where the backup files are stored. If the file is to be located in a subdirectory of the share, use this format: <i>directory_name/</i> Notice that the directory name needs both a leading slash and a trailing slash. If the file is to be located in the top level of the share (no subdirectory), use this format: <i>/directory_name</i> Notice that there is only one leading slash required. There must be an entry in the Location field for the backup to work.
Use Encryption	Check this box to encrypt the backup data using AES 256-bit encryption. By default, the password (key) for the encrypted file is the name of the appliance.
Schedule	Select the days of the week when the backup should occur.
Start Time	Enter the time when the backup should occur. This field uses a 24-hour clock.
	Click this button to save your changes.
	Click this button to discard your changes.

Appliances - Backup File List

When you have a backup event, you can click **File List** on the Backup Listing page to see all the backup files that have been generated from the system.

Note that the Appliance and Backup Plan are listed at the top of the page.

¹Secure Copy Protocol is the most basic backup protocol and does not require much adjustment before it can work properly. It can work effectively on Linux and other Unix-like systems. To start work, its enough to install the SCP program on the server and establish the connection.

Feature	Description
File Name	The name of the backup file. The name is typically generated in this format: <appliance name>-<date: yyyyMMDDHHMMSS>
Date	The date and time when the backup file was generated.
Restore	Click this button to restore the backup to the appliance.
Return	Click to return to the Appliance Backup Listing page.

Appliances - Logs Listing Page

When you select the **Logs** tab from the Appliance Edit page, the Appliance Log Listing page is displayed.

The most commonly used logs are:


- <backup task name>.txt: This log contains information about the last backup that was performed. The log uses the same name as the backup schedule that is configured in the appliance Backups tab.
- identity_collab.txt: This log contains information about identity collaborations.
- upgrade.txt: This log contains information about the last appliance upgrade that was installed.
- upgradehistory.txt: This log contains information about all the upgrades that have been installed on the appliance.
- testemail.txt: This log contains details about communication between the appliance and the configured email server.

The other appliance logs include:

- hal.txt: This log contains information about hardware connectivity/communication, event and alarm processing and database operations
- mercury.txt: This log contains Mercury-specific information about hardware communications to and from the appliance.
- rails_log.txt: This log contains information and details about errors in the user interface.
- thin.0.txt - thin.5.txt: These six logs store information about client connections and activity with the appliance.
- webserver_log.txt: This log contains information about the appliance web server process.

The Appliance Log Listing page displays the appliance details at the top of the page, along with the following details about each log.

Feature	Description
Name	The name of the log. Click the name of the log to display the full log text. Tip: Right-click the name and select the save link as option to save a copy of the log in HTML format.
Size (Bytes)	The size of the text file, in bytes.
Last Modified	The last time and date this file was modified.

Feature	Description
Delete	Click  to clear the contents of the log file. The system automatically re-populates the log with new details as they occur.

Appliances - Logs Page

When you select a log from the Appliance Logs Listing page, the full text of the log is displayed.



Each log will look different because of the different activities that are tracked by the log.

The Appliance and Log display at the top of the screen for each log.

Be aware that the log details are displayed in chronological order. The earliest log event is displayed at the top, and the most recent is displayed at the bottom.

Appliances - Software Updates Page



When you select the **Software Update** tab from the Appliance Edit page, the Software Updates Listing page is displayed. This page displays all the software updates that have been uploaded to the appliance.

Feature	Description
Report Trx backlog	The number of software updates still waiting to be transferred.
Report Audit backlog	The number of audit reports still waiting to be sent.
File Name	The name of the update file currently available to this appliance.
Size (Bytes)	The size of the update file in bytes.
Upload Date	The time and date when this update file was uploaded to the appliance.
Actions	 – Click this button to apply the update to this appliance.  – Click this button to delete the update file from this list.
Add New Software Update	Click this button to add a new update file to the list.

Appliances - Software Update Add Page

When you click **Add New Software Update** on the Software Update Listing page, the Software Update: Add New page is displayed.

This page allows you to upload a new version of the software from anywhere on the network to the appliance.



Feature	Description
Upload Software file	Click the Browse button to locate the latest software file that you downloaded from the Avigilon website.
	Click this button to upload the new software to the appliance.
	Click this button to discard your changes.

Appliances - About Page

When you select the **About** tab from the Appliance Edit page, the appliance version, status and license details are displayed.









On this page, you can add or upgrade licenses on the appliance.

Feature	Description
Appliance Name	The name of the appliance.
Avigilon Access Control Manager Application Software Version	The current software version running on this appliance.
Avigilon Access Control Manager Database Version	The current database version running on this appliance.
Licensing Status	
This product is licensed to	The person or company this appliance is licensed to.
End User License Agreement Status	The current status of the license.
View End User License Agreement Terms and Conditions	Click this link to review the software end user license agreement.
License File Information	
Counts	The number of readers licensed to this appliance. Includes: <ul style="list-style-type: none">• Mercury readers.• HID readers.• ACM migrations.
Fingerprint	The ID of this appliance. It matches the appliance's MAC address and is the primary method you will use to identify your unit when you call Avigilon technical support or sales.
License Expiration	The date when the appliance's license expires.
License Generated	The date when appliance's license was generated.
Manufacturers	The panel and reader vendors that are licensed to run with the appliance. Only the vendors listed here will appear as an option when you configure the Access Control Manager system.
Video	The video system vendors that are licensed to run with the appliance. Only the vendors listed here will appear as an option when you configure the Access Control Manager system.
Collaborations	Specifies the database protocols that are licensed to this application.
Options	Specifies the features this appliance supports.
License	The license number of this appliance. You can paste a new license into this field to upgrade the license.
License Key	The encrypted license key that enables this appliance to communicate securely with attached panels and doors. You can paste a new license into this field to

Feature	Description
	upgrade the license.
Appliance Diagnostic Information	
Appliance name	Displays the name of the current appliance.
Timestamp	Displays the date and time when the appliance initially went online.
Up	Displays the time this appliance has been running.
RAM	Displays the percentage of installed RAM that is available.
Program	Displays the number of programs that is running on the appliance.
Database	Displays the free space currently available on the data (writable) portion of the disk.
Load	Indicates the current compute load the Access Control Manager server is experiencing.
Port	Indicates the number of ports the server is currently using to connect to the Access Control Manager system.
Link	Indicates the current state of the link supported by the indicated port. This is either Normal or None .
Rx	Indicates the number of data packets the designated Access Control Manager server port has received.
Tx	Indicates the number of data packets the designated Access Control Manager server port has transmitted.
	Click this button to save your changes.
	Click this button to discard your changes.

Physical Access - Main Page

When you click **Physical Access** from the icon task bar on the home page, the following sub-options are displayed:

Feature	Description
	Doors - This feature enables the qualified operator to define and maintain doors connected to the defined panels.
	Panels - This feature enables the qualified operator to define and maintain panels connected to an existing appliance.
	Areas - This feature enables the qualified operator to define and maintain areas within a physical installation.
	EOL Resistance - This feature enables the qualified operator to define and maintain end-of-line resistance values for inputs.
	Card Formats - This feature enables the qualified operator to define and maintain card formats that are assigned to badges for different reader types.
	Events - Introduction on page 197 - This feature enables the qualified operator to define and maintain events that can be detected by doors and panels and routed to the Avigilon Access Control Manager application.
	Global Actions - This feature enables the qualified operator to define an action (as defined by a macro or video server soft trigger) to be performed on a specified number of doors controlled by a single panel or subpanel.
	Global Linkages - This feature enables the qualified operator to define an action (as defined by a macro) to be performed for multiple devices or events controlled by an appliance.

Output Modes

Outputs operate in two modes:

- **Operating mode** – how the output behaves during normal operation.
- **Offline mode** – how the output behaves if the appliance or panel is not available.

Operating Mode

If you see 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.

Offline Mode

Some outputs are able to act independently in the event of a communication failure. If you see the Offline Mode option when editing an output, you can set one of the following options to define how the output behaves if it is unable to communicate with the appliance or panel.

Feature	Description
No Change	The output acts the same in operating and offline mode.
Inactive	The output is inactive if the connected panel is offline.
Active	The output continues to be active if the connected panel is offline.

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 57 and *Configuring Panels* on page 111.

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 through the Subpanel Status page.

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.

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* below and *Configuring Panels* on page 111.

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 entirely through these methods:

Configuring Doors

Doors 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

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.

Adding Doors

To add a new door:

1. From the icon task bar, click **Physical Access**.
2. On the Door listing page, click **Add New Door**.
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. For more information see *Doors - Mercury Security New Parameters Page* on page 71 or *Doors - HID™ New Parameters Page* on page 69.

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 117.

1. From the icon task bar, select **Physical Access**.
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

1. From the Door Listing page, click on the name of an existing door.
The Door Edit screen for that specific door is displayed.
2. Edit each tab as required. 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.
3. After editing each tab, click  to save your changes.

Doors - Editing HID™ Doors


1. At the main page, click on the **Physical Access**.
2. At the left icon bar, click on **Doors**.
The Doors Listing page appears.
3. From the Doors Listing page, click the HID door name you want to edit.
The Doors Edit screen for that specific door type appears.
4. Edit the door by changing values on each of the door option tabs.
5. When you're finished, click  .
You are returned to the Listing page with all changes saved.

Doors - Editing Mercury Security Doors

To edit an existing Mercury Security door:

1. At the icon task bar of the home page, click **Physical Access**.
The Doors Listing page appears.
2. Click the door name to select the door you want to edit.
The Mercury Security Door Edit screen for that specific door appears.
3. Edit this door by changing values on these pages:

- [Parameters](#)
- [Operations](#)
- [Hardware](#)
- [Elev](#)
- [Cameras](#)
- [Interlocks](#)
- [Events](#)
- [Access](#)
- [Transactions](#)

4. When you're finished, click .

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

Searching for Existing Doors

Many facilities require the control and monitoring of dozens, even hundreds, of doors simultaneously. This can result in a very crowded listing page. You can search for specific doors to narrow the list of doors appearing on the Door Listing page.

1. At the top of the Door Listing page, enter your search term in the **Criteria** field.

Tip: Use any series of letters and numbers to search for the doors you want to see. If needed, use wildcard characters.

2. If you know, select the appliance the door is connected to.
3. If you know, select if the door is currently installed or not.
4. Click **Search**.

The Door Listing page refreshes to show the doors that meet your search criteria.










Controlling Doors

From the Door Listing page, you can choose to control the door through the Access Control Manager software.


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. Click any of the following buttons:

-  — Click this button to disable the specified door. This door will stop operating and allow no access.
-  — Click this button to unlock the specified door. This door will remain unlocked until the **Lock** command is issued or until another change of state is directed (either via operator override or scheduled action).
-  — Click this button to lock the specified door. This door will remain locked until the **Unlock** command is issued or until another change of state is directed (either via operator override or scheduled action).
-  — Click this button to reset the door to its default configuration values.
-  — Click this button to grant the current user temporary access to the specified door. The door will be momentarily unlocked to permit entry through the door.
-  — Click this button to mask the Door Held Open Alarm for this door.
-  — Click this button to unmask the Door Held Open Alarm for this door.
-  — Click this button to mask the Forced Held Open Alarm for this door.
-  — Click this button to unmask the Door Forced Open Alarm for this door.

Deleting Doors

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.
Card & 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.
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	This indicates that this door possesses a reader/keypad on both sides, entry and exit, and that this side is the master. 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.
Paired Slave	This indicates that this door possesses a reader/keypad on both sides, entry and exit, and that this side is the slave. If you select this option, the Paired Door option is automatically displayed for you to specify the other reader that is installed on the door.
Elev no feedback	This door is an elevator with no feedback input.
Elev feedback	This door is an elevator with a feedback input.

Anti-Passback

The anti-passback (APB) feature 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.

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.

Tip: For HID 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	Allows you to configure APB with just one reader. The door keeps track of each badge to enter and does not allow the same badge to enter twice in a row unless the APB time limit is reached. 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.
Token-Based Timed APB	Tracks each door a badge has accessed. Once 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. 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.
Hard Door APB	Tracks each badge that enters a door and does not allow the same badge to enter twice in a row. This badge will not be able to enter through the same door until it has accessed a second door. NOTE: This mode is only available if using HID hardware.
Soft Door APB	Tracks each badge that enters a door and generates a warning transaction if the same badge is used at the same door twice in a row. This badge is still able to enter the door the second time, but the access is logged as an APB violation. NOTE: This mode is only available if using HID hardware.
Hard Area APB	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. Make sure you configure the area entering and area leaving setting for the specified door.

Mode	Description
Soft Area APB	Tracks each badge that enters a specific area and defines which areas the badge may access next. The badge is allowed to access the area, but the access is logged as an APB violation. Make sure you configure the area entering and area leaving setting for the specified door.
Timed Area APB	Time based hard area APB. When the time limit expires, the hard area APB becomes a soft area APB. Make sure you configure the area entering and area leaving setting for the specified door.

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 cardreader 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** from the icon task bar.
2. From the Identities listing page, click on the name of the identity.

The Identities Edit screen appears.

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.

Tip: For HID 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	Allows you to configure APB with just one reader. The door keeps track of each badge to enter and does not allow the same badge to enter twice in a row unless the APB time limit is reached. 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.
Token-	Tracks each door a badge has accessed. Once the badge has accessed one door, it must access a

Mode	Description
Based Timed APB	second door or wait until the APB time limit is reached before it may access the first door again. 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.
Hard Door APB	Tracks each badge that enters a door and does not allow the same badge to enter twice in a row. This badge will not be able to enter through the same door until it has accessed a second door. NOTE: This mode is only available if using HID hardware.
Soft Door APB	Tracks each badge that enters a door and generates a warning transaction if the same badge is used at the same door twice in a row. This badge is still able to enter the door the second time, but the access is logged as an APB violation. NOTE: This mode is only available if using HID hardware.
Hard Area APB	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. Make sure you configure the area entering and area leaving setting for the specified door.
Soft Area APB	Tracks each badge that enters a specific area and defines which areas the badge may access next. The badge is allowed to access the area, but the access is logged as an APB violation. Make sure you configure the area entering and area leaving setting for the specified door.
Timed Area APB	Time based hard area APB. When the time limit expires, the hard area APB becomes a soft area APB. Make sure you configure the area entering and area leaving setting for the specified door.

Interlocks

NOTE: Only Mercury Security doors support interlocks.

Interlocks are the 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* below
- *Accessing Interlocks from Subpanel Inputs* on the next page
- *Accessing Interlocks from Subpanel Outputs* on the next page


Accessing Interlocks through Doors

1. From the icon task bar, select **Physical Access**.
2. From the sub-options list, select **Doors**. The Doors Listing page is displayed.
3. Select the Mercury door that you want to interlock. The Door Edit screen is displayed.
4. Click the **Interlocks** tab. The Door Interlocks Listing page is displayed.

Accessing Interlocks from Subpanel Inputs


1. From the icon task bar, select **Physical Access**.
2. From the sub-options list, select **Panels**. The Panels Listing page is displayed.
3. Select the panel you want to interlock. The Panel Status screen is displayed.
4. Click the **Subpanels** tab. The Subpanels listing page is displayed.
5. Click  for the subpanel that is connected to the input you want to interlock. The Inputs Listing page is displayed.
6. Click the **Interlocks** link beside the required input. The Input Interlock Listing page is displayed.

Accessing Interlocks from Subpanel Outputs


1. From the icon task bar, select **Physical Access**.
2. From the sub-options list, select **Panels**. The Panels Listing page is displayed.
3. Select the panel you want to interlock. The Panel Status screen is displayed.
4. Click the **Subpanels** tab. The Subpanels listing page is displayed.
5. Click  for the subpanel that is connected to the output you want to interlock. The Outputs Listing page is displayed.
6. 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 the previous page.
2. On the following Interlock Add page, add the required information.

Notice that as you select options, new fields are displayed to help you further define your requirements.
3. When you're finished, click  to save the new interlock.

Editing Interlocks

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











Doors - Listing Page

The Door Listing Page lists all doors that have been defined in the system.

If you have a long list of doors, you can choose to search for a specific door. For more information, see *Searching for Existing Doors* on page 60

From this page, you can also control the door through the application. For more information, *Controlling Doors* on page 60.



The listed doors details include:

Feature	Description
Name	The name assigned to this door. Click on this name to bring up the Door Parameters page of the door properties sheet for this door.
Installed	 indicates the door is installed and able to communicate with the appliance.  indicates that the door is not fully installed. No communications to the panel will be attempted. Click the icon to change the installation status.
Panel	The name of the panel to which this door is connected. Click on this name to bring up the Configure page of the properties sheet for this panel.
Status	The current status of the device is indicated by the background color. For more information, see <i>Status Colors</i> on page 409. <ul style="list-style-type: none"> •  — Indicates the status of communications between the door and specified panel. •  — Indicates whether this door is locked or not. •  — Indicates the status of the power on the door. •  — Indicates the status of the tamper switch on the door. •  — Indicates the status of the battery backup on the door. •  — Indicates whether this door is currently in a forced state. •  — Indicates whether this door is currently in a held open state.
Door Mode	Indicates the door mode — the method by which the door is opened.
Delete	Click  to delete an existing door.
Add New Door	Click this button to define a new door. As you can see, there is also an add button at the bottom of this page.
Create New Report	Click this button to generate a standard report on the doors in this list.

Doors - Add Page

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

Feature	Description
Name	Enter a name for the door. Duplicate names are not allowed.
Partitions	Select one or more partitions.

Feature	Description
	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Alt. Name	If required, enter an alternate name for the door.
Location	Enter a short description of the door location.
Appliance	Select the appliance that the door is connected to.
Vendor	Select the type of panel this door is connected to. The page refreshes to display new options.
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.



Doors - HID™ 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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Panel	Specify 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	Specify the subpanel that is connected to the door. This option is only displayed if there is a subpanel connected to the specified panel.

Feature	Description
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 specified subpanel.</p>
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	<p>Select the entry mode for the door when the door controller is online and communicating with the panel.</p>
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 Mode option is Facility code only.</p>
Custom Mode	<p>Select any additional door mode the door must support outside the Door Mode and Offline Mode options.</p>
Custom Schedule	<p>Define when the Custom Mode would be active.</p> <p>Select a schedule from the drop down list.</p> <p>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.</p> <p>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.</p> <p>Only schedules that have been defined in the system are listed.</p>
Always Mask Forced	<p>Check this box to mask all Forced Door events.</p>
Always Mask Held	<p>Check this box to mask all Door Held Open events.</p>
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>



Feature	Description
Deny Duress	If a user indicates duress at a door, checking this box denies access.
Don't Pulse Door Strike on REX	Check this box to disable the pulse of the door strike when request-to-exit button is activated.
Detailed Events	Check this box to generate detailed events of all hardware at the door including door position masking, timer expiration and output status. This feature is useful for circumstances where it is important to know all the details of an event.
Enable Cipher Mode	Check this box to enable cipher mode. 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: Some of the listed fields may not be displayed if it is not supported by the door module.

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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
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.

Feature	Description
	This option is only displayed if there is a subpanel connected to the selected main panel.
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>
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 Mode option is Facility code only.</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 5 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 5 seconds) on the exterior may also be used to change status. Not to be used on mortise deadbolt.
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.</p> <p>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.</p>

Feature	Description
	Only schedules that have been defined in the system are listed.
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.</p> <p>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>
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 generate detailed events of all hardware at the door including door position masking, timer expirations and output status.</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.

Feature	Description
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.

- *Doors - HID VertX® Edit Screen* below
- *Doors - Mercury Security Edit Screen* on page 88

Doors - HID VertX® Edit Screen

When you specify **HID** as the vendor for a door, the door options change to show what is supported by that manufacturer.



The page options that are available to HID doors include:

Doors - HID™ Parameters Page

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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Panel	Specify the panel the door is assigned to. After you make your selection, new options may be displayed to define how the door is

Feature	Description
	connected to the panel.
Subpanel	Specify the subpanel that is connected to the door. This option is only displayed if there is a subpanel connected to the specified 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 specified subpanel.
Access Type	Select the Access Type for the door. 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.
Door Mode	Select the entry mode for the door when the door controller is online and communicating with the panel.
Offline Door Mode	Select the entry mode used for the door if the door controller is no longer communicating with the panel. 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 Mode option is Facility code only .
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. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Mask Forced Schedule	Define when Door Forced Open alarms from this door will be masked. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Mask Held Schedule	Define when Door Held Open alarms from this door will be masked. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Always Mask Forced	Check this box to mask all Forced Door events.
Always Mask Held	Check this box to mask all Door Held Open events.
Door Processing Attributes	
Door use Tracking	Select one of the listed options to define the level of door event tracking that is logged in the Monitor screen. <ul style="list-style-type: none"> • None: only standard door events are logged • Used: includes the details of when the door is used



Feature	Description
	<ul style="list-style-type: none"> • 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.

Doors - HID™ Operations Page

When you click the **Operations** tab on the Door Edit screen, the HID 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>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</p>

Feature	Description
	<p>partition, anyone with access to the system can edit the item.</p> <p>Only the partitions that have been defined in the system appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</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 63.</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.
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	Specifies the number of seconds before the held open door event is generated.

Feature	Description
time	Enter the number of seconds.
Extended Access	Specifies the strike time for a door configured for persons that require more time to enter. For example, persons with physical disabilities may require more time to enter through a door. Enter the number of seconds.
Extended Held Open Time	Specifies the amount of time before the held open door event is generated for tokens marked with extended access. Enter the number of seconds.
Card Formats	Specifies the card formats that are compatible with the reader at the door. Check the box beside the card formats that apply.
Simple Macros	
Type	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: <ul style="list-style-type: none"> • Forced • Held
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	Click Save Macro to save the settings for this canned macro. If this is a new macro, a new row is automatically added below. Click Remove Macro to delete a macro. This button only appears if the macro has been saved in the system. For more information, see <i>Adding Simple Macros</i> on page 58.
	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.


Doors - HID™ Hardware Page



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>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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</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>
	<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.
	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	Click this button to generate a PDF report on the current door policy.


Feature	Description
Policy	



Doors - HID™ Subpanel Reader Edit Page

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	From the drop down option list, select the keypad decode/encryption method you want to use for this reader. Choose from these options: <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.
NCI magstripe	Check this box to indicate that this reader supports the NCI magstripe standard.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	Click this button to save your changes.
	Click this button to discard your changes.


Doors - HID™ Subpanel Input Edit Page

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.
Debounce ¹	From the drop down list, select the number of units this input should be allowed to debounce. The units are listed in milliseconds (ms).
Cameras	Select the camera from the window that this input activates if it goes into alarm. Only the cameras that have been added to the system are listed.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	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" software is designed to anticipate it. This is known as "debouncing a switch".

Doors - HID™ Subpanel Output Edit Page

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: HID 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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	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.

Doors - HID™ Cameras Page

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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.

Feature	Description
Panel	Specifies the panel the door is assigned to. This is a display only field when editing the hardware (the panel can be changed when editing the door operations).
Subpanel	Specifies the subpanel that is connected to the door. Only subpanels that are connected to the panel are listed.
Lock Number	Specifies the number ID for the set of inputs/ outputs that are connected from the subpanel to the door.
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 102.
Available	The 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.
Show Policy	Click this link to view a PDF report indicating the current policy associated with this door.

Doors - HID™ Events Page

When you click the **Events** tab from the Door Edit screen, the HID Events page 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 HID™ 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.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge.

¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
	If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

Doors - HID™ Access Page

When you click the **Access** tab on the Door Edit screen, the HID Access page is displayed. This page provides a list of the access groups, roles and identities that have permission to edit or use this door.

Feature	Description
Access Group	The name of this access group. Click this link to edit the access group.
Roles	Lists the roles this access group is a member of. Click the + or - symbol beside each role to show or hide the identities that are in the access group through the role.
Identities	Lists the users who are members of the access group.

Doors - HID™ Transactions Page

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.

Feature	Description
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 - Mercury Security Edit Screen

When you specify **Mercury Security** as the vendor for a door, the door options change to show what is supported by that manufacturer.

The page options that are available to Mercury Security doors include:


Doors - Mercury Security Parameters Page


When you click the **Parameters** tab on the Door Edit screen, the Mercury Parameters page is displayed. This page allows you to define the door connections, door mode, schedule and processing attributes.

NOTE: Some of the listed fields may not be displayed if it is not supported by the door module.

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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
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.
Access Type	Select the Access Type from the drop down list.

Feature	Description
	<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 Mode option is Facility code only.</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 5 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 5 seconds) on the exterior may also be used to change status. Not to be used on mortise deadbolt.
Custom Mode	<p>Select any additional door mode the door must support outside the Door Mode and Offline Mode options.</p>
Custom Schedule	<p>Define when the Custom Mode would be active.</p> <p>Select a schedule from the drop down list.</p> <p>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.</p> <p>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.</p> <p>Only schedules that have been defined in the system are listed.</p>
Always	<p>Check this box to specify that Door Forced Open alarms at this door are always masked.</p>

Feature	Description
Mask Forced	Normally, this box is unchecked.
Always Mask Held	Check this box to specify that Door Held Open alarms at this door are always masked. Normally, this box is unchecked.
Door Processing Attributes	
Log Grants Right Away	When this box is checked, the system logs an extra event as soon as there is a grant (that is, before entry / no entry is determined). This event is not turned into a Access Control Manager event. Check this box in order to initiate local I/O in the panel using the panel triggers. Certain customers may have a trigger they want to fire (to execute a macro) as soon as there is a grant but before entry / no entry is determined.
Deny Duress	Check this box to deny access to a user that indicates duress at a door.
Don't Pulse Door Strike on REX	Check this box to disable the pulse of the door strike output when the request-to-exit button is pressed and can be used for a 'quiet' exit. If this box is not checked, the output is pulsed.
Require Two Card Control	Check this box to specify that two tokens are required to open this door. This enforces two-person rule at a specified door.
Door Forced Filter	Check this box to enable the filter feature for door forced alarms. There are instances when a door is either slow to close or is slammed shut and bounces open for a few seconds. With this filter, the monitor allows three seconds for a door to close before issuing an alarm.
Log All Access as Used	Check this box to log all access grant transactions as if the person used the door. If this box is not checked, the door determines if it was opened and will distinguish if the door was used or not used for grant.
Detailed Events	Check this box to generate detailed events of all hardware at the door including door position masking, timer expirations and output status. 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.

Feature	Description
	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.



Mercury Security Operations Page

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

NOTE: Some of the listed fields may not be displayed if it is not supported by the door module.

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>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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</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	Select the Anti-Passback (APB) mode for the door.

Feature	Description
	For more information on Anti-Passback modes, see <i>Anti-Passback Modes</i> on page 63.
APB Delay	Enter the number of seconds before another APB entry is allowed.
Into Area	Select the area that the user enters by passing through the door. Only the areas that have been previously configured in the system appear in this list.
Out of Area	Select the area that the user exits by passing through the door. Only the areas that have been previously configured in the system appear in this list.
PIN Timeout	Enter the number of seconds that is allowed for a user to enter a PIN before it times out.
PIN Attempts	Enter the number of times a user can attempt to enter a PIN before an Invalid PIN event is generated.
Strike Mode	Select the strike mode. <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	Select the LED mode to specify how the reader LEDs are displayed. For more information on LED modes, see <i>LED Modes</i> on page 1.
Held Pre-Alarm	Enter the number of seconds a door can be held open before a pre-alarm is issued. Instead of generating an alarm, it sends a warning signal to the Access Control Manager host.
Access time when open	Enter the number of seconds the door remains unlocked after a card has been swiped.
Standard Access time	Enter the number of seconds the door remains unlocked after access has been granted. If the door is not opened within this time, it will automatically lock.
Held Open Time	Enter the number of seconds the door can be held open before a Door Held Open event is generated.
Extended Access	Enter the number of seconds the door remains unlocked after access has been granted to token holders with extended access permissions. This feature is useful for users that may require more time to enter a door, such as individuals with physical disabilities.
Extended Held Open Time	Enter the number of seconds the door can be held open for users with extended access permissions. This feature is useful for users that may require more time to enter a door, such as individuals with physical disabilities.
Card Formats	Select the card formats that are compatible with the reader at the door.
Simple Macros	
Type	Select a default macro that is triggered when the following conditions are met for this door. Currently available macros include: <ul style="list-style-type: none"> • Forced






Feature	Description
	<ul style="list-style-type: none"> • Held • Pre-Alarm
Schedule	<p>Define when this macro can be triggered.</p> <p>Select a schedule from the drop down list.</p> <p>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 58.</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 button to generate a PDF report on the current door policy.

Doors - Mercury Security Hardware Page

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: Some of the listed fields may not be displayed if it is not supported by the door module.



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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</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	<p>The number that has been assigned to the door module by the wireless lock configuration device.</p>
Unassign All	<p>Click this button to reset all of the values below and start over.</p>
	<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.


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>

Feature	Description
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.


Doors - Subpanel Reader Edit Page



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.
Type	Select the type of reader this is.
Address	The address of this reader.
Keypad decode	Select the keypad decode/encryption method that is used by this reader. The options include: <ul style="list-style-type: none"> • MR20 8-bit tamper • Hughes ID 4-bit • Indala • MR20 8-bit no tamper
LED drive	Select the LED driver for this reader. The options include: <ul style="list-style-type: none"> • None • Gen 1 wire • Reserved • Sep Red/Grn no buzz • Dorado 780 • LCD MR50T • OSDP
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.
NCI magstripe	Check this box to indicate that this reader supports the NCI magstripe standard.
Supervised	Check this box to indicate that this reader is supervised (outfitted with detection devices)
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.
Inputs on reader	Check this box to indicate that this reader provides one or more input ports for serial input arrays.

Feature	Description
Partitions	<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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</p>
	Click this button to save your changes.
	Click this button to discard your changes.


Doors - Subpanel Input Edit Page



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.
EOL resistance	Select the End of Line resistance of this input. Only the EOL resistance that have been defined in the system are listed.
Debounce 1	From the drop down list, select the number of units this input should be allowed to debounce. Each unit is approximately 16 ms.
Hold time	Set the amount of time that the alarm will stay in alarm after returning to normal. 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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	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" software is designed to anticipate it. This is known as "debouncing a switch".

Doors - Subpanel Output Edit Page

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.

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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	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.

Doors - Mercury Security Elev Page



When you click the **Elev** tab at the Door Edit screen, the Mercury Elev page 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 Door Edit Parameters page.
Inputs	List of inputs for the related elevator input module.
Outputs	List of outputs for the related elevator output module.

Doors - Mercury Security Cameras Page

When you click the **Cameras** tab on the Door Edit screen, the Mercury Camera page is displayed. From this page, you can assign specific cameras to record video of the selected door.

NOTE: Some of the listed fields may not be displayed if it is not supported by the door module.

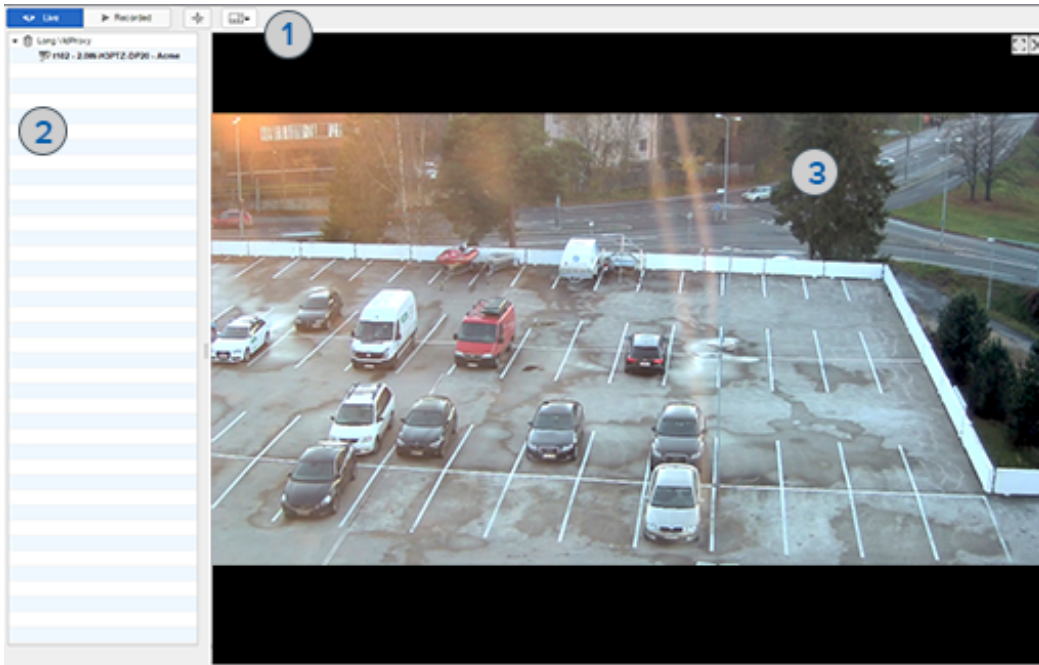
Feature	Description
Name	The name of the door.
Alt Name	The alternative name of the door.
Location	The location of the door.
Appliance	The appliance the door is connected to.
Vendor	The name of the door manufacturer.
Installed	Check this box to indicate the appliance can communicate with the connected device.
Partitions	<p>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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</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 102.</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	<p>The window displays a list of cameras that are currently connected to the door.</p> <p>To disconnect a camera from the door, select the camera from the Members list, then click  to move it to the Available list.</p>
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>

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 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	This area includes all the features that you would need to view and control the related camera video. Options typically include switching from live to recorded video, PTZ controls for PTZ cameras, and changing the video display layout.
2	Camera List	This area lists all the cameras that are linked to the event. Click the name of a camera to display the video. Use one of the multi-video layouts to display more than one camera at a time.
3	Image Panel	This area displays the video stream from the connected cameras. In the top-right corner, you can minimize and maximize the display or close the video.


Doors - Mercury Security Interlocks Page

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
Interlocks	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 New Interlock	Click this button to add a new interlock to the system.

Interlocks - Add Page

When you click **Add New 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.

Interlocks - Door 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.

Doors - Mercury Security Events Page

When you click the **Events** tab from the Mercury edit screen, the Mercury Events page 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

Feature	Description
	specific device.

Doors - Creating Local Events for Mercury 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.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge.

¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
	If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

Doors - Mercury Security Access Page

When you click the **Access** tab on the Mercury Edit Screen, the Mercury Access page is displayed. This page provides a list of the access groups, roles and identities that have permission to edit or use this door.

Feature	Description
Access Group	The name of this access group. Click this link to edit the access group.
Roles	Lists the roles this access group is a member of. Click the + or - symbol beside each role to show or hide the identities that are in the access group through the role.
Identities	Lists the users who are members of the access group.

Doors - Mercury Security Transactions Page

When you click the **Transactions** tab on the Door Edit screen, the Mercury 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.

Feature	Description
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 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.

Searching for Panels


If you have many panels in your system, you can choose to search for the panel you want to see or edit.

1. From the Panels Listing page, enter a panel name in the **Criteria** field.
You can enter any letters or numbers that may be in the panel name. If you can't remember the panel's full name, you can use wildcard characters. For more information, see *Wildcard Characters* on page 419.
2. If you have more than one appliance in your system, select the appliance the panel is connected to in the **Appliance** drop down list.
3. From the **Installed** drop down list, you can select Yes or No to indicate if the panel is installed and able to communicate with the appliance.
4. Click **Search**.

The Panel Listing page filters the panels and displays the ones that meet your search criteria.

Adding Panels

To add a panel to the system:



1. From the icon task bar, select **Physical Access > Panels**.
2. Click **Add New Panel**. The Panel Add page is displayed.
3. Complete the **Vendor** and **Model** fields. Depending on the selected Vendor and Model, different options are displayed.
4. When you're finished, click  to save your changes.

The Properties screen for this specific panel expands to display the complete list of available properties.

Depending on the vendor and model that was selected, a specific set of tab options are displayed.



Adding HID VertX® Panels

If you selected HID 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 Add 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.
NOTE: If you are adding PIM400 subpanels for wireless locks, you cannot add any other subpanel models to the same panel. If you have already physically wired a PIM400 subpanel and another model of subpanel to the same controller panel, you will need to disconnect one of the subpanels.
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 HID 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

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. On the Panels Listing page, select the panel you want to reset.
2. 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 Firmware

Panel firmware is 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 a new firmware update provided by the panel manufacturer, click **Add New Firmware**.
 - a. On the following Firmware Upload Page, click **Choose File** then locate the firmware file.
 - b. 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.
 - c. 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.

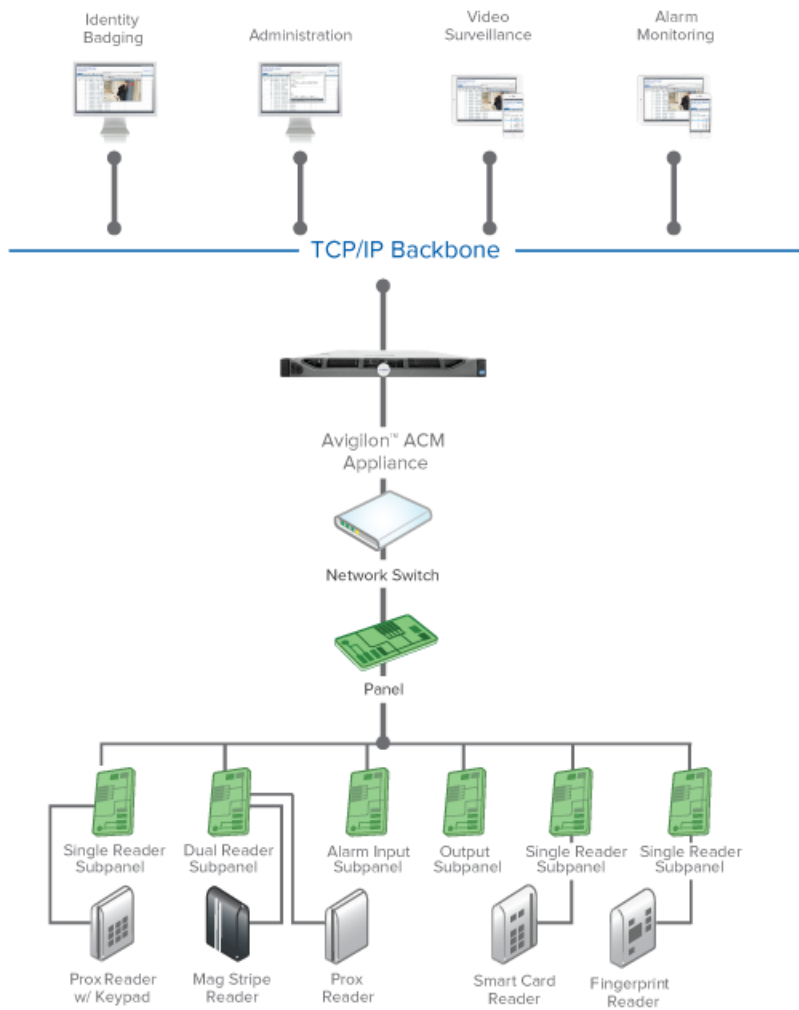
Deleting Panels

1. From the Panels Listing page, click  for the panel you want to remove.
2. When the confirmation message appears, click **OK**.

Subpanels

Some panels support hierarchical connections. These panels can be connected in a master-slave relationship where one panel is the master and all the panels connected to it are slaves. These slave panels, or subpanels, transmit their data to the Access Control Manager appliance through the master panel.

One master panel can be connected to a large number of specialized subpanels.




Adding Subpanels

Subpanels are typically batch added when a panel is first added to the system. For more information, see [Adding Panels](#) on page 111.





If a new subpanel is installed later, you can add the subpanel to the panel on the Panel screen.

NOTE: If you are adding PIM400 subpanels for wireless locks, you cannot add any other subpanel models to the same panel. If you have already physically wired a PIM400 subpanel and another model of subpanel to the same controller panel, you will need to disconnect one of the subpanels.

1. From the icon task bar, 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. From the icon task bar, 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.

Deleting Subpanels

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

1. From the icon task bar of the home page, 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, un.masks 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 58.


Adding Macros

1. From the icon task bar of the home page, 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* on the next page.

To create quick macros that are specific to a particular door (simple macros), see *Adding Simple Macros* on page 58

Editing Macros

1. From the icon task bar of the home page, 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. From the icon task bar of the home page, 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 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 facing 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 58 and *Mercury Security Operations Page* on page 91

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. From the icon task bar of the home page, 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. From the icon task bar of the home page, 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. From the icon task bar of the home page, 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**.

Panels - Listing Page

When you select **Panels** from the **Physical Access** sub-options task bar, the **Panels Listing** page is displayed.

This page lists all the panels that have been added to the system and displays the following information about each panel.

If you have a long list of panels, you can use the search feature to find the panel you need to edit. For more information, see *Searching for Panels* on page 111.

Feature	Description
Name	The name of the panel. Click the name to edit the panel details.
Installed	 indicates the panel is installed and able to communicate with the appliance.  indicates that the panel is not installed. No communications to the panel will be attempted. Click the icon to change the panel's installed status.
Appliance	Identifies the appliance that is currently responsible for all communications to the panel. If appliance redundancy has been set up, the secondary stand-by appliance will replace the primary appliance if it fails.
Vendor	Identifies the panel manufacturer.
Status	The current status of the device is indicated by the background color. For more information, see <i>Status Colors</i> on page 409. <ul style="list-style-type: none"> •  — Indicates the communications status of the panel. •  — Indicates the power status of the panel. •  — Indicates the tamper alarm status of the panel. •  — Indicates the low battery alarm status of the panel (if available).
Delete	Click  to delete the panel from the system.
Add New Panel	Click this button to add a new panel to the list.

Panels - Panel Add Page

When you click the **Add New Panel** button from the Panel Listing page, the Panel Add page is displayed.



Enter the details of the new panels. After you select the vendor, more options are displayed.

Feature	Description
Name	Enter a name for this panel. It is recommended that you enter a name that will help you identify the devices it controls. Duplicate names are not allowed.
Physical Location	Enter where this panel is installed.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Appliance	From the drop down list, select the appliance this panel is connected to. Only appliances that have been defined for this system are listed.
Vendor	From the drop down list, select the name of the panel manufacturer. Once a vendor is selected from the drop down list, the Panel Add page will display new fields that are specific to the panel manufacturer: <ul style="list-style-type: none"> • <i>HID</i> below • <i>Mercury Security</i> below
Installed	Check this box if this panel is already installed and ready to communicate with the appliance.

HID



If you specify **HID** as the vendor, the screen displays the following new fields:

Feature	Description
Model	Select the model of this panel from the drop down list.
Timezone	Select the panel's local time zone. The time zone is used to set the local time in the panel for correct operation of door schedules and for associated local time-based decision making.
	Click this button to save your changes.
	Click this button to discard your changes.

Mercury Security



If you specify **Mercury Security** as the vendor, the screen displays the following new fields:

Feature	Description
Model	Select the specific panel model from the drop down list. Tip: Lenel panels are can be configured as Mercury panels. For more information, see <i>Lenel™ Panel Support</i> on page 114.
Timezone	Select the panel's local time zone. The time zone is used to set the local time in the panel for correct operation of door schedules and for associated local time based decision making.
Wiring Type (SCP models only)	From the drop down list, select the type of port this panel uses to connect to door or subpanels. The possibilities are: <ul style="list-style-type: none"> • (4) 2-Wire Ports • (2) 4-Wire Ports

Feature	Description
	<ul style="list-style-type: none"> • (1) 4-Wire/(2) 2-Wire <p>NOTE: The options that appear depend on the type of SCP panel you specify.</p>
Total Memory (SCP models only)	Select the total memory this panel contains.
Max Elevator Floors (SCP models only)	Select the number of floors this panel oversees. There is a maximum of 128 floors that can be stipulated. For more information on defining elevator door access, see Elevator Access Levels - Adding.
Allocate space for:	
Credentials	Enter the number of credentials that can be in the panel. This amount is dependent on the amount of memory, vendor and model of the panel.
Events	Enter the number of transactions to buffer in the panel. This quantity is dependent on the amount of memory, vendor and model of the panel.
DB Version	The current version of the database.
	Click this button to save your changes.
	Click this button to discard your changes.

Panels - Batch Add HID Subpanels Page



This page only appears if you are adding a new panel. After you save the initial panel details, the following page allows you to batch add all the subpanels that may be connected to the controller panel.

Feature	Description
Port #	The port on the panel that the subpanel is connected to.
Model	The supported subpanel models.
Quantity	Select the number of each subpanel that is installed at each port.
	Click this button to save your changes.
	Click this button to discard your changes.

Panels - Batch Add Mercury Subpanels Page

This page only appears if you are adding a new panel. After you save the initial panel details, the following page appears so that you can batch add all the subpanels that may be connected to the controller panel.

NOTE: If you are adding PIM400 subpanels for wireless locks, you cannot add any other subpanel models to the same panel. If you have already physically wired a PIM400 subpanel and another model of subpanel to the same controller panel, you will need to disconnect one of the subpanels.

Feature	Description
Model	The supported subpanel models.
Quantity	Select the number of each subpanel that is installed at each port.
	Click this button to save your changes.
	Click this button to discard your changes.





HID VertX® Panel Pages





Click a link below to view details of HID VertX panel pages.

Panels - HID VertX® Status Page

When you select an HID panel from the Panel Listing page, the Status page of the panel Edit screen is displayed. Return to this page by selecting the Status tab.

The current status of the device is indicated by the background color. For more information, see *Status Colors* on page 409.

Feature	Description
Panel Status	
	Indicates communication status between this panel and the appliance.
	Indicates power status to this panel.
	Indicates status of the tamper switch on this panel.
	Indicates the status of the backup battery for this panel.
Download	
Parameters	Click this button to download the panel's configuration, event and access parameters to the panel.
Tokens	Click this button to download tokens to the panel.
Reset/Download	Click this button to reset and download current data to the panel's connected doors.
APB Reset	Click this button to reset the anti-passback configuration for this panel.
Status	
Command	Indicates the number of commands downloaded to this panel.
Current	Indicates the number of items currently being downloaded.

Feature	Description
Queued	Indicates the number of items still in the queue to be downloaded.
Tags	Indicates the number of tags being downloaded.
Tokens	Indicates the number of tokens being downloaded.
Firmware	Click this button to update the panel firmware.
Last comms	Indicates the date and time of the last message communicated between the panel and the appliance.
Memory	Indicates the amount of memory in MB this panel currently possesses.
Available	Indicates the amount of memory, in MB, that is available for storing parameters and tokens.
Cards in use	Indicates the number of cards currently in use on this panel.
Subpanel Matrix	
Subpanel	The name of the connected subpanel. Click the name to see the status of all the devices that are connected to the subpanel.
	Indicates the communications status between the panel and the subpanel.
	Indicates the power status to the subpanel.
	Indicates the tamper switch status on the subpanel.
	Indicates the backup battery status for the subpanel.

Subpanels - HID VertX® Status Listing Page

When you click on one of the available subpanels from the panel Status page, the Subpanel Status Listing page is displayed.

This page lists all inputs, outputs and readers that are supported by the selected subpanel.

The current status of the device is indicated by the background color. For more information, see *Status Colors* on page 409.



Feature	Description
Subpanel Details	
Name	The name of the subpanel. Click this name to edit the subpanel.
Comms	Indicates the current status of communication between this subpanel and the appliance.
Power	Indicates the current source and status of power to the subpanel.
Tamper	Indicates the current status of the tamper switch on the subpanel .
Battery	Indicates the current status of the subpanel battery.
Message	Displays information related to alarms or events that affect the subpanel.
Model	Indicates the model of this subpanel.

Feature	Description
Firmware	Click this button to update the subpanel firmware.
Subpanel Matrix	
Inputs	The name of the input. Click the name to edit the input.
Actions	Click the Mask button to mask the input.
	Click the Unmask button to unmask input.
Outputs	The name of the output. Click the name to edit the output.
Actions	Click the On button to activate the output.
	Click the Off button to deactivate the output.
	Click the Pulse button to pulse the output.
Readers	Click one of the listed readers to edit its details.

Panels - HID™ Firmware Listing Page

When you click the **Firmware** button on the Panel Status page, the Firmware Listing page is displayed.



Only the files that have been added to the system are listed.

Feature	Description
Name	The name of the firmware file.
Size	The total size of the firmware file in bytes.
Upload Date	The date and time when the firmware file was uploaded to the appliance.
Apply	Click  to apply this firmware update to the panel.
Delete	Click  to delete this firmware file from the appliance.
Add New Firmware	Click this button to add a new firmware file to the list.

Panels - HID™ Firmware Upload Page



When you click **Add New Firmware** from the Firmware Listing page, the Firmware Upload page is displayed.

This page allows you to select and upload the latest panel firmware file.

Feature	Description
Upload Firmware file	Click Choose File to locate the firmware update file.
	Click this button to upload the file to the appliance.
	Click this button to discard your changes.

Panels - HID VertX® Configure Page



When you click the **Configure** tab from the Panel Edit screen, the Panel Configure page is displayed. This page allows you to define the panel's identity in the system.

Feature	Description
Name	The name of the panel.
Physical Location	A description of where the panel is installed.
Appliance	This read-only field indicates the appliance that is connected to the panel.
Vendor	The read-only field displays HID .
Installed	Check this box to indicate that the panel is installed and can communicate with the appliance.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Model	The read-only field displays the panel model.
Timezone	Select the panel's local time zone from the drop down list.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Panel	Click this button to add a new panel.
Show Policy	Click this button to download a PDF report of the policies that are currently configured for the panel.

Panels - HID VertX® Host Page






When you click the **Host** tab from the Panel Edit screen, the Panel Host page is displayed. This page allows you to define the panel's IP address and port number.


Feature	Description
Name	The name of the panel.
Physical Location	Where the panel is located.
Appliance	This read-only field indicates the appliance that is connected to the panel.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.

Feature	Description
Installed	Check this box to indicate that the panel is installed and can communicate with the appliance.
IP Address	Enter the IP address of this panel.
Port	Enter the port number used by this panel.
Offline Timeout	From the list, select the number of milliseconds this panel can remain offline (disconnected from the host) before the panel attempts to contact an alternative host, if one exists.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Panel	Click this button to add a new panel.
Show Policy	Click this button to download a PDF of the panel's current policy.

Panels - HID VertX® Subpanels Page



When you click the **Subpanels** tab from the Panel Edit screen, the Subpanels Listing page is displayed. This page lists all the subpanels that have been added to the system and displays the following details about each subpanel:

Feature	Description
Name	The name of the subpanel. Click the name to edit the subpanel.
Type	This read-only column indicates the type of subpanel this is.
Port	This read-only column indicates the port that this subpanel is currently connected to on the master panel.
Address	This read-only column indicates the RS45 address of this subpanel.
Installed	 indicates the subpanel is installed and able to communicate with the appliance.  indicates that the subpanel is not installed. No communications to the subpanel will be attempted. Click the icon to change the installed status.
	Click this icon to display the subpanel inputs listing page. This displays the input points available on the subpanel. For more information, see <i>Editing Subpanels</i> on page 117 and <i>Inputs</i> on page 56.
	Click this icon to display the subpanel outputs page. This displays the output points available on the subpanel. For more information, see <i>Editing Subpanels</i> on page 117 and <i>.Outputs</i> on page 55.
	Click this icon to display the subpanel readers page for the specified subpanel. This displays the readers available with this module.

Feature	Description
	For more information, see <i>Editing Subpanels</i> on page 117.
	Click this icon to delete the subpanel from the list.
Add New Subpanel	Click this button to add another subpanel to this panel. The Subpanel Add page appears.



Subpanels - HID™ Subpanel Add Page

When you click **Add New Subpanel** from the Subpanels Listing page, the Subpanels Listing page is displayed. This page allows you to define new subpanels for the system.


Feature	Description
Name	Enter a name for this new subpanel.
Physical Location	Enter a brief description where this subpanel is located.
Model	Select the model of this new subpanel.
Port	Select the port that this subpanel is connected to on the main panel.
Address	After you select the subpanel model, the Address field appears. Select the RS45 address for the selected port.
Installed	Check this box to indicate that the subpanel is installed and able to communicate with the main panel.
	Click this button to save your changes.
	Click this button to discard your changes.





Subpanels - HID™ Subpanel Edit Page

When you click the name of a subpanel from the Subpanels Listing page, the Subpanel Edit page is displayed. This page allows you to define the identity of the panel and where it is connected to the master panel.

Feature	Description
Name	The name of this subpanel.
Physical Location	A brief description of where this subpanel is located.
Model	The read-only field displays the subpanel descriptor or model number.
Port	Select the port that this subpanel is connected to on the master panel.
Address	Select the RS45 address for the selected port.
Installed	Make sure this check box is selected to indicate that the subpanel is installed and able to communicate with the master panel.
	Click this button to save your changes.
	Click this button to discard your changes.

Subpanels - HID™ Input Listing Page

If you click  from the Subpanels Listing page, the Input Listing page is displayed. This page lists all the input points that are available on the subpanel, and displays the following details about each input:



Feature	Description
Inputs	The name of the input. The default name of the input is the input's location on the subpanel. Click the name to edit the input.
Address	The read-only address of this input point on the subpanel.
Masked	The current masking status for this input. <ul style="list-style-type: none">  indicates the point is masked.  indicates the point is not masked. Click the icon to change the masking status.
Installed	The current input connection status. <ul style="list-style-type: none">  indicates the input is installed and able to communicate with the appliance.  indicates that the input is not installed. No communications to the subpanel will be attempted. Click the icon to change the installed status.

Subpanels - HID™ Input Edit Page


When you click the name of an input from the Inputs Listing page, the Input Edit page is displayed. This page allows you to define the details of the input.



Feature	Description
Input	The name of the input. The default name of the input is the input's location on the subpanel.
Installed	Check to indicate that this point is connected and active.
Address	The read-only address of this input 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. Each unit is approximately 16 ms.
Masked	Check this box to indicate that this input is normally masked.
Cameras	Select the camera from the window that this input activates if it goes into alarm.

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" software is designed to anticipate it. This is known as "debouncing a switch".

Feature	Description
	Only those cameras previously defined for this system appear in this window.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Canned Macros	
Type	Select a type of macro. Only the macros supported by the input point are listed.
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Operation Type	The read-only summary of the macro operation type.
Output	Select the output that is triggered when the macro is activated.
Save Macro	Click this button to save the canned macro settings. You can create more than one canned macro per input. For more information, see <i>Adding Simple Macros</i> on page 58.
	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.



Subpanels - HID™ Outputs Listing Page

When you click  from the Subpanels Listing page, the Outputs Listing page is displayed. This page lists all the output points that are available on the subpanel, and displays the following details about each output:


Feature	Description
Outputs	The name of the output. The default name of the output is the output's location on the subpanel. Click the name to edit the output.
Address	The read-only address of this output point on the subpanel.
Installed	The current output connection status. <ul style="list-style-type: none">  indicates the output is installed and able to communicate with the appliance.  indicates that the output is not installed. No communications to the subpanel will be attempted. Click the icon to change the installed status.



Subpanels - HID™ Outputs Edit Page

When you click the name of an output from the Outputs Listing page, the Outputs Edit page is displayed. This page allows you to define the details of this output.

Feature	Description
Output	The name of the output point. The default name is the location of the output point on the subpanel.
Installed	Check this box to indicate that this output point is connected and active.
Address	The read-only address for this output point on the subpanel.
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).
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	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.



Subpanels - HID™ Readers Listing Page

When you click  from the Subpanels Listing page, the Readers Listing page is displayed. This page lists all the reader points that are available on the subpanel, and displays the following details about each reader:

Feature	Description
Reader	The name of the reader. The default name of the reader is the reader's location on the subpanel. Click the name to edit the reader.
Alt Name	The alternative name assigned to the reader.
Address	The read-only address of this reader on the subpanel.
Location	The physical location of this reader.
Installed	The current reader connection status. <ul style="list-style-type: none">  indicates the reader is installed and able to communicate with the appliance.  indicates that the reader is not installed. No communications to the reader will be attempted. Click the icon to change the installed status.

Subpanels - HID™ Reader Edit Page

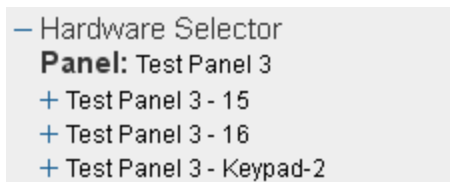
When you click the name of a reader from the Readers Listing page, the Reader Edit page is displayed. This page allows you to define the details of the connected card reader.

Feature	Description
Name	The name of the reader. The default name of the reader is the reader's location on the subpanel.
Alt. name	Enter an alternative name for this reader.
Location	Enter a brief description of where the reader is installed.
Keypad decode	From the drop down option list, select the keypad decode/encryption method you want to use for this reader. Choose from these options: <ul style="list-style-type: none"> • Hughes ID 4-bit • Indala • MR-20 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	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	Click this button to save your changes.
	Click this button to discard your changes.

Panels - HID VertX® Events Page

If you click the **Events** tab from the Panel Edit screen, the Events page is displayed. This page gives you a list of all the global events that are available to each device that is connected to this panel.








- In the top left corner of the page, click the + sign in **+Hardware Selector** to display a list of all the devices that are connected to the panel. For example:



If you click + beside a subpanel, a list of the connected inputs and outputs is displayed. For example:

- Hardware Selector
 - Panel: Test Panel 3**
 - Test Panel 3 - 15
 - o **Input:**
 - Input - subpanel 0 Address 1
 - Input - subpanel 0 Address 2
 - Input - subpanel 0 Address 3
 - Input - subpanel 0 Address 4
 - Input - subpanel 0 Address 5
 - Input - subpanel 0 Address 6
 - Input - subpanel 0 Address 7
 - Input - subpanel 0 Address 8
 - o **Output:**
 - Output on subpanel 0 Address 1
 - Output on subpanel 0 Address 2
 - Output on subpanel 0 Address 3
 - Output on subpanel 0 Address 4
 - + Test Panel 3 - 16
 - + Test Panel 3 - Keypad-2

Click the - sign to hide the list items.

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.

Feature	Description
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.




Panels - Create Local Events for HID™ Panels

When you click the **Create Local** button from the Panel 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 panel.

NOTE: Changes on this page do not affect the global event.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.

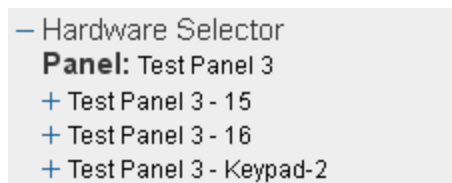
¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

Subpanels - HID VertX® Events Page

If you select a subpanel from the Panel Events page, the page refreshes to display the related subpanel events.








- In the top left corner of the page, click the + sign in **+Hardware Selector** to display a list of all the devices that are connected to the panel. For example:



If you click + beside a subpanel, a list of the connected inputs and outputs is displayed. For example:

- Hardware Selector
 - Panel: Test Panel 3**
 - Test Panel 3 - 15
 - o **Input:**
 - Input - subpanel 0 Address 1
 - Input - subpanel 0 Address 2
 - Input - subpanel 0 Address 3
 - Input - subpanel 0 Address 4
 - Input - subpanel 0 Address 5
 - Input - subpanel 0 Address 6
 - Input - subpanel 0 Address 7
 - Input - subpanel 0 Address 8
 - o **Output:**
 - Output on subpanel 0 Address 1
 - Output on subpanel 0 Address 2
 - Output on subpanel 0 Address 3
 - Output on subpanel 0 Address 4
 - + Test Panel 3 - 16
 - + Test Panel 3 - Keypad-2

Click the - sign to hide the list items.

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.

Feature	Description
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.

Subpanels - Create Local Events for HID™ Subpanels




When you click the **Create Local** button from the Subpanel 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 subpanel.

NOTE: Changes on this page do not affect the global event.

Make any changes as required.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
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 an event type for the RTN event.

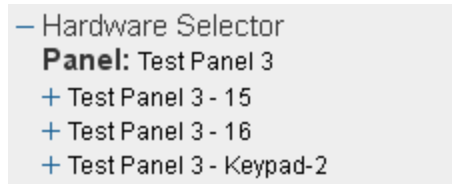
¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

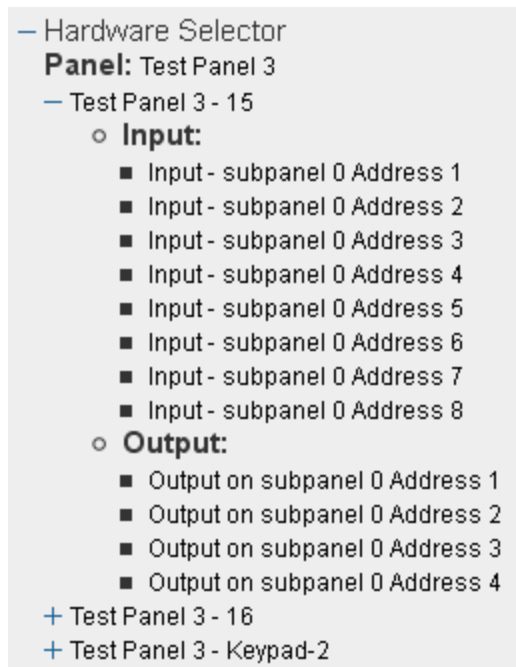
Inputs - HID VertX® Events Page

If you select an input from the Panel Events page, the page refreshes to display the related input events.





- In the top left corner of the page, click the + sign in **+Hardware Selector** to display a list of all the devices that are connected to the panel. For example:






If you click + beside a subpanel, a list of the connected inputs and outputs is displayed. For example:



Click the - sign to hide the list items.

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 ().

Feature	Description
	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.

Inputs - Create Local Events for HID™ Inputs




When you click the **Create Local** button from the Input 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 input.

NOTE: Changes on this page do not affect the global event.

Make any changes as required.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
Alarm Sound	Select an alarm sound that is played when a new alarm occurs while you are monitoring the

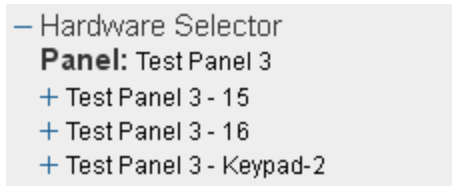
¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
	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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

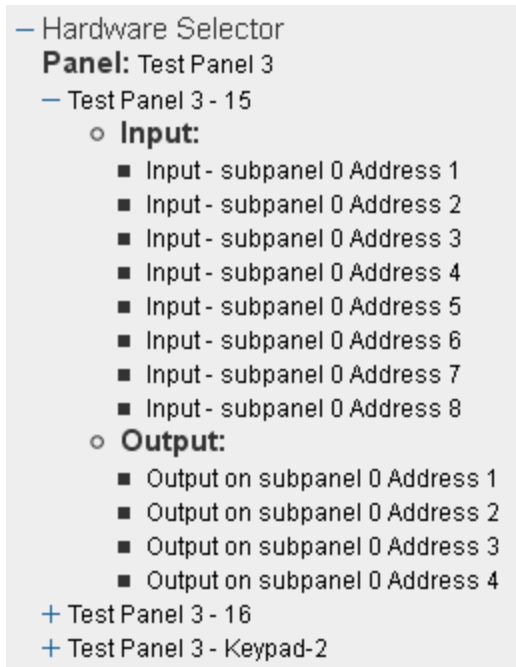
Outputs - HID VertX® Events Page

If you select an output from the Panel Events page, the page refreshes to display the related output events.





- In the top left corner of the page, click the + sign in **+Hardware Selector** to display a list of all the devices that are connected to the panel. For example:






If you click + beside a subpanel, a list of the connected inputs and outputs is displayed. For example:



Click the - sign to hide the list items.

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 ().

Feature	Description
	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.

Outputs - Create Local Events for HID™ Outputs




When you click the **Create Local** button from the Output 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 output.

NOTE: Changes on this page do not affect the global event.

Make any changes as required.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.

¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

Mercury Security Panel Pages




Click a link below to view details of Mercury Security panel pages.

Panels - Mercury Security Status Page

When you select a Mercury panel from the Panel Listing page, the Status page of the panel Edit screen is displayed. Return to this page by selecting the Status tab.

The current status of the device is indicated by the background color. For more information, see *Status Colors* on page 409.

Feature	Description
Panel Status	
	Indicates communication status between this panel and the appliance.
	Indicates power status to this panel.
	Indicates status of the tamper switch on this panel.
	Indicates the status of the backup battery for this panel.
Download	
Parameters	Click this button to download the panel's configuration, event and access parameters to the panel.
Tokens	Click this button to download tokens to the panel.
Reset/Download	Click this button to reset and download current data to the panel's connected doors.
APB Reset	Click this button to reset the anti-passback configuration for this panel.
Status	
Command	Indicates the number of commands downloaded to this panel.
Current	Indicates the number of items currently being downloaded.
Queued	Indicates the number of items still in the queue to be downloaded.
Tags	Indicates the number of tags being downloaded.
Tokens	Indicates the number of tokens being downloaded.
Clock	Click this button to re-sync the panel time.
Firmware	Click this button to update the panel firmware.
Last comms	Indicates the date and time of the last message communicated between the panel and the appliance.
Cycles	Indicates the number of cycles required to update the firmware.
Memory	Indicates the amount of memory in MB this panel currently possesses.
Available	Indicates the amount of memory, in MB, that is available for storing parameters and tokens.
Max Cards	Indicates the maximum number of cards supported by this panel.
In use	Indicates the number of cards currently in use on this panel.

Feature	Description
Subpanel Matrix	
Subpanel	The name of the connected subpanel. Click the name to see the status of all the devices that are connected to the subpanel.
	Indicates the communications status between the panel and the subpanel.
	Indicates the power status to the subpanel.
	Indicates the tamper switch status on the subpanel.

Subpanels - Mercury Security Status Listing Page

When you click on one of the available subpanels from the panel Status page, the Subpanel Status Listing page is displayed.

This page lists all inputs, outputs and readers that are supported by the selected subpanel.



The current status of the device is indicated by the background color. For more information, see *Status Colors* on page 409.

Feature	Description
Subpanel Details	
Name	The name of the subpanel. Click this name to access the Subpanel Edit page.
Comms	Indicates the current status of communication between this subpanel and the appliance.
Power	Indicates the current source and status of power to the subpanel.
Tamper	Indicates the current status of the tamper switch on the subpanel .
Message	Indicates the current status of the subpanel battery.
Model	Displays information related to alarms or events that affect the subpanel.
Firmware	Indicates the model of this subpanel.
Subpanel Matrix	
Inputs	Click one of the listed inputs and the Input Edit page appears.
Actions	Click the Mask button to mask the input.
	Click the Unmask button to unmask input.
Outputs	Click one of the listed outputs and the Output Edit page appears.
Actions	Click the On button to activate the output.
	Click the Off button to deactivate the output.
	Click the Pulse button to pulse the output.
Readers	Click one of the listed readers to edit its details.

Panels - Mercury Firmware Listing Page

When you click the **Firmware** button on the Panel Status page, the Firmware Listing page is displayed.



Only the files that have been added to the system are listed.

Feature	Description
Name	The name of the firmware file.
Size	The total size of the firmware file in bytes.
Upload Date	The date and time when the firmware file was uploaded to the appliance.
Apply	Click  to apply this firmware update to the panel.
Delete	Click  to delete this firmware file from the appliance.
Add New Firmware	Click this button to add a new firmware file to the list.

Panels - Mercury Firmware Upload Page

When you click **Add New Firmware** from the Firmware Listing page, the Firmware Upload page is displayed.



This page allows you to select and upload the latest panel firmware file.

Feature	Description
Upload Firmware file	Click Choose File to locate the firmware update file.
	Click this button to upload the file to the appliance.
	Click this button to discard your changes.

Panels - Mercury Security Configure Page

When you click the **Configure** tab from the Panel Edit screen, the Panel Configure page is displayed. This page allows you to define the panel's identity in the system.



Feature	Description
Name	The name of the panel.
Physical Location	A description of where the panel is installed.
Appliance	This read-only field indicates the appliance that is connected to the panel.
Vendor	The read-only field displays Mercury Security .
Installed	Check this box to indicate that the panel is installed and can communicate with the appliance.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.

Feature	Description
Model	The read-only field displays the panel model.
Time zone	Select the panel's local time zone from the drop down list.
Allocate space for:	
Credentials	Set the number of credentials that can be stored in the panel.
	Enter a number between 0 and 100,000. The default value is 10,000. Credentials and events share storage space on the panel, so setting a higher number of credentials leaves less space for events.
Events	Set the number of events to buffer in the panel.
	Enter a number between 0 and 5,000. The default value is 5,000. Credentials and events share storage space on the panel, so setting a higher number of events leaves less space for credentials.
DB Version	This read-only field displays the Access Control Manager database version used by the panel.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Panel	Click this button to add a new panel.
Show Policy	Click this button to download a PDF report of the policies that are currently configured for the panel.

Panels - Mercury Security Host Page



When you click the **Host** tab from the Panel Edit screen, the Panel Host page is displayed. This page allows you to define the panel's IP address and port number.





Feature	Description
Name	The name of the panel.
Physical Location	Where the panel is located.
Appliance	This read-only field indicates the appliance that is connected to the panel.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Installed	Check this box to indicate that the panel is installed and can communicate with the appliance.
IP Client Connection	Check this box if you want the appliance to locate the panel by its MAC address.
	Once checked, some of the options are no longer required and are replaced by the MAC Address

Feature	Description
	field. Enter the panel's MAC address. The appliance will use this address to communicate with the appliance.
TLS Required	Check this box to indicate that this panel must use Transport Layer Security.
IP Address	Enter the IP address of this panel. The default TCP port used for this address is 3001. If you are using a different TCP port, enter the port as a fifth group in the IP address. For example, 69.143.66.10.333 indicates that port 3333 should be used instead).
Reply Timeout	Select the number of milliseconds this panel is allowed to wait for a reply from the appliance.
Offline Timeout	Enter the number of milliseconds this panel can be disconnected from an appliance before the panel attempts to connect to a standby appliance.
Retries	Select the number of times the panel will try to contact the appliance.
Poll Delay	Set the number of milliseconds the panel will wait between each attempt to contact the appliance.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Panel	Click this button to add a new panel.
Show Policy	Click this button to download a PDF of the panel's current policy.

Panels - Mercury Security Subpanels Page

When you click the **Subpanels** tab from the Panel Edit screen, the Subpanels Listing page is displayed. This page lists all the subpanels that have been added to the system and displays the following details about each subpanel:



Feature	Description
Name	The name of the subpanel. Click the name to edit the subpanel.
Type	This read-only column indicates the type of subpanel this is.
Port	This read-only column indicates the port that this subpanel is currently connected to on the master panel.
Address	This read-only column indicates the RS45 address of this subpanel.
Installed	 indicates the subpanel is installed and able to communicate with the appliance.  indicates that the subpanel is not installed. No communications to the subpanel will be attempted. Click the icon to change the installed status.

Feature	Description
	Click this icon to display the subpanel inputs listing page. This displays the input points available on the subpanel. For more information, see <i>Editing Subpanels</i> on page 117 and <i>Inputs</i> on page 56.
	Click this icon to display the subpanel outputs page. This displays the output points available on the subpanel. For more information, see <i>Editing Subpanels</i> on page 117 and <i>Outputs</i> on page 55.
	Click this icon to display the subpanel readers page for the specified subpanel. This displays the readers available with this module. For more information, see <i>Editing Subpanels</i> on page 117.
	Click this icon to delete the subpanel from the list.
Add New Subpanel	Click this button to add another subpanel to this panel. The Subpanel Add page appears.

Subpanels - Mercury Subpanel Add Page

When you click **Add New Subpanel** from the Subpanels Listing page, the Subpanels Listing page is displayed. This page allows you to define new subpanels for the system.



NOTE: Some of the listed fields may not be displayed if it is not supported by the door module.

Feature	Description
Name	Enter a name for this new subpanel.
Physical Location	Enter a brief description of where this subpanel is located.
Model	Select the model of this new subpanel.
Port	Select the port that this subpanel is connected to on the main panel.
Installed	Check this box to indicate that the subpanel is installed and able to communicate with the main panel.
Address	Select the RS45 address for the selected port.
Elevator Inputs	Check this box to indicate that the door module is used as an input for an elevator.
Elevator Outputs	Check this box to indicate that the door module is used as an output for an elevator.
IP Address	Enter the subpanel IP address.
MAC Address	Enter the subpanel MAC address.
Low Door	Enter the lowest door number in the series that is managed by the subpanel.
High Door	Enter the highest door number in the series that is managed by the subpanel.
	Click this button to save your changes.
	Click this button to discard your changes.


Subpanels - Subpanel Edit Page



When you click the name of a subpanel from the Subpanels Listing page, the Subpanel Edit page is displayed. This page allows you to define the identity of the panel and where it is connected to the master panel.



NOTE: Some of the listed fields may not be displayed if it is not supported by the door module.

Feature	Description
Name	The name of this subpanel.
Physical Location	A brief description of where this subpanel is located.
Model	The read-only field displays the subpanel descriptor or model number.
Port	Select the port number that connects this subpanel to the main panel.
Installed	Check this box to indicate that the subpanel installed and able to communicate with the main panel.
Address	Select the RS45 address for the selected port.
Elevator Inputs	Check this box to indicate that the door module is used as an input for an elevator.
Elevator Outputs	Check this box to indicate that the door module is used as an output for an elevator.
IP Address	The subpanel IP address.
MAC Address	The subpanel MAC address.
Low Door	The lowest door number in the series that is managed by the subpanel.
High Door	The highest door number in the series that is managed by the subpanel.
	Click this button to save your changes.
	Click this button to discard your changes.

Subpanels - Mercury Input Listing Page

If you click  from the Subpanels Listing page, the Input Listing page is displayed. This page lists all the input points that are available on the subpanel, and displays the following details about each input:

Feature	Description
Inputs	The name of the input. The default name of the input is the input's location on the subpanel. Click the name to edit the input.
Address	The read-only address of this input point on the subpanel.
Masked	The current masking status for this input. <ul style="list-style-type: none">  indicates the point is masked.  indicates the point is not masked. Click the icon to change the masking status.

Feature	Description
Installed	<p>The current input connection status.</p> <ul style="list-style-type: none"> •  indicates the input is installed and able to communicate with the appliance. •  indicates that the input is not installed. No communications to the subpanel will be attempted. <p>Click the icon to change the installed status.</p>
Interlocks	Click Interlocks to open the Interlocks List page for the input.

Subpanels - Mercury Input Edit Page



When you click the name of an input from the Inputs Listing page, the Input Edit page is displayed. This page allows you to define the details of the input.

Feature	Description
Input	The name of the input. The default name of the input is the input's location on the subpanel.
Installed	Check this box to indicate that this point is connected and active.
Address	The read-only address of this input point.
Mode	Select the input mode: <ul style="list-style-type: none"> • Normal – this input point is in normal mode. • Non-latching – this input point does not latch. • Latching – this input point must latch.
EOL¹ resistance	Select the end-of-line resistance option used by the input. Only the EOL resistance options defined for the system are listed. For more information, see <i>EOL Resistance</i> on page 189.
Logging	Select the level of logging that is required for this input: <ul style="list-style-type: none"> • Log all changes – log any change to this input. • Do not mask CoS² if masked – Do not mask the change of state reporting if the input is already masked. • Do not mask CoS if masked and no trouble CoS – Do not mask the change of state reporting if the input is already masked and there is no issue with this change of state.
Debounce³	Select how often the unit is allowed to debounce in a row. 1 = 16 ms, 2 = 32 ms, etc.
Entry Delay	Enter the number of seconds allowed for each entry before the input reports an event.
Exit Delay	Enter the number of seconds allowed for each exit before the input reports an event.
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.
Schedule	Define when the input is active. Select a schedule from the drop down list.

¹End-Of-Line (EOL) are resistors that supervise the wiring between the alarm panel and the switch. Preset resistance levels must be maintained at input points or an alarm event is triggered.


²Change of State

³Due 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" software is designed to anticipate it. This is known as "debouncing a switch".

Feature	Description
	Only schedules that have been defined in the system are listed.
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.
Masked	Check this box to indicate that this input is normally masked.
Canned Macros	
Type	Select a type of macro. Only the macros supported by the input point are listed.
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Operation Type	The read-only summary of the macro operation type.
Output	Select the output that is triggered when the macro is activated.
Save Macro	Click this button to save the canned macro settings. You can create more than one canned macro per input. For more information, see <i>Adding Simple Macros</i> on page 58.
	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.

Interlocks - Input Listing Page


When you click the **Interlocks** link from the subpanels input listing page, the Input Interlocks Listing page is displayed.


Feature	Description
Interlocks	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 New Interlock	Click this button to add a new interlock to the system.



Interlocks - Input Add Page


When you click **Add New 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.


Interlocks - Input Edit Page



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

Subpanels - Mercury Outputs Listing Page



When you click  from the Subpanels Listing page, the Outputs Listing page is displayed. This page lists all the output points that are available on the subpanel, and displays the following details about each output:

Feature	Description
Outputs	The name of the output. The default name of the output is the output's location on the subpanel. Click the name to edit the output.
Address	The read-only address of this output point on the subpanel.
Installed	The current output connection status. <ul style="list-style-type: none">  indicates the output is installed and able to communicate with the appliance.  indicates that the output is not installed. No communications to the subpanel will be attempted. Click the icon to change the installed status.
Interlocks	Click Interlocks to open the Interlocks List page for the output.




Subpanels - Mercury Outputs Edit Page

When you click the name of an output from the Outputs Listing page, the Outputs Edit page is displayed. This page allows you to define the details of this output.

Feature	Description
Output	The name of the output point. The default name is the location of the output point on the subpanel.
Installed	Check this box to indicate that this output point is connected and active.
Address	The read-only address for this output point on the subpanel.
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.</p> <p>Only schedules that have been defined in the system are listed.</p>
Partitions	<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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</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 module.

Interlocks - Output Listing Page


When you click the **Interlocks** link from the subpanels output listing page, the Output Interlocks Listing page is displayed.


Feature	Description
Interlocks	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 New Interlock	Click this button to add a new interlock to the system.



Interlocks - Output Add page


When you click **Add New 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.


Interlocks - Output Edit Page



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

Subpanels - Mercury Readers Listing Page



When you click  from the Subpanels Listing page, the Readers Listing page is displayed. This page lists all the reader points that are available on the subpanel, and displays the following details about each reader:

Feature	Description
Reader	The name of the reader. The default name of the reader is the reader's location on the subpanel. Click the name to edit the reader.
Alt Name	The alternative name assigned to the reader.
Address	The read-only address of this reader on the subpanel.
Location	The physical location of this reader.
Installed	<p>The current reader connection status.</p> <ul style="list-style-type: none">  indicates the reader is installed and able to communicate with the appliance.  indicates that the reader is not installed. No communications to the reader will be attempted. <p>Click the icon to change the installed status.</p>

Subpanels - Mercury Reader Edit Page

When you click the name of a reader from the Readers Listing page, the Reader Edit page is displayed. This page allows you to define the details of the connected card reader.


Feature	Description
Name	The name of the reader. The default name of the reader is the reader's location on the subpanel.
Alt. name	Enter an alternative name for this reader.
Location	Enter a brief description of where the reader is installed.
Type	Select the type of reader this is.
Address	The read-only address of this reader.
Keypad decode	Select the keypad decode/encryption method used by this reader. The options are: <ul style="list-style-type: none"> • MR20 8-bit tamper • Hughes ID 4-bit • Indala • MR20 8-bit no tamper
LED drive	Select the LED driver for this reader. The options are: <ul style="list-style-type: none"> • None • Gen 1 wire • Reserved • Sep Red/Grn no buzz • Dorado 780 • LCD MR50T • OSDP
Wiegand	Check this box to indicate that the reader supports the Wiegand standard.
Trim Zero Bit	Check this box to indicate that the reader supports the trim zero bit standard.
NCI magstripe	Check this box to indicate that the reader supports the NCI magstripe standard.
Format by nibble	Check this box to indicate that the reader supports the format by nibble.
Supervised	Check this box to indicate that the reader is supervised by some detection device, like a tamper switch.
Bidirectional	Check this box to indicate that the reader is bidirectional.
F/2F	Check this box to indicate that the reader uses either an F or 2F decoding scheme.

Feature	Description
Decoding	
Inputs on reader	Check this box to indicate that the reader possesses one or more input ports, allowing other input devices to be connected further downstream.
	Click this button to save your changes.
	Click this button to discard your changes.

Panels - Mercury Security Macros

When you click the **Macros** tab from the Panel Edit screen, the Macro Listing page is displayed. You can also access this page by clicking the **Macro** button on the Triggers Listing page.

This page lists all the macros that have been added to the system and displays the following details about each macro:

Feature	Description
Name	<p>The name of each macro that has been defined for the panel. There may be predefined macros and user defined macros.</p> <p>The default name of user defined macros is "Macro" followed by an auto-assigned system number. (The system numbering begins at 3075 and is incremented for each new macro.)</p> <p>Click the macro name to display the Macro Command Listing page. This page lists all the commands that are part of the selected macro.</p>
In use	This column indicates the number of triggers that are using the macro.
Triggers	Click this button to display the Triggers page for this panel.
	<p>Click this button to delete the macro from the list.</p> <p>When the confirmation message appears, click OK.</p>
Add New Macro	Click this button to add a new macro. The Macro Command Listing page for the new macro is displayed.


Macros - Macro Command Listing Page

When you add or edit a macro, the Macro Command Listing page is displayed. This page lists all the commands that are managed by a macro.

The name of the panel and macro appear at the top of this page.



- The panel name links to the panel's Configure page.
- Click the Macro name to change it.

Feature	Description
Sequence	The order in that the commands are executed when the macro is triggered. By default, the commands are listed in the order they were created.

Feature	Description
	If you want to change the sequence order, click the Sort button. For more information, see <i>Sorting Macros</i> on page 119.
Command	The type of command that would be executed. Click the command type to edit the command details.
Group	The macro group to which this command belongs.
Sort	Click this button to re-order the listed commands. The order of the commands defines what action is taken first when the macro is initiated. This button only appears if there are two or more macro commands. For more information, see <i>Sorting Macros</i> on page 119.
Delete	Click  to remove this command from the list.
Add New Macro Command	Click this button to add a new macro command.

Macros - Macro Command Add Page







If you click **Add New Macro Command** from the Macro Command Listing page, the Add New Macro Command page is displayed.

Feature	Description
Macro Command Name	Enter a name for this command.
Command	Select the type of macro command this is. Depending on option that is selected, new options are displayed.
Sequence:	After you save this command, the system assigns it a number based on where the command appears in the Macro Command List.
Group	Select the group this command belongs to. You can assign the command to Group A , Group B , Group C or Group D . Once the macro is added to a group, you can combine the macro groups into sequences. For example, Group A is followed by Group B, or Group D is triggered by Group C. Also, assigning a macro to a specific macro group enables you to subdivide and sort macros for Global Actions and Global Linkages .
	Click this button to save your changes.
	Click this button to discard your changes.

Macros - Macro Command Edit Page

If you click the command type from the Macro Command Listing page, the Macro Command Edit page is displayed.


Make the changes that are required.

Feature	Description
Name	The name of the macro command.
Command	The macro command type.
Group	The group this macro belongs to.
Additional fields	Depending on the command type, there may be different options displayed on the page. For example, in the screenshot above, choosing the Delay in Seconds option causes the Delay (in seconds) field to appear.
Macro command navigation buttons	<ul style="list-style-type: none"> Click  to display the first command in sequence for this macro. Click  to display the previous command in sequence for this macro. Click  to display the next command in sequence for this macro. Click  to display the last command in sequence for this macro. <p>These buttons are only displayed if there are more than one command for a macro.</p>
	Click this button to save your changes.
	Click this button to discard your changes.

Triggers - Listing page



When you click the **Triggers** tab from the Panel Edit screen, the Triggers Listing page is displayed. You can also access this page by clicking the **triggers** button from the Macros Listing page.

This page lists all the triggers that have been added to the system and displays the following details about each trigger:

Feature	Description
Trigger name	The name of the trigger.
	Click the name to edit the trigger.
Enabled	Indicates if this trigger is active (Yes) or inactive (No).
Schedule	Indicates schedule used by the trigger.
Commands	Click Macro to go to the Macro Listing page.
	Click  to delete the trigger.
Add New Trigger	Click this button to add a new trigger.

Triggers - Add Page



When you click the **Add New Trigger** button from the Trigger Listing page, the Trigger Add page is displayed.

Feature	Description
Trigger Name	Enter a name for the trigger.
Enabled	Check this box to indicate that the trigger is active.
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Macro	Select the macro that is activated by this trigger. Only the macros that have been defined in the system are listed. Once you have selected a macro, edit appears beside the selected macro. Click edit to view or edit the macro commands.
Command	Select the action that the macro should perform when the trigger conditions are met. The letters in the option list reference the group the individual macro commands are part of. For more information, see <i>Macros - Macro Command Add Page</i> on page 169.
Triggering on these conditions:	
Source Type	Select the type of device that is the source of this trigger. After you select one of the options, the Event fields are populated with the options available to the source type.
Source	Select the specific device that is the source of this trigger.
Additional fields	After you select a Source Type option, new fields may be displayed to provide you with more options.
Event Type	Select the type of event that should be part of the trigger conditions. The event type you select here determines the events that populate the Event list.
Event	Select one or more events that define the trigger conditions.
Trigger Variables	
Var1/Var2/Var3/Var4	Select the value that represents the variable. Values range from 0 - 127 where 0 is the default value. Up to four trigger variables can be defined for a specific trigger. Trigger variables are 127 general-purpose boolean variables. Triggers can fire based on a trigger variable changing state. Most commonly, trigger variables are used to create a toggle effect where a pair of triggers are created with identical terms except one requires a trigger variable to be true and the other requires the same trigger variable to be false. A macro can also set the state of a trigger variable as part of its command set.
Invert?	Check this box to indicate that the logic of this specified variable is only triggered when the term is inverted. That is, if the trigger variable itself is true, inverting it makes the trigger occur only if the variable is deemed false.
	Click this button to save your changes.
	Click this button to discard your changes.

Triggers - Edit Page

When you click the name of a trigger from the Triggers Listing page, the Trigger Edit page is displayed.

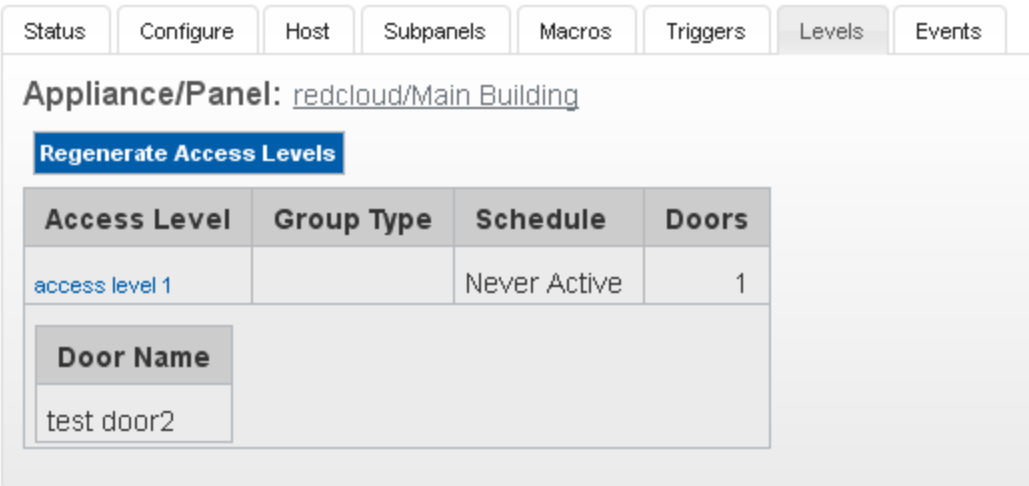
This page can include many different fields depending on the options that have been selected. The most common fields are listed in the following table. You can change any of the following fields as required:

Feature	Description
Trigger Name	The name of the trigger.
Enabled	Check this box to indicate that the trigger is active.
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Macro	The macro that is activated by this trigger. Click edit to view and edit the macro commands.
Command	The action that the macro should perform when the trigger conditions are met. The letters in the option list reference the group the individual macro commands are part of. For more information, see <i>Macros - Macro Command Add Page</i> on page 169.
Triggering on these conditions:	
Source Type	The type of device that is the source of this trigger.
Source	The specific device that is the source of this trigger.
Additional fields	The selected Source Type option determines what additional fields are displayed. Edit the relevant options.
Event Type	The type of event that is part of the trigger conditions.
Event	The specific events that define the trigger conditions.
Trigger Variables	
Var1/Var2/Var3/Var4	The value that represents the variable. Values range from 0 - 127 where 0 is the default value. Up to four trigger variables can be defined for a specific trigger. Trigger variables are 127 general-purpose Boolean variables. Triggers can fire based on a trigger variable changing state. Most commonly, trigger variables are used to create a toggle effect where a pair of triggers are created with identical terms except one requires a trigger variable to be true and the other requires the same trigger variable to be false. A macro can also set the state of a trigger variable as part of its command set.
Invert?	Check this box to indicate that the logic of this specified variable is only triggered when the term is inverted. That is, if the trigger variable itself is true, inverting it makes the trigger occur only if the variable is deemed false.
	Click this button to save your changes.
	Click this button to discard your changes.

Panels - Mercury Security Access Levels Page

When you click the **Access Levels** tab from the Panel Edit screen, the Access Level Listing page is displayed.

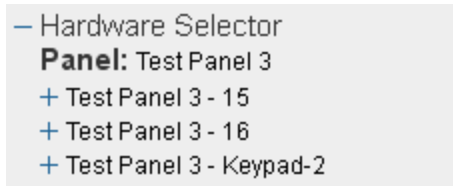
Access levels are the result of applying various rules to each panel and are computed in the background. These levels are sent down to the panel automatically and do not require any manual configuration. This page displays a list of all the access levels that have been generated for the panel.

Feature	Description
Regenerate Access Levels	<p>Click this button to regenerate the access levels that apply to the panel. You will immediately see the following warning message:</p> <p><i>WARNING: All Tokens will be removed and re-downloaded.</i></p> <p>Click OK to remove the existing tokens and update them with the latest tokens.</p>
Access Level	<p>The name of the access level.</p> <p>To see the doors that use the access level, click the access level name and the connected doors are displayed below.</p> 
Group Type	<p>If the access level is part of a group type, it is identified in this column.</p>
Schedule	<p>Displays the schedule that defines when the access level is active.</p>
Doors	<p>Lists the total number of doors that use this access level. Click the Access Level name to see the full list of door names.</p>

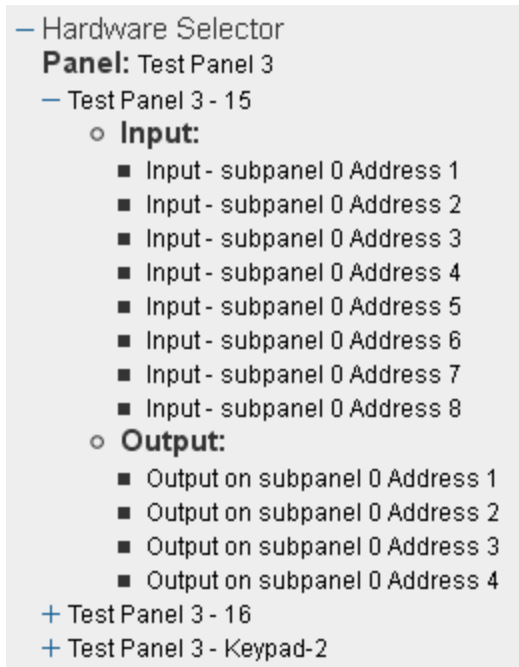
Panels - Mercury Security Events Page

If you click the **Events** tab from the Panel Edit screen, the Events page is displayed. This page gives you a list of all the global events that are available to each device that is connected to this panel.





- In the top left corner of the page, click the + sign in **+Hardware Selector** to display a list of all the devices that are connected to the panel. For example:






If you click + beside a subpanel, a list of the connected inputs and outputs is displayed. For example:



Click the - sign to hide the list items.

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 ().

Feature	Description
	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.




Panels - Create Local Events for Mercury Panels

When you click the **Create Local** button from the Panel 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 panel.

NOTE: Changes on this page do not affect the global event.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
Alarm Sound	Select an alarm sound that is played when a new alarm occurs while you are monitoring the Alarms page.

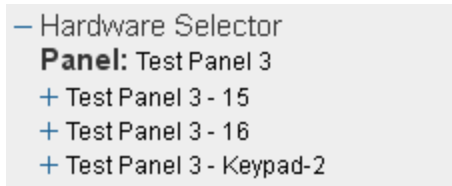
¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

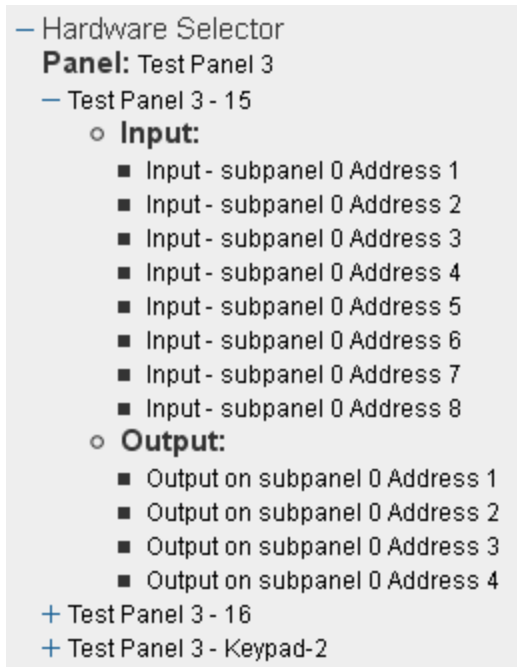
Subpanels - Mercury Security Events Page

If you select a subpanel from the Panel Events page, the page refreshes to display the related subpanel events.





- In the top left corner of the page, click the + sign in **+Hardware Selector** to display a list of all the devices that are connected to the panel. For example:






If you click + beside a subpanel, a list of the connected inputs and outputs is displayed. For example:



Click the - sign to hide the list items.

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 ().

Feature	Description
	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.

Subpanels - Create Local Events for Mercury Subpanels




When you click the **Create Local** button from the Subpanel 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 subpanel.

NOTE: Changes on this page do not affect the global event.

Make any changes as required.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.

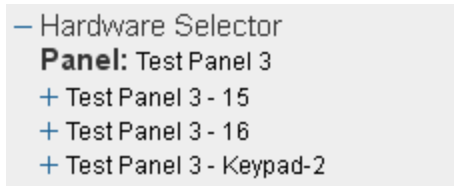
¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

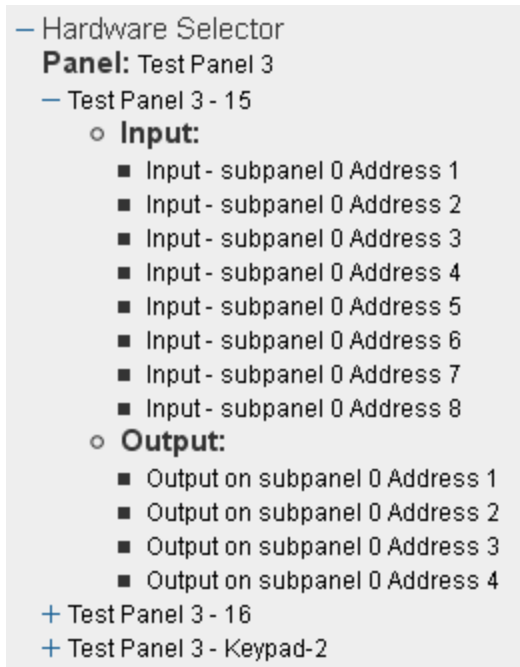
Inputs - Mercury Security Events Page

If you select an input from the Panel Events page, the page refreshes to display the related input events.





- In the top left corner of the page, click the + sign in **+Hardware Selector** to display a list of all the devices that are connected to the panel. For example:






If you click + beside a subpanel, a list of the connected inputs and outputs is displayed. For example:



Click the - sign to hide the list items.

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 ().

Feature	Description
	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.

Inputs - Create Local Events for Mercury Inputs




When you click the **Create Local** button from the Input 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 input.

NOTE: Changes on this page do not affect the global event.

Make any changes as required.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
Alarm Sound	Select an alarm sound that is played when a new alarm occurs while you are monitoring the

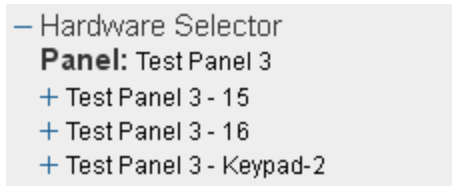
¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
	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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

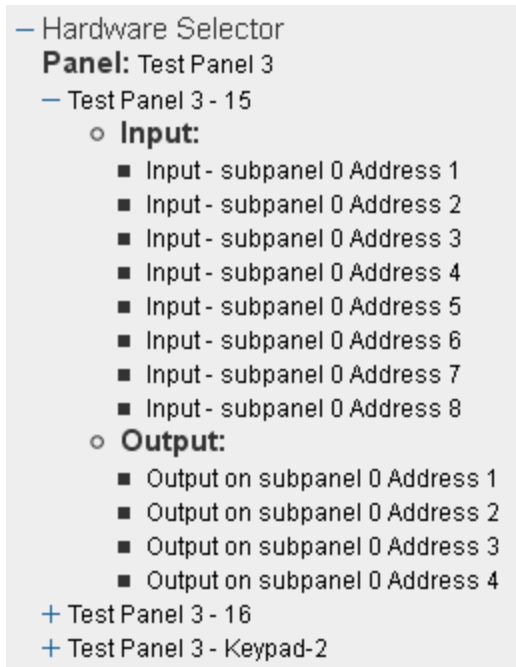
Outputs - Mercury Security Events Page

If you select an output from the Panel Events page, the page refreshes to display the related output events.





- In the top left corner of the page, click the + sign in **+Hardware Selector** to display a list of all the devices that are connected to the panel. For example:






If you click + beside a subpanel, a list of the connected inputs and outputs is displayed. For example:



Click the - sign to hide the list items.

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 ().

Feature	Description
	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.

Outputs - Create Local Events for Mercury Outputs




When you click the **Create Local** button from the Output 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 output.

NOTE: Changes on this page do not affect the global event.

Make any changes as required.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	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 Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.

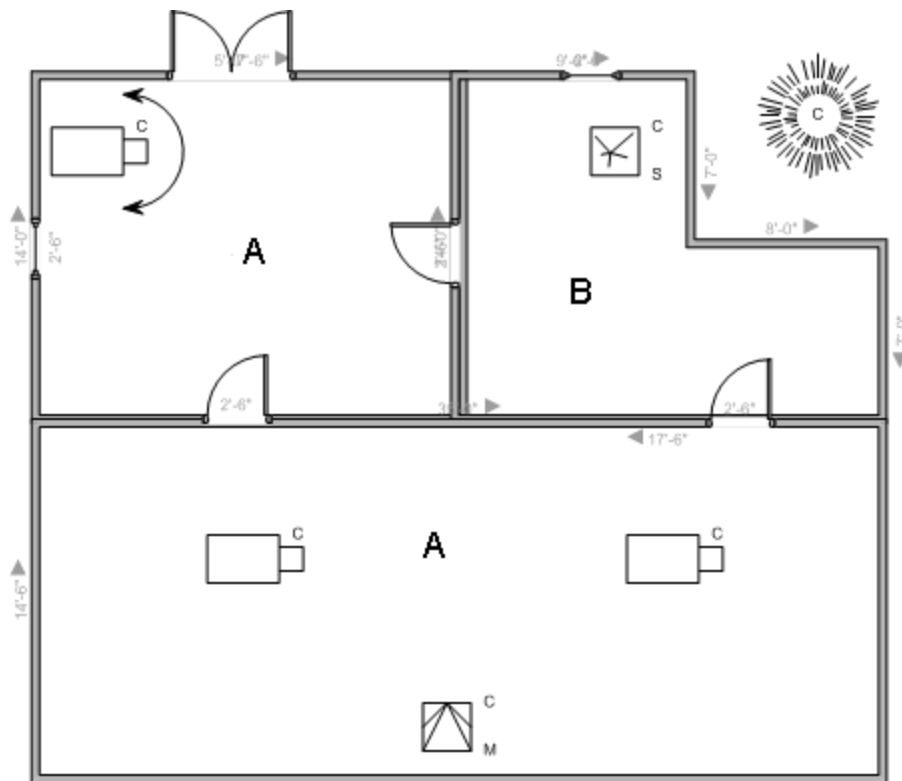
¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.
	Click this button to discard your changes.

Areas


Areas are zones that Access Control Manager 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. Once an area is defined, it can be assigned to a role or policy to limit user access within a building or facility.

For example, a scientist works in a laboratory in Area A. As long as he accesses doors leading into or exiting that area, he is granted access. But if he attempts to enter an area designated as Area B, he is denied access.



Defined areas are added to the **Area into area** and **Area out of area** option list on the Doors Operations page. For more information, see *Configuring Doors* on page 57.

Areas - Adding

1. From the icon task bar on the home page, select **Physical Access > Areas**.
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. See *Areas - Add Page* on the next page for more detail.
7. Click .

The new area is added to the Area Listings page.


Areas - Editing

1. From the icon task bar on the home page, select **Physical Access > Areas**.
2. Click the name of the area you want to edit.
3. On the following page, make the required changes.

If you want to change the doors that are connected to the area, you must do so from the door's Operations page.

4. Click  .


Areas - Deleting

1. From the icon task bar on the home page, select **Physical Access > Areas**.
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**.

Areas - Listing Page

When you select **Areas** from the Physical Access sub-options task bar, the Areas Listing page is displayed.



The Area Listing page lists all the areas that have been defined in the system, or your area search results.

Feature	Description
Name	Name of the area. Click the name to edit the area.
Appliance	The appliance this area is configured on.
Enabled	This column indicates if this area is currently enabled (Yes) or disabled (No).
Door Count	The number of doors in this area.
Delete	Click  to delete the area from the system.
Add New Area	Click this button to create a new area.
Create New Report	Click this button to generate a report of all the available areas.

Areas - Add Page

When you click the **Add New Area** button from the Areas Listing page, The Areas Add page is displayed. This page allows you to add a new area to the system.

Feature	Description
Name	Enter a name for this area.
Appliance	Select the appliance that will maintain this area. Tip: You can add doors from different appliances to an area.
Maximum Occupancy	Enter the maximum number of cardholders allowed in this area at a time.
Log Min Reached	Enter the minimum number of cardholders that must enter this area before a transaction is logged in the system.



Feature	Description
Log Max Reached	Enter the maximum number of cardholders that must enter this area before a transaction is logged in the system.
Enable Area	Check this box to enable this area in the system.
2-Person Control	<p>Check this box to indicate a two-person rule is imposed for this area.</p> <p>If enabled, two or more people must be in the area at all times. When the area is empty, two valid cardholders must present their credentials to the entry reader before entry is granted. Once occupied by two or more people, individual access can be granted. The same rules apply for exit until two cardholders are left in the area - at this point, both cardholders must present their credentials and must exit the area together.</p>
Partitions	<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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</p>
	Click this button to save your changes.
	Click this button to discard your changes.

Areas - Edit Page

When you click the name of an area from the Areas Listing page, the Areas Edit page is displayed.

This page allows you to edit area details and see a list of all the doors that have been assigned to this area. Make changes as required.

Feature	Description
Name	Enter a name for this area.
Appliance	The appliance the area is assigned to.
Maximum Occupancy	Enter the maximum number of cardholders allowed in this area at a time.
Log Min Reached	Enter the minimum number of cardholders that must enter this area before a transaction is logged in the system.
Log Max Reached	Enter the maximum number of cardholders that must enter this area before a transaction is logged in the system.
Enable Area	Check this box to enable this area in the system.
2-Person Control	<p>Check this box to indicate a two-person rule is imposed for this area.</p> <p>If enabled, two or more people must be in the area at all times. When the area is empty, two valid cardholders must present their credentials to the entry reader before entry is granted. Once occupied by two or more people, individual access can be granted. The same rules apply for exit until two cardholders are left in the area - at this point, both cardholders must present their</p>

Feature	Description
	credentials and must exit the area together.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Doors In	The list of doors that enter this area. Doors are added to this list when you assign this area to the door from the Door Operations page.
Doors Out	The list of doors that exist this area. Doors are added to this list when you assign this area to the door from the Door Operations page.
	Click this button to save your changes.
	Click this button to discard your changes.


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. From the icon task bar, 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 to HID Input Points

To add an EOL Resistance definition for an HID input point:

1. From the icon task bar, select **Physical Access > EOL Resistance > HID**.
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. From the icon task bar, 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 HID Input Points



To edit an EOL Resistance definition for an HID input point:

1. From the icon task bar, select **Physical Access > EOL Resistance > HID**.
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.

EOL Resistance - HID Listing Page



The HID Listing page is displayed when you select the **HID** tab from the EOL Resistance Listing page.

This page lists all the EOL resistance states that are available in the system and the address that is set for each.

Feature	Description
Name	The name of the EOL resistance. Click the name to edit the EOL resistance. If you cannot click the name, it is a system default resistance value and cannot be edited.
Delete	Click  to delete the selected resistance setting. Default resistance values cannot be deleted.
Add	Click  to add a resistance setting.

EOL Resistance - Add Page



When you click **Add** from the HID Listing page, the EOL Resistance Add page is displayed. This page allows you to add a resistance range to a specific input point on the panel.

Feature	Description
Name	Enter a name for this EOL input point.
Inactive Range	In the left drop down list, select the beginning value of the inactive range. In the right drop down list, select the ending value of the inactive range. Values range from 0 to 13000 ohms in 50-ohm increments, or Infinite .
Active Range	In the left drop down list, select the beginning value of the active range. In the right drop down list, select the ending value of the active range. Values range from 0 to 13000 ohms in 50-ohm increments, or Infinite .
	Click this button to save your changes.
	Click this button to discard your changes.

EOL Resistance - Edit Page

When you click an EOL resistance name from the HID Listing page, the EOL Resistance Edit page is displayed.

Make changes as required.


Feature	Description
Name	The name of this EOL input point.
Inactive Range	In the left drop down list is the beginning value of the inactive range. In the right drop down list is the ending value of the inactive range. Values range from 0 to 13000 ohms in 50-ohm increments, or Infinite .
Active Range	In the left drop down list is the beginning value of the active range. In the right drop down list is the ending value of the active range. Values range from 0 to 13000 ohms in 50-ohm increments, or Infinite .
	Click this button to save your changes.
	Click this button to discard your changes.

EOL Resistance - Mercury Listing Page

When you select **EOL Resistance** from the Physical Access sub-options task bar, the first page you see is the Mercury Listing page. Select the Mercury tab to return to this page.



This page lists all the EOL resistance states that are available in the system and the address that is set for each.

Feature	Description
Name	The name of the EOL resistance. Click the name to edit the EOL resistance. If you cannot click the name, it is a system default resistance value and cannot be edited.
Address	The address assigned to this resistance.

Feature	Description
Delete	Click  to delete the selected resistance setting. Default resistance values cannot be deleted.
Add-Normal	Click this button to add a normal resistance setting.
Add-Advanced	Click this button to add an advanced resistance setting.

EOL Resistance - Add Normal Page



When you click **Add-Normal** from the Mercury Listing page, the EOL Resistance Add Normal page is displayed. This page allows you to add a normal resistance range to a specific input point on the panel.

Feature	Description
Name	Enter a name for this EOL input point.
Address	Select the address for this input point.
Inactive Range	In the left drop down list, select the beginning value of the inactive range. In the right drop down list, select the ending value of the inactive range. Values range from 100 to 9950 ohms in 50-ohm increments.
Active Range	In the left drop down list, select the beginning value of the active range. In the right drop down list, select the ending value of the active range. Values range from 100 to 9950 ohms in 50-ohm increments.
	Click this button to save your changes.
	Click this button to discard your changes.

EOL Resistance - Add Advanced Page

When you click **Add-Advanced** from the Mercury Listing page, the EOL Resistance Add Advanced page is displayed. This page allows you to add multiple resistance ranges, plus define priority and status for the input point on the panel.

Feature	Description
Name	Enter a name for this EOL input point.
Address	Select the address for this input point.
Priority	Select the priority level for this input point. The options are Low , Medium , and High .
Status	Select the input state that you are defining. The options are: <ul style="list-style-type: none"> • Inactive • Active • Ground Fault • Shorted • Open



Feature	Description
	<ul style="list-style-type: none"> • Foreign
Low Range	Select the beginning value of the range. The options are: <ul style="list-style-type: none"> • Infinite — The resistance value is infinite (no ohm value is specified). • Shorted — The wire is shorted. • Ground A — The wire is detected as ground A. • Ground B — The wire is detected as ground B. • 0 - 10000 — The ohms specified for this resistance in 50-ohm increments.
High Range	Select the ending value of the range. The options are: <ul style="list-style-type: none"> • Infinite — The resistance value is infinite (no ohm value is specified). • Shorted — The wire is shorted. • Ground A — The wire is detected as ground A. • Ground B — The wire is detected as ground B. • 0 - 10000 — The ohms specified for this resistance in 50-ohm increments.
	Click this button to save your changes.
	Click this button to discard your changes.



EOL Resistance - Edit Page

When you click the name of an EOL resistance from the Listing page, the EOL Resistance Edit page is displayed. The options are different depending on the type of resistance you selected.

Make changes as required.

Normal Edit Page

Feature	Description
Name	The name of this EOL input point.
Address	The address of this input point.
Inactive Range	In the left drop down list is the beginning value of the inactive range. In the right drop down list is the ending value of the inactive range. Values range from 100 to 9950 ohms in 50-ohm increments.
Active Range	In the left drop down list is the beginning value of the active range. In the right drop down list is the ending value of the active range. Values range from 100 to 9950 ohms in 50-ohm increments.
	Click this button to save your changes.
	Click this button to discard your changes.


Feature	Description
Name	The name of this EOL input point.
Address	The address of this input point.
Priority	The priority level for this input point. The options are Low , Medium , and High .
Status	The input state. The options are: <ul style="list-style-type: none"> • Inactive • Active • Ground Fault • Shorted • Open • Foreign
Low Range	The beginning value of the range. The options are: <ul style="list-style-type: none"> • Infinite — The resistance value is infinite (no ohm value is specified). • Shorted — The wire is shorted. • Ground A — The wire is detected as ground A. • Ground B — The wire is detected as ground B. • 0 - 10000 — The ohms specified for this resistance in 50-ohm increments.
High Range	The ending value of the range. The options are: <ul style="list-style-type: none"> • Infinite — The resistance value is infinite (no ohm value is specified). • Shorted — The wire is shorted. • Ground A — The wire is detected as ground A. • Ground B — The wire is detected as ground B. • 0 - 10000 — The ohms specified for this resistance in 50-ohm increments.
	Click this button to save your changes.
	Click this button to discard your changes.

Card Formats

Readers that control access to doors come in many varieties and use many different card protocols. The most commonly used card formats have been Wiegand and magnetic stripe. However, newer cards that use embedded chips and proprietary formats have become more popular with the increase of security requirements.


The Access Control Manager application supports the most popular card formats and enables the qualified operator to define custom card formats.

Adding Card Formats


1. From the icon task bar, select **Physical Access > Card Formats**.
2. Click **Add New Card Format**.
3. In the Card Format Add page, enter the required details for the new card format.
4. Click  to save the new card format.

This new card format is now available and can be assigned to doors in the system.

Editing Card Formats

1. From the icon task bar, 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 new card format.


Deleting Card Formats

1. From the icon task bar, 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**.

Card Formats - Listing Page

When you select **Card Formats** from the Physical Access sub-options task bar, the Card Formats Listing page is displayed.

This page lists all the card formats that have been defined for this system.



Feature	Description
Name	The name of the card format. Click the name to edit the card format.
Delete	Click  to delete the card format.
Add New Card Format	Click this button to add a new card format.

Card Formats - Add Page

When you click **Add New Card Format** from the Card Format Listing page, the Card Format Add page is displayed. This page allows you to add a custom card format.

NOTE: The some of the options that are displayed depend on the selected card format type.

Feature	Description
Name	Enter a name for this card format.
Card Format Type	Select the card format type. The current options are:



Feature	Description
	<ul style="list-style-type: none"> • Wiegand • ABA Mag <p>The option you select will determine which of the following options are displayed.</p>
Facility Code	The facility code of this card format.
Offset	The offset number for this code.
Max Bits	The maximum number of bits this card format can possess.
Min Digits	The minimum number of bits this card format can possess.
Even Parity Length	The even parity length of the number on this card format.
Even Parity Location	The location in the number string where the even parity bits reside.
Odd Parity Length	The length of the odd parity bits on this card format.
Odd Parity Location	The location in the number string where the odd parity bits reside.
Facility Code Length	The length of the facility code in digits.
Facility Code Location	The location in the number string where the odd parity bits reside.
Card Number Length	The total length of the card number on this card.
Card Location	The location of the card number in the number string.
Issue Level Length	The length of the issue level number in the number string.
Issue Location	The location of the issue level number in the number string.
Step parity by 2	Check this box to indicate that the parity must be stepped by 2.
Suppress facility check	Check this box to ignore a facility check. This operation will not be performed.
Corporate card mode	Check this box to enable use of the corporate card format.
Enable 37 bit parity w/4	Check this box to enable 37-bit parity by 4 format.
Enable 37 bit parity w/2	Check this box to enable 37-bit parity by 2 format.
Enable 75 bit transparent mode	Check this box to enable 78-bit transparent mode.
Reverse card format	Check this box to enable reverse card format.
	Click this button to save your changes.
	Click this button to discard your changes.

Card Formats - Edit Page

When you click the name of a card format from the listing page, the Card Formats Edit page is displayed.

NOTE: The some of the options that are displayed depend on the selected card format type.

Feature	Description
Name	The name of this card format.
Card Format Type	The card format type. The current options are:

Feature	Description
	<ul style="list-style-type: none"> • ABA Mag • Wiegand <p>The option you select will determine which of the following options are displayed.</p>
Facility Code	The facility code of this card format.
Offset	The offset number for this code.
Max Bits	The maximum number of bits this card format can possess.
Min Digits	The minimum number of bits this card format can possess.
Even Parity Length	The even parity length of the number on this card format.
Even Parity Location	The location in the number string where the even parity bits reside.
Odd Parity Length	The length of the odd parity bits on this card format.
Odd Parity Location	The location in the number string where the odd parity bits reside.
Facility Code Length	The length of the facility code in digits.
Facility Code Location	The location in the number string where the odd parity bits reside.
Card Number Length	The total length of the card number on this card.
Card Location	The location of the card number in the number string.
Issue Level Length	The length of the issue level number in the number string.
Issue Location	The location of the issue level number in the number string.
Step parity by 2	Check this box to indicate that the parity must be stepped by 2.
Suppress facility check	Check this box to ignore a facility check. This operation will not be performed.
Corporate card mode	Check this box to enable use of the corporate card format.
Enable 37 bit parity w/4	Check this box to enable 37-bit parity by 4 format.
Enable 37 bit parity w/2	Check this box to enable 37-bit parity by 2 format.
Enable 75 bit transparent mode	Check this box to enable 78-bit transparent mode.
Reverse card format	Check this box to enable reverse card format.
	Click this button to save your changes.
	Click this button to discard your changes.

Events - Introduction

The system will generate 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 new events but 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 231.

Events - Searching

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.

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 doors you want to see. If needed, use wildcard characters. For more information, see *Wildcard Characters* on page 419.

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.

Events - Editing

1. From the icon task bar, select **Physical Access > Events**.
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.

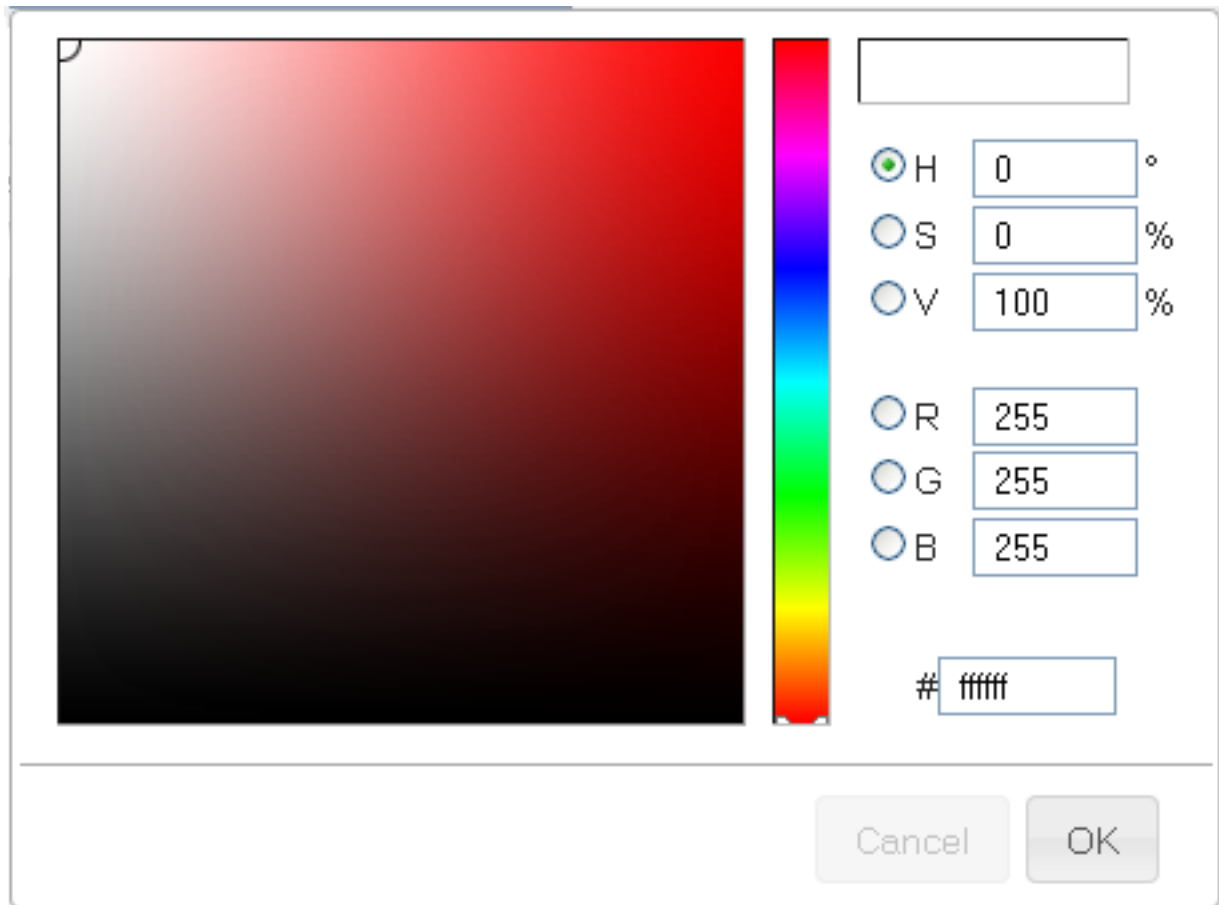
Events - Assigning Priority Colors


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. From the icon task bar, 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.
4. On the following page, enter the priority number that this color set should be assigned to.

- For each of the color options, click the color field to display the color map.



- Pick the color that you want on the left, or enter the color code on the right.
- Once you've selected the color you want, click **OK**.
- Click  to save.

Events - Listing Page

When you select **Events** from the Physical Access sub-options task bar, the first page you see is the Events Listing page. Select the Events tab to return to this page.









This page lists all the system defined events. You cannot add or delete events, but you can click the name of an event to customize it for your purposes.

The listed events may be highlighted in different colors to reflect their priority in the system. For more information, see *Events - Colors Listing Page* on page 202

You can perform a search to locate a specific event. For more information, see *Events - Searching* on the previous page

NOTE: Local device versions of events are listed in the device events page.

Feature	Description
Name	The name of this event.

Feature	Description
	Click the name to edit the event details.
Event Type	The event type that is assigned to this event. Click the event type to edit its settings.
Source	The device that generates this event.
Has On/Off	Indicates if this event has a physical on/off switch. Yes() or No (). Click the icon to change the status.
Masked	Indicates if this event is masked/ not reported in the Event Monitoring or Alarm Monitoring screen. Yes () or No (). Click the icon to change the status.
Logged	Indicates if this event is physically logged in the transaction database. 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.
Delete	Not currently used.
Create New Report	Click this button to generate a PDF summary of all the events.



Events - Edit Page


When you click the name of an event from the Events Listing page, the Event Edit page is displayed. Click the Events tab to return to this page.

This page allows you to define what happens when the event occurs, including who will be notified of the event. Make any changes that may be required.

Feature	Description
Name	The name of the event.
Return Name	The name used to identify that this event is over, or the return-to-normal (RTN ¹) name of this event.
Event Type	The event type. Only events types that have been defined in the system appear in the drop down list.

¹Return to normal. This is normally associated with an event that effectively cancels an original event. For example, a door open too long event is canceled by a door closed RTN.

Feature	Description
Source Type	The device that is the source of the event.
Priority	Specify the priority of this event. The Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
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 an event type for the RTN event.
Return Priority	Enter the priority number for the RTN event. The priority range is 1 - 999.
Has on/off	Check this box to indicate that this event is a toggle, involving an on/off switch logic.
Masked	Check this box to indicate that this a masked event.
Logged	Check this box to log the event.
Show Video	Check this box to auto-launch video from the linked camera feed when the event occurs. This feature only works if video is enabled.
Two Person Required To Clear	Check this box to specify that two people are required to acknowledge and clear this event. If this box is checked then the operator that executes the Clear cannot be the same operator that executes the Acknowledge. If the same operator attempts to clear the alarm, then nothing will happen.
Email	Enter the email address of all the people who should be notified when this event occurs. You can enter more than one email address separated by a comma.
Roles:	
Available	A list of all the roles that are available to you in the system. 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. To move one or more roles to the Members window, click to select one role then Ctrl + click to select a non-consecutive group of roles, or Shift + click to select a consecutive roles.
Members	A list of all the roles that are able to view or edit this event. 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.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.

Events - Colors Listing Page

When you select the **Colors** tab from the Events Listing Page, the Colors Listing page is displayed.

This page lists all the colors that have been assigned to an event priority number. The color is used to highlight events in the Alarm page and highlight events on other Event pages (like the Panel Event page or Door Events page).

Feature	Description
Priority	The event priority number that the colors are assigned to.
Alarm Color	The color of the event on the Alarm page when it is in the alarm state.
Acknowledge Color	The color of the event on the Alarm page when it is in the acknowledged state.

Events - Color Add Page

When you click **Add New Color** from the Colors Listing page, the Color Add page is displayed. This page allows you to assign colors to specific priority alarms.

Feature	Description
Priority	Enter the event priority that this color will be used to highlight.
Alarm Color	Click the field to display the color map and select a specific color, or manually enter the color hex code.
Acknowledge Color	Click the field to display the color map and select a specific color, or manually enter the color hex code.

Events - Color Edit Page

When you click a priority color from the Colors Listing page, the Color Edit page is displayed.

Make changes as required.

Feature	Description
Priority	The event priority that this color is assigned to.
Alarm Color	Click the field to display the color map and select a specific color, or manually enter the color hex code.
Acknowledge Color	Click the field to display the color map and select a specific color, or manually enter the color hex code.


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. From the icon task bar, select Physical **Access > Global Actions**.
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. From the icon task bar, select **Physical Access > Global Actions**.
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 group(s) 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 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 intrusion panel areas
Intrusion Outputs	
Intrusion Points	Specifies intrusion panel points
Output	Specifies that one or more designated outputs are activated/inactivated.


Feature	Description
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. From the icon task bar on the home page, select **Physical Access > Global Actions**.
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 Listing Page


When you click **Global Actions** from the Physical Access sub-options task bar, the Global Actions Listing page is displayed. This page lists all the global actions that have been configured in the system.





Feature	Description
Name	The name of the global action. Click the name to edit the global action.
Type	Indicates the type of action performed by this global action.
Points	Indicates the global linkages that use this global action.
Run	Click the Execute button to manually initiate this action.
Schedule	Click Schedule to create a batch job for the global action. For more information, see <i>Scheduling Batch Jobs</i> on page 8.
Delete	Click  to delete the specified action from this list.
Add New Global Action	Click this button to create a new global action.






Global Actions - Add Page




When you click **Add New Global Action** from the Global Actions Listing page, the Global Actions Add page is displayed. This page allows you to add a new global action to the system.

Feature	Description
Name	The name of the global action. Enter a descriptive name of the action.
Appliance	Select the appliance that the related panels and devices are connected to.
Partitions	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 appear in this list. You can only

Feature	Description
	see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Type	Select the type of action you want to be performed. The additional options appear depending on the option you choose.
If you select Panel Macro in the Type field:	
NOTE: Macros are only supported on Mercury panels.	
Sub-Type	Select a macro group. You can choose Execute Group A to Execute Group D .
Macro	Select a specific macro.
If you select Exacq Soft Trigger in the Type field:	
NOTE: You must set up an external system connection with an Exacq server to use this option.	
Sub-Type	Select one of the following options: <ul style="list-style-type: none"> • Single Set — run the selected trigger once. • Continuous Set — repeat the selected trigger until the Unset command is executed. • Unset — stop the continuous repetition of the selected trigger.
Trigger	Select the trigger action for this video server to perform, such as tilting, focusing or going to a preset position. Triggers are defined through the Exacq server.
If you select Door Install/Uninstall in the Type field:	
Sub-Type	Selected option will be applied to the doors in the Members list. Choose from the following: <ul style="list-style-type: none"> • Install — Install the doors in the Members list. • Uninstall — Uninstall the doors in the Members list. To add a door to the Members list, select a door from the Available list then click  .
If you select Door Mode in the Type field:	
Sub-Type	The selected option will be applied to the doors in the Members list. Choose from the following: <ul style="list-style-type: none"> • Restore — Restore the normal mode of the selected doors. • Disable — Disable the selected doors. • Unlock — Unlock the selected doors. • Lock — Lock the selected doors. • Facility Code — Specify the selected doors can be accessed by entering the facility code. • Card Only — Specify the selected doors can be accessed by card only.

Feature	Description
	<ul style="list-style-type: none"> • Pin Only — Specify the selected doors can be accessed by PIN only. • Card and Pin — Specify the selected doors can be accessed by using both card and PIN. • Card or Pin — Specify the selected doors can be accessed by using either card or PIN. <p>To add a door to the Members list, select a door from the Available list then click .</p>
If you select Door Grant in the Type field:	
Sub-Type	<p>No sub-type is required. The Door Grant action is performed on the doors in the Members list.</p> <p>To add a door to the Members list, select a door from the Available list then click .</p>
If you select Door Mask in the Type field:	
Sub-Type	<p>The selected option will be applied to the doors in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Mask Forced and Held — Mask the selected doors and hold that masked state until unmasked. • UnMask Forced and Held — Unmask the selected doors and hold that unmasked state until masked again. • Mask Held — Hold the masked state on the selected doors until the Unmask Held command is issued. • UnMask Held — Hold the unmasked state on the selected doors until the Mask Held command is issued. • Mask Forced — Force the selected doors to be masked. • UnMask Forced — Force the selected doors to be unmasked. <p>To add a door to the Members list, select a door from the Available list then click .</p>
If you select Policy Install/Uninstall in the Type field:	
Sub-Type	<p>The selected option will be applied to the policies in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Install — Install the policy selected in the Members window. • Uninstall — Uninstall this policy. <p>To add a policy to the Members list, select a input from the Available list then click .</p>
If you select Input in the Type field:	
Sub-Type	<p>The selected option will be applied to the inputs in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Unmask — Unmask the selected inputs. • Mask — Mask the selected inputs.

Feature	Description
	To add an input to the Members list, select an input from the Available list then click  .
If you select Output in the Type field:	
Sub-Type	<p>The selected option will be applied to the output in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • De-Activate — Deactivate the selected outputs. • Activate — Activate the selected outputs. • Pulse — Intermittently activate and deactivate the selected outputs. <p>To add an output to the Members list, select an output from the Available list then click .</p>
If you select Panel Install/Uninstall in the Type field:	
Sub-Type	<p>The selected option will be applied to the panel in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Install — Install the selected panels. • Uninstall — Uninstall the selected panels. <p>To add a panel to the Members list, select a panel from the Available list then click .</p>
If you select Access Group Install/Uninstall in the Type field:	
Sub-Type	<p>The selected option will be applied to the access group in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Install — Install the selected access groups. • Uninstall — Uninstall the selected access groups. <p>To add an access group to the Members list, select an access group from the Available list then click .</p>
If you select Schedule Set Mode in the Type field:	
Sub-Type	<p>The selected option will be applied to the schedule in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Off — Turn off the selected schedules. • On — Activate the selected schedules. • Scan — Manually activate and scan the selected schedules. <p>To add a schedule to the Members list, select a schedule from the Available list then click .</p>
If you select Email in the Type field:	
Email Address(es)	Enter the email addresses of the persons or organizations that you want to notify for this action.

Feature	Description
If you select Action Group in the Type field:	
Sub-Type	No sub-type is required. The Action Group option executes all the global actions in the Members list together. To add a global action to the Members list, select a global action from the Available list then click  .
	Click this button to save your changes.
	Click this button to discard your changes.

Global Actions - Edit Page

When you click the name of a global action from the Global Actions Listing page, the Global Action Edit page is displayed.

Make changes as required.

Feature	Description
Name	The name of the global action. Enter a descriptive name of the action.
Appliance	Select the appliance that the related panels and devices are connected to.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Type	Select the type of action you want to be performed. The additional options appear depending on the option you choose.

If you select Panel Macro in the Type field:




NOTE: Macros are only supported on Mercury panels.


Sub-Type	Select a macro group. You can choose Execute Group A to Execute Group D .
Macro	Select a specific macro.

If you select Exacq Soft Trigger in the Type field:


NOTE: You must set up an external system connection with an Exacq server to use this option.

Sub-Type	Select one of the following options: <ul style="list-style-type: none"> • Single Set — run the selected trigger once. • Continuous Set — repeat the selected trigger until the Unset command is
-----------------	---


Feature	Description
	<p>executed.</p> <ul style="list-style-type: none"> • Unset — stop the continuous repetition of the selected trigger.
Trigger	<p>Select the trigger action for this video server to perform, such as tilting, focusing or going to a preset position.</p> <p>Triggers are defined through the Exacq server.</p>
If you select Door Install/Uninstall in the Type field:	
Sub-Type	<p>Selected option will be applied to the doors in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Install — Install the doors in the Members list. • Uninstall — Uninstall the doors in the Members list. <p>To add a door to the Members list, select a door from the Available list then click .</p>
If you select Door Mode in the Type field:	
Sub-Type	<p>The selected option will be applied to the doors in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Restore — Restore the normal mode of the selected doors. • Disable — Disable the selected doors. • Unlock — Unlock the selected doors. • Lock — Lock the selected doors. • Facility Code — Specify the selected doors can be accessed by entering the facility code. • Card Only — Specify the selected doors can be accessed by card only. • Pin Only — Specify the selected doors can be accessed by PIN only. • Card and Pin — Specify the selected doors can be accessed by using both card and PIN. • Card or Pin — Specify the selected doors can be accessed by using either card or PIN. <p>To add a door to the Members list, select a door from the Available list then click .</p>
If you select Door Grant in the Type field:	
Sub-Type	<p>No sub-type is required. The Door Grant action is performed on the doors in the Members list.</p> <p>To add a door to the Members list, select a door from the Available list then click .</p>
If you select Door Mask in the Type field:	
Sub-Type	<p>The selected option will be applied to the doors in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Mask Forced and Held — Mask the selected doors and hold that masked state until unmasked.

Feature	Description
	<ul style="list-style-type: none"> • UnMask Forced and Held — Unmask the selected doors and hold that unmasked state until masked again. • Mask Held — Hold the masked state on the selected doors until the Unmask Held command is issued. • UnMask Held — Hold the unmasked state on the selected doors until the Mask Held command is issued. • Mask Forced — Force the selected doors to be masked. • UnMask Forced — Force the selected doors to be unmasked. <p>To add a door to the Members list, select a door from the Available list then click .</p>


If you select Policy Install/Uninstall in the Type field:

Sub-Type	<p>The selected option will be applied to the policies in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Install — Install the policy selected in the Members window. • Uninstall — Uninstall this policy. <p>To add a policy to the Members list, select a input from the Available list then click .</p>
-----------------	--

If you select Input in the Type field:







Sub-Type	<p>The selected option will be applied to the inputs in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Unmask — Unmask the selected inputs. • Mask — Mask the selected inputs. <p>To add an input to the Members list, select an input from the Available list then click .</p>
-----------------	---

If you select Output in the Type field:

Sub-Type	<p>The selected option will be applied to the output in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • De-Activate — Deactivate the selected outputs. • Activate — Activate the selected outputs. • Pulse — Intermittently activate and deactivate the selected outputs. <p>To add an output to the Members list, select an output from the Available list then click .</p>
-----------------	--

If you select Panel Install/Uninstall in the Type field:

Sub-Type	<p>The selected option will be applied to the panel in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> • Install — Install the selected panels.
-----------------	--

Feature	Description
	<ul style="list-style-type: none"> Uninstall — Uninstall the selected panels. <p>To add a panel to the Members list, select a panel from the Available list then click .</p>
If you select Access Group Install/Uninstall in the Type field:	
Sub-Type	<p>The selected option will be applied to the access group in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> Install — Install the selected access groups. Uninstall — Uninstall the selected access groups. <p>To add an access group to the Members list, select an access group from the Available list then click .</p>
If you select Schedule Set Mode in the Type field:	
Sub-Type	<p>The selected option will be applied to the schedule in the Members list. Choose from the following:</p> <ul style="list-style-type: none"> Off — Turn off the selected schedules. On — Activate the selected schedules. Scan — Manually activate and scan the selected schedules. <p>To add a schedule to the Members list, select a schedule from the Available list then click .</p>
If you select Email in the Type field:	
Email Address(es)	Enter the email addresses of the persons or organizations that you want to notify for this action.
If you select Action Group in the Type field:	
Sub-Type	<p>No sub-type is required. The Action Group option executes all the global actions in the Members list together.</p> <p>To add a global action to the Members list, select a global action from the Available list then click .</p>
	Click this button to save your changes.
	Click this button to discard your changes.

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. From the icon task bar, select **Physical Access > Global Linkages**.
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. From the icon task bar, select **Physical Access > Global Linkages**.
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.

Global Linkages - Listing Page



When you click **Global Linkages** from the Physical Access sub-options task bar, the Global Linkage Listing page is displayed. This page lists all the global linkage that have been configured in the system.

Feature	Description
Name	The name of the global linkage. Click the name to edit the global linkage.
Schedule	Indicates when this linkage is active.
Devices	Indicates the number of devices this linkage affects.
Events	Indicates the number of events that will trigger this linkage.
Tokens	Indicates the number of identity tokens that will be affected by this linkage.
Actions	Indicates the number of global actions that are triggered by one of the specified events.
Delete	Click  to delete the global linkage.

Feature	Description
Add New Global Linkage	Click this button to create a new global linkage.

Global Linkages - Add Page

When you click **Add New Global Linkage** from the Global Action Listing page, the Global Action Add page is displayed. The page allows you to start a new global linkage.

Feature	Description
Name	Enter a name for this new global linkage.
Appliance	Select the appliance that maintains this linkage.
Schedule	Define when this linkage is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Threshold	The length of time before the linkage will timeout because the chain of events is forced to stop or is broken. Enter the time in seconds. The default is 60 seconds (1 minute). For example: the global linkage is set to pulse an output on Panel A when an invalid access attempt occurs at a door on Panel B. But assume that Panel B is offline with the appliance at that moment. The appliance and Panel B comes back online ten minutes later and the event is then uploaded from the panel to the appliance. At that point, ten minutes or more after the fact, you may not want to pulse the output any longer.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Points Return	Check this box to indicate that the points defined in this linkage must return to normal before an action is triggered.
	Click this button to save your changes. After you save, the Global Linkage Edit page is displayed. For more information, see <i>Global Linkages - Linkage Page</i> on the facing page
	Click this button to discard your changes.



Global Linkages - Edit Screen

After you save a new global linkage or click the name of an existing global linkage from the listing page, the Global Linkage Edit screen is displayed. Refer to the following pages to learn more about the tabs that you can edit:

Global Linkages - Linkage Page

When you click the name of a global linkage from the Global Linkage Listing page, the Global Linkage Edit screen displayed the Linkage page. This page is also displayed after you save a new global linkage for the first time.





Feature	Description
Name	The name of this new global linkage.
Appliance	The appliance that maintains this linkage.
Schedule	When this linkage is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Threshold	The length of time before the linkage will timeout because the chain of events is forced to stop or is broken. Enter the time in seconds. The default is 60 seconds (1 minute). For example, consider a global linkage to pulse an output on Panel A when an invalid access attempt occurs at a door on Panel B. But assume that Panel B is offline with the appliance at that moment. The appliance and Panel B comes back online ten minutes later and the event is then uploaded from the panel to the appliance. At that point, ten minutes or more after the fact, you may not want to pulse the output any longer.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Points Return	Check this box to indicate that the points defined in this linkage must return to normal before an action is triggered.
Devices	A list of the devices that are associated with the global linkage. Devices are added to the linkage from the Devices page.
Events	A list of the events that are associated with the global linkage. Events are added to the linkage from the Events page.
Tokens	A list of the tokens that are associated with the global linkage. Tokens are added to the linkage from the Tokens page.
Actions	A list of the global actions that are associated with the global linkage. Global actions are added to

Feature	Description
	the linkage from the Actions page.
	Click this button to save your changes.
	Click this button to discard your changes.

Global Linkages - Devices Page

When you click the **Devices** tab on the Global Linkages Edit screen, the Global Linkage Devices page is displayed. This page allows you to add doors, inputs, outputs, specific panels, subpanels and external system devices to the global linkage.





Feature	Description
Name	The name of this new global linkage.
Appliance	The appliance that maintains this linkage.
Schedule	When this linkage is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Threshold	The length of time before the linkage will timeout because the chain of events is forced to stop or is broken. Enter the time in seconds. The default is 60 seconds (1 minute). For example, consider a global linkage to pulse an output on Panel A when an invalid access attempt occurs at a door on Panel B. But assume that Panel B is offline with the appliance at that moment. The appliance and Panel B comes back online ten minutes later and the event is then uploaded from the panel to the appliance. At that point, ten minutes or more after the fact, you may not want to pulse the output any longer.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Points Return	Check this box to indicate that the points defined in this linkage must return to normal before an action is triggered.
Type	Select the type of devices you want to add. The options in the Available list changes to match your selection. Tip: To add different types of devices to the linkage, select a type and add the required devices to the Members list then repeat this procedure with other device types until all required devices have been added to the Members list.

Feature	Description
Available	A list of the devices that are available in the system. The list changes to match the selected type. To add a device to the linkage, select a device from the Available list then click  .
Members	A list of all the devices that have been added to the linkage. To remove a device from the linkage, select a device from the Members list then click  .
Search	If the Available list includes enough options to require a scroll bar, the search option is displayed to help you find specific devices. <ol style="list-style-type: none"> 1. Enter your search term in the text field. Use wildcard characters if you are unsure of the device name. Check the Case-sensitive box to further narrow your search results. 2. Click Filter. The Available list updates to only show devices that match your search criteria. To restart your search, click Clear .
	Click this button to save your changes.
	Click this button to discard your changes.

Global Linkages - Events Page

When you click the **Events** tab on the Global Linkages Edit screen, the Global Linkage Events page is displayed. This page allows you to add specific events to the global linkage.

Feature	Description
Name	The name of this new global linkage.
Appliance	The appliance that maintains this linkage.
Schedule	When this linkage is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Threshold	The length of time before the linkage will timeout because the chain of events is forced to stop or is broken. Enter the time in seconds. The default is 60 seconds (1 minute). For example, consider a global linkage to pulse an output on Panel A when an invalid access attempt occurs at a door on Panel B. But assume that Panel B is offline with the appliance at that moment. The appliance and Panel B comes back online ten minutes later and the event is then uploaded from the panel to the appliance. At that point, ten minutes or more after the fact, you may not want to pulse the output any longer.
Partitions	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


Feature	Description
	partition, anyone with access to the system can edit the item. Only the partitions that have been defined in the system appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Points Return	Check this box to indicate that the points defined in this linkage must return to normal before an action is triggered.
Available	A list of all the available input events. The list changes to match the types of devices selected on the Devices page. To add an event to the linkage, select an event from the Available list then click  .
Members	A list of all the events that have been added to the linkage. To remove an event from the linkage, select an event from the Members list then click  .
Search	To help you find the specific events you want to add to the linkage, use the search feature. <ol style="list-style-type: none"> 1. Enter your search term in the text field. Use wildcards if you are unsure of the event name. 2. Click Filter. The Available list updates to only show events that match your search criteria. To restart your search, click Clear .
	Click this button to save your changes.
	Click this button to discard your changes.




Global Linkages - Tokens Page

When you click the **Tokens** tab on the Global Linkages Edit screen, the Global Linkage Tokens page is displayed. This page allows you to add identities with token numbers to the global linkage.

You must perform a search to locate specific identities and tokens.


Feature	Description
Name	The name of this new global linkage.
Appliance	The appliance that maintains this linkage.
Schedule	When this linkage is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Threshold	The length of time before the linkage will timeout because the chain of events is forced to stop or is broken. Enter the time in seconds. The default is 60 seconds (1 minute). For example, consider a global linkage to pulse an output on Panel A when an invalid access




Feature	Description
	attempt occurs at a door on Panel B. But assume that Panel B is offline with the appliance at that moment. The appliance and Panel B comes back online ten minutes later and the event is then uploaded from the panel to the appliance. At that point, ten minutes or more after the fact, you may not want to pulse the output any longer.
Partitions	<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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</p>
Points Return	Check this box to indicate that the points defined in this linkage must return to normal before an action is triggered.
Token Search	<p>Search for the identity that is assigned to the token you want to include in this linkage. After you click Search, the Available list refreshes to display your search results.</p> <p>If you only know the identity's name, enter the identity's Last Name, First Name then click Search.</p> <p>If you know the internal token number, enter it in the Internal Number field then click Search.</p> <p>If you only know the identity's group, enter it in the Group field then click Search.</p> <p>If you are unsure of the name, group or internal token number, use wildcard characters, use one of the following drop down list options, or the Advanced search (see Search Field below) to help you refine your search:</p> <ul style="list-style-type: none"> • Starts With — the identity name starts with the characters that you've entered. • Equals — the identity name is exactly the same as what you have entered. • Contains — the identity name includes all of the characters you've entered. • Ends With — the identity name ends with the characters that you've entered. • And — the identity has this last name and is also part of the selected group. • Or — the identity has this last name or is part of the selected group. <p>To restart your search, click Clear Search.</p>
Search Field	<p>If the Token Search did not locate the identity you want, add extra search fields in the Advanced Search area.</p> <ol style="list-style-type: none"> 1. In the Search Field drop down list, select one of the search options. 2. Select or enter the Search Value. The Search Value option changes depending on the selected Search Field. 3. Click Add Criteria to add a new Search Field line. 4. Click Search. <p>To restart your search, click Clear Search. To remove an added Search Field line, click Remove.</p>
Available	<p>A list of the identities and tokens that match your search criteria. No tokens are listed if you do not perform a search.</p> <p>To add an identity to the linkage, select the identity from the Available list then click .</p>

Feature	Description
Members	A list of all the identities and tokens that have been added to the linkage. To remove an identity from the linkage, select an identity from the Members list then click  .
	Click this button to save your changes.
	Click this button to discard your changes.

Global Linkages - Actions Page

When you click the **Actions** tab on the Global Linkages Edit screen, the Global Linkage Actions page is displayed. This page allows you to add identities with token numbers to the global linkage.

Feature	Description
Name	The name of this new global linkage.
Appliance	The appliance that maintains this linkage.
Schedule	When this linkage is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Threshold	The length of time before the linkage will timeout because the chain of events is forced to stop or is broken. Enter the time in seconds. The default is 60 seconds (1 minute). For example, consider a global linkage to pulse an output on Panel A when an invalid access attempt occurs at a door on Panel B. But assume that Panel B is offline with the appliance at that moment. The appliance and Panel B comes back online ten minutes later and the event is then uploaded from the panel to the appliance. At that point, ten minutes or more after the fact, you may not want to pulse the output any longer.
Points Return	Check this box to indicate that the points defined in this linkage must return to normal before an action is triggered.
Available	A list of the available global actions. To add a global action to the linkage, select the global action from the Available list then click  .
Members	A list of the global actions that have been added to the linkage.

Feature	Description
	To remove a global action from the linkage, select the global action from the Members list then click  .
	Click this button to save your changes.
	Click this button to discard 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 *Areas - Adding* on page 186.
2. To organize related areas together, you can combine them into groups. For more information, see *Groups - Introduction*.
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. For more information, see *Access Groups - Access Group Add page* on page 372.
5. Assign the access group to a role that would need access to the mustering area. For more information, see *Assigning an Access Group to a Role* on page 346.

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. For more information, see *Identities - Roles Page* on page 293.


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. From the Setup links area, select **Settings > Maps**.
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 .

For more information, see *Maps - Add Page* on page 420.

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:

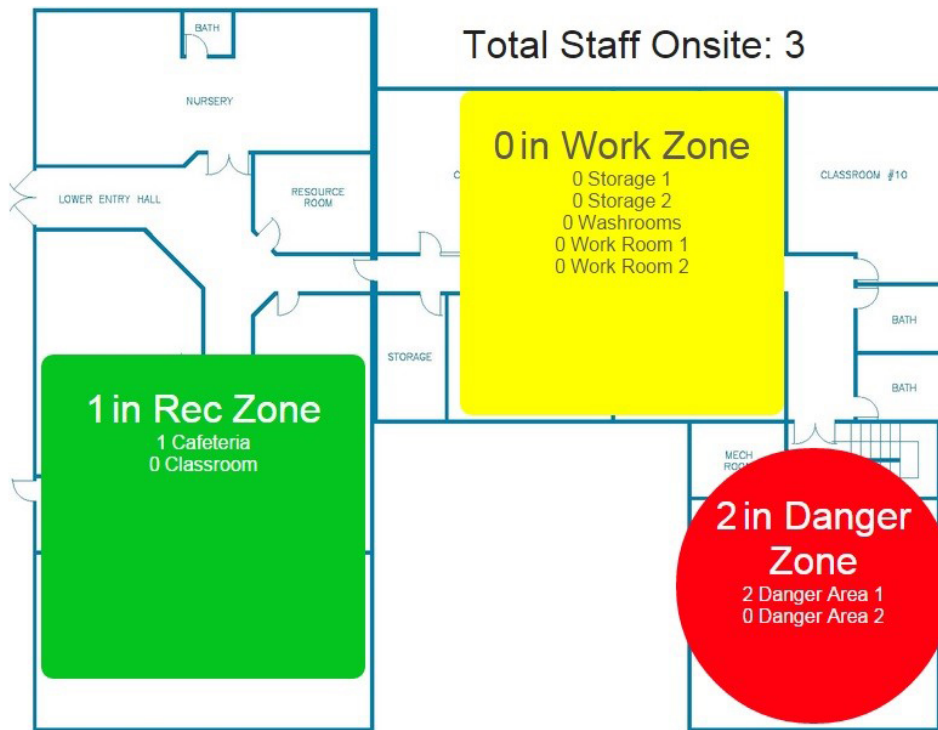
- a. In the **Area Group/Area** drop down list, select the muster area this dashboard element represents. You can select a specific area or a group of areas.
 - b. From the **Graphic Shape** drop down list, select Circle or Square.
 - c. Click the **Graphic Color** field to change the graphic shape color.
 - 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 410.

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. From the icon task bar of the home page, 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. For more information, see *Reports - Area Identity* on page 428.


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. In the icon task bar, select **Identities > Identity Name**.

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  .

Settings - Main Page

When you click or mouse-over the **Settings** option in the setup links, the following options are displayed:

- [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.
- [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 schedule 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 holidays.

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. From the Setup links area, select **Settings > Schedules**.
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. From the Setup links area, select **Settings > Schedules**.
2. From the Schedules Listing page, click the name of the schedule you want to edit.
3. Edit the schedule as required. For more information, see *Schedules - Edit Page* on page 228.
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. From the Setup links area, select **Settings > 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. From the Setup links area, select **Settings > Holidays**.
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. Define how you want the holiday to be activated.
 - Allow the system to automatically disable all schedules on the date of the holiday — leave the **Preserve schedule days** check box *clear*. Only schedules that include the holiday will be active on the date of the holiday.
 - The holiday remains inactive unless it is assigned to a schedule — check the **Preserve schedule days** box. The holiday must be assigned to a schedule to initiate any special actions. Any other active schedule remains active on the holiday.
7. Click  to save the new holiday.

Holidays - Editing

1. From the Setup links area, select **Settings > Holidays**.
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. For more information, see *Holidays - Edit Page* on page 230.
4. Click  to save your changes.

Holidays - Deleting


1. From the Setup links area, select **Settings > Holidays**.
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**.

Schedules - Listing Page

When you select **Settings > Schedule** from the Setup links area, the Schedules Listing page is displayed.

The two default system schedules are Never Active and 24 Hours Active.



The Schedule Listing page displays the following details about each schedule:

Feature	Description
Name	The name of the schedule. Click the name to edit the schedule. For more information, see <i>Editing Schedules</i> on page 225.
Mode	Identifies the current status of the schedule. <ul style="list-style-type: none"> Green (ON) indicates the schedule is always active, overriding any specific date or time settings. Yellow (SCAN) indicates the schedule is active and is relying on the system time settings to initiate scheduled actions. Most schedules would be using this setting. Red (OFF) indicates the schedule is inactive.
Delete	Click  to delete the selected schedule. For more information, see <i>Deleting Schedules</i> on page 225. NOTE: You cannot delete the default system schedules.
Add New Schedule	Click this button to create a new schedule. For more information, see <i>Adding Schedules</i> on page 225.
Create New Report	Click this button to generate a report of the schedules on the listing page. For more information, see <i>Reports - Schedule</i> on page 442.

Schedules - Add New Page

When you click the **Add New Schedule** button from the Schedule Listing page, the Schedule Add New page is displayed.

Feature	Description
Name	Enter a meaningful name for the schedule.
Mode	Select the mode from the drop down list. The options include: <ul style="list-style-type: none"> ON – the schedule is constantly on. You do not need to set specific dates or times for the schedule. OFF – the schedule off. SCAN – the schedule follows the date and time settings defined through the check boxes below.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Days of the	Specify the days of the week that the schedule is active. Check the boxes for each day the



Feature	Description
week Sun, Mon, Tue, Wed, Thu, Fri, Sat	schedule is active.
Holidays 1, 2, 3, 4, 5, 6, 7, 8	Specify the holidays that the schedule is active. Holidays are assigned a number in the Access Control Manager system. Each number represents a different type of holiday that is configured.
Active	Enter when the schedule starts for the days in each row. You must use 24 hour clock format (for example, 1:00 p.m. is 13:00 in the 24-hour clock format). NOTE: If 09:00 is entered as the Active time, the actual active time will be 09:00:00.
Inactive	Enter when the schedule ends for the days in each row. You must use 24 hour clock format. NOTE: 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.
	Click this button to save your changes.
	Click this button to discard your changes.

Schedules - Edit Page

When you click the name of a schedule from the Schedule Listing page, the Schedule Edit page is displayed.

Make any changes that are required.

Feature	Description
Name	The name of the schedule.
Mode	Select the mode from the drop down list. The options include: <ul style="list-style-type: none"> • ON – the schedule is constantly on. You do not need to set specific dates or times for the schedule. • OFF – the schedule off. • SCAN – the schedule follows the date and time settings defined through the check boxes below.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Days of the	Specify the days of the week that the schedule is active. Check the boxes for each day the


Feature	Description
week Sun, Mon, Tue, Wed, Thu, Fri, Sat	schedule is active.
Holidays 1, 2, 3, 4, 5, 6, 7, 8	Specify the holidays that the schedule is active. Holidays are assigned a number in the Access Control Manager system. Each number represents a different type of holiday that is configured.
Active	Enter when the schedule starts for the days in each row. You must use 24 hour clock format (for example, 1:00 p.m. is 13:00 in the 24-hour clock format). NOTE: If 09:00 is entered as the Active time, the actual active time will be 09:00:00.
Inactive	Enter when the schedule ends for the days in each row. You must use 24 hour clock format. NOTE: 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.
	Click this button to save your changes.
	Click this button to discard your changes.

Holidays - Listing Page

When you select **Settings > Holidays** from the Setup links area, the Holidays Listing page is displayed. The Holiday Listing page lists all of the holidays that have been defined for the system.

A holiday is a specific day (or days) that may be an exception to the regular schedule. Each holiday is assigned a number so that it can be added to a schedule. You can define the priority of each number as a specific holiday type within your organization.

The Holiday Listing page lists holidays in chronological order. The listing page displaying the following details for each holiday:



Feature	Description
Name	The name of the holiday. Click the name to edit the holiday. For more information, see <i>Holidays - Editing</i> on page 226.
Date	The date of the holiday.
Type	The holiday type number.
Delete	Click  to delete the holiday. For more information, see <i>Holidays - Deleting</i> on page 226.
Add New Holiday	Click this button to add a new holiday. For more information, see <i>Holidays - Adding</i> on page 226.
Create New	Click this button to generate a report of the holidays on the listing page. For more

Feature	Description
Report	information, see Holidays - Create Report.

Holidays - Add New Page

When you click the **Add New Holiday** button from the Holidays Listing page, the Holiday Add page is displayed.



On this page, you can add a new holiday and assign a holiday type number.

Feature	Description
Name	Enter a name for the holiday.
Date	Enter the date of the holiday for this year. Click the Date field to display the pop-up calendar and select the date, or enter it in this format: MM/DD/YYYY NOTE: You will need to update the date of the holiday each year.
Additional Days	Enter the number of consecutive days this holiday covers. A setting of 0 indicates that the holiday only spans the one date.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Type	Assign a holiday type number. The holiday type number allows you to group specific types of holidays together. The priority of the number is defined externally by your organization and does not affect how the system handles the holiday. For example, you can define 1 as a government holiday, 2 as a cultural holiday and 3 as company holiday. Once you define the holiday type numbers, you can create schedules that match the level of access required for each of these holiday types.
Preserve schedule days	Check this box to indicate that the holiday will only be active when it is assigned to a schedule. If this box is clear, the system automatically deactivates all schedules that this holiday is not part of on the date of the holiday.
	Click this button to save your changes.
	Click this button to discard your changes.

Holidays - Edit Page

When you click the name of a holiday from the Holiday Listings page, the Holiday Edit page is displayed. From this page, you can edit the date of the holiday and the holiday type number.

Make any changes as required.

Feature	Description
Name	The name of the holiday.
Date	The date of the holiday for this year. Click the Date field to display the pop-up calendar and select the date, or enter it in this format: MM/DD/YYYY NOTE: You will need to update the date of the holiday each year.
Additional Days	The number of consecutive days this holiday covers. A setting of 0 indicates that the holiday only spans the one date.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Type	The holiday type number. The holiday type number allows you to group specific types of holidays together. The priority of the number is defined externally by your organization and does not affect how the system handles the holiday. For example, you can define 1 as a government holiday, 2 as a cultural holiday and 3 as company holiday. Once you define the holiday type numbers, you can create schedules that match the level of access required for each of these holiday types.
Preserve schedule days	Check this box to indicate that the holiday will only be active when it is assigned to a schedule. If this box is clear, the system automatically deactivates all schedules that this holiday is not part of on the date of the holiday.
	Click this button to save your changes.
	Click this button to discard your changes.

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 large number of event types are defined by default but you can add or delete event types as needed.

Adding Event Types

1. From the Setup links area, select **Settings > Event Types**.
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.

For more information, see *Event Types - Add New Page* on the next page.

6. Click  to save the new event type.

Editing Event Types


1. From the Setup links area, select **Settings > Event Types**.
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.

For more information, see *Event Types - Edit Page* on page 234.

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. From the Setup links area, select **Settings > 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**.



Event Types - Listing Page






When you select **Settings > Event Types** from the Setup links area, the Event Types Listing page is displayed.

The Event Types Listing page displays a list of all the event types that are currently defined in the system.

Event types provide instructions on how to handle an event generated in the Access Control Manager system. For example, you can create an event type that displays color-coded event message text on the event viewer and plays a sound in the alarm monitor.

The Event Types Listing page displays the following information about each event type:

Feature	Description
Name	The name of the event type. Click the name to edit the event type. For more information, see <i>Editing Event Types</i> above.
Masked	Indicates if all events in this event type are masked. <ul style="list-style-type: none">•  all events in this event type are masked.•  all events in this event type are not masked. Click the icon to change the masking status.
Logged	Indicates if all events in this event type are logged.



Feature	Description
	<ul style="list-style-type: none">  all events in this event type are logged.  all events in this event type are not logged. <p>Click the icon to change the logging status.</p>
Alarm	<p>Indicates if all events in this event type generate an alarm.</p> <ul style="list-style-type: none">  all events in this event type generate an alarm.  all events in this event type do not generate an alarm. <p>Click the icon to change the alarm status.</p>
Delete	<p>Click  to delete the event type.</p> <p>For more information, see <i>Deleting Event Types</i> on the previous page.</p> <p>NOTE: System default event types cannot be deleted.</p>
Add New Event Type	<p>Click this button to add a new event type.</p> <p>For more information, see <i>Adding Event Types</i> on page 231.</p>
Create New Report	<p>Click this button to generate a report of the event types on the listing page.</p> <p>For more information, see <i>Reports - Event Type</i> on page 436.</p>

Event Types - Add New Page

When you click **Add New Event Type** from the Event Types Listing page, the Event Type: Add New page is displayed.

This page allows you to add a new event type to the system.



Feature	Description
Name	Enter a name for the event type.
Suppress Schedule	Select a schedule when events are not reported. Only schedules that have been defined in the system are listed.
Priority	Specify the priority of this event type. The Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
Masked	Check this box to indicate that this event type is masked.
Logged	Check this box to indicate that this event type is logged.
Alarm	Check this box to indicate that this event type generates an alarm.
Email	Enter an email to receive notifications about this event type. You can enter more than one email address separated by a comma.
Instructions	Enter instructions about how events of this type should be handled.

Feature	Description
	These instructions are provided with the event on the monitor screens.
	Click this button to save your changes.
	Click this button to discard your changes.

Event Types - Edit Page

When you click an event type name from the Event Types Listing page, the Event Type Edit page is displayed.

Make any changes that are required.

Feature	Description
Name	The name of the event type.
Suppress Schedule	Select a schedule when events are not reported. Only schedules that have been defined in the system are listed.
Priority	Specify the priority of this event type. The Alarm Monitor displays alarms according to their priority. Priority 1 is the highest priority and is always displayed at the top. The priority range is 1 - 999.
Masked	Check this box to indicate that this event type is masked.
Logged	Check this box to indicate that this event type is logged.
Alarm	Check this box to indicate that this event type generates an alarm.
Send Email to	Enter an email to receive notifications about this event type. You can enter more than one email address separated by a comma.
Instructions	Enter instructions about how events of this type should be handled. These instructions are provided with the event on the monitor screens. You can use the resizing handle in the lower right corner to make this pane larger or smaller to see your instructions more clearly.
	Click this button to save your changes.
	Click this button to discard your changes.

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. For more information, see *Badge Designer - Add DB Field* on page 253.

User defined fields can also be used for advanced searching for identities. For more information, see *Searching for an Identity* on page 282.

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. From the Setup links area, select **Settings > 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. See *Adding an Identity Profile* on page 302 and *Identity Profiles - Batch Update* on page 305 for more detail.

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. From the Setup links area, select **Settings > User Fields**.
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. For more information, see *User Defined Tabs - Add Page* on page 238.


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. From the Setup links area, select **Settings > User Fields**.
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. For more information, see *User Defined Tabs - Edit Page* on page 238.
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. From the Setup links area, select **Settings > 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. From the Setup links area, select **Settings > 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 Defined Fields - Listing Page

When you select **Settings > User Fields** from the Setup links area, the User Defined Fields Listing page is displayed.



This page lists all the user defined fields in the system.

Feature	Description
Name	The name of the user defined field.
Type	This read-only column indicates what type of field this is.
Delete	Click  to delete the user defined field. You can only delete fields that are not part of a user defined tab. For more information, see <i>User Defined Fields - Deleting Fields</i> on the previous page.
Add New User Defined Field	Click this button to add a new user defined field to the system. For more information, see <i>Adding a User Defined Field</i> .
Create New Report	Click this button to generate a report of the user defined fields on this listing page.

User-Defined Fields - Add New Page

When you click **Add New User Defined Field** from the User Defined Fields Listing page, The User Defined Field: Add New page is displayed.


This field allows you to add a new field to the Identity page. The new field can be a string of words, numbers, a check box or date.

Feature	Description
Name	Enter a name of this user-defined field. This also becomes the label of the field. Consider how the field will be read when it is displayed on the Identities page.
Type	Select the field type. The options are: <ul style="list-style-type: none">• 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. Check the box to indicate "yes", and clear the box to indicate "no".• Date — the field supports a date only. Click the field to display a calendar then select a date.
	Click this button to save your changes. NOTE: Once you save the user defined field, you cannot edit the field again.
	Click this button to discard your changes.

User Defined Tabs - Listing Page


When you select the **Tabs** tab from the User Defined Fields Listing page, the User Defined Tabs Listing page is displayed.

This page displays all the tabs that user defined fields can be organized into.

Feature	Description
Name	The name of the user defined tab. Click the name to edit the tab. For more information, see <i>User Defined Fields - Editing User Defined Tabs</i> on page 236.
# Fields	The number of user defined fields that are displayed by the tab.
Delete	Click  to delete the tab. For more information, see <i>User Defined Fields - Deleting Fields</i> on page 236.
Add New User Defined Tab	Click this button to add a new tab. For more information, see <i>User Defined Fields - Adding User Defined Tabs</i> on page 235.
Create New Report	Click this button to generate a report of the tabs listed on this page.

User Defined Tabs - Add Page

When you click **Add New User Defined Tab** from the User Defined Tab Listing page, the User Defined Tab: Add New page is displayed.




Enter a name for the tab then click  to save the new tab.


After the page refreshes to display the User Defined Tabs Edit page, add the user defined fields that you want to be available in this tab. For more information, see *User Defined Tabs - Edit Page* below.

User Defined Tabs - Edit Page

When you click the name of a tab from the User Defined Tab Listing page, the Edit page is displayed. This page is also displayed immediately after you save a new tab.

Make any changes that may be required on this page.

Feature	Description
Name	The name of the tab.
Available	A list of user defined fields that have been added to the system. To add a field to this tab, select a field from the Available list then click  to add the field to the Members list.
Members	A list of user defined fields that are members of this tab. To remove a field from this tab, select a field from the Members list then click  .
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.



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. From the Setup links area, select **Settings > User Lists**.
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. From the Setup links area, select **Settings > User Lists**.
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. From the Setup links area, select **Settings > User Lists**.
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.

User Lists - User-Defined Lists

When you select **Settings > User Lists** from the Setup links area, the User Defined Lists Listing page is displayed.





This page includes all the list values that appear on the Identity page. You can edit what options are available in each list but you cannot add or delete lists.

Feature	Description
Name	The name of the Identity option that you can modify. Click the name to edit the user defined list options. For more information, see <i>User Lists - Editing Items</i> on the previous page.
Record Count	The total number of options that are in each list.
Create New Report	Click this button to generate a PDF report of all the user defined list values.

User Lists - User List Edit Screen

When you click the name of a list from the User Defined Lists Listing page, the User List Edit screen is displayed.

This page allows you to add custom values to the list field on the Identities page.

Feature	Description
Name	The name of the list field.
New Value	Enter a new option for the list then click  .
Current Values	A list of the options that are currently available in the list field. Select one of the list options then click  to delete the option.
	Click this button to save your changes.
	Click this button to discard your changes.

System Settings






When you select **Settings > System Settings** from the Setup links area, 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 Setup links area, select **Settings > 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 panels. Enhanced access levels allow Mercury panels to accept more access groups per token.
Identity Auto Increment Field	Check this box to enable the system to automatically increments the read-only Sequence Number field on the Identity page. This option is disabled by default. NOTE: The system will only apply this setting to new identities.
Identity Auto Increment Start	If you enabled Identity Auto Increment, enter the number the system will start counting from then click  . The default value is 1. NOTE: The system will only apply this setting to new identities.
Identity Auto Increment Step	If you enabled Identity Auto Increment, enter the value the system uses to increment the sequence number then click  . 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.). NOTE: The system will only apply this setting to new identities.
Language	Select a language that the system will display by default. Each user with access to the Access Control Manager system will be able to set their own language preferences from the My Account page. Click Translate Default Data to translate all of the system default values into the selected language. It is recommended that you only perform this action once, or your reports and logs will display values in multiple languages.
Maximum Active Tokens	Enter the maximum number of tokens that can be active per identity then click  .
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	Enter a title you want to use for the system then click  . The title is displayed under the Access Control Manager banner on each screen, and the title is used for all messages sent by the system.
System Support	Enter the contact details of your Avigilon support representative then click  .

Feature	Description
	This information is displayed when a user clicks Support .
Token Expiration Time	Enter the default number of days before a token expires then click  .
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 Active Directory (AD) to authenticate users that need access to the system. This allows users to use their local domain username and passwords to access the system, and will not need a separate password configured in the Access Control Manager. However, user access permissions are still based on the roles they are assigned within the Access Control Manager.

To use remote authentication, you need to add one or more AD servers to the system and enable remote authentication. 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. A default domain for remote authentication can still be configured. This domain will be used for any identities that do not have a domain configured for them.


To confirm that remote servers are valid and not an imposter, you can add certificates to the system to validate each AD server that is used for remote authentication.





System Settings - Configuring Remote Authentication


Requirements:

- Windows domain controller, with TLS encryption activated.
- The IP address of your domain's DNS server.
- Active Directory Certificate Services.
- An export of the Domain Controller's CA certificate in Base-64 encoded X.509 (.CER) format. You will need to change the export file extension to `.pem` before you upload it 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 Setup links area, click **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 Setup links area, select **Settings > System Settings**.
5. Select the **External Domains** tab.
6. Click **Add New External Domain**.

7. On the External Domain: Add New page, enter a name for this external domain.
8. In the **New 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 New 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.
17. In the **Default Domain** drop down list, select the domain you just added in the ExternDomains tab.
18. In the **Default Server** field, enter the full DNS name of your domain controller.
19. Select the **Validate Certificates** check box.
20. Click .
21. Reboot the appliance. You must restart the appliance before the changes take effect.
22. Repeat the previous steps on each appliance in your system that requires remote authentication.
23. Enable remote authentication for each identity that will be logging into the Access Control Manager 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 **Remote Domain** drop down list, select the external domain that you added earlier.
 - d. In the 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`
 - e. Click .



Next time the user logs in to the Access Control Manager appliance, they will need to use `username@domain.org` as their login name, and the password that is stored in the Active Directory server.

System Settings - Remote Authentication

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

This page 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	Select a domain from the drop down list.


Feature	Description
Domain	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 Certificates	<p>Check this box to enable the system to validate all certificates from the server before use.</p> <p>To use this feature, you must upload a certificate that the system can use for the validation process. For information on importing and using certificates, see <i>System Settings - Certificates Listing Page</i> on the next page.</p> <p>If this setting is changed, you must reboot the appliance for the change to take affect.</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 of the values on this page.

System Settings - External Domains Listing Page

When you select the **External Domains** tab from the System Settings page, the External Domains Listing page is displayed.





This page lists any external domains that have been added to the system. You must add the external domain before you can use remote authentication.

You can grant remote authentication access to individual identities from the Identity page. For more information, see *Identities - Identity Page* on page 292.

Feature	Description
Name	<p>The name of this external domain.</p> <p>Click the name to edit the external domain. For more information, see <i>System Settings - External Domains Edit Page</i> on the next page.</p>
Delete	Click  to delete the selected external domain.
Add New External Domain	Click this button to define a new external domain. For more information, see <i>System Settings - External Domains Add Page</i> below.
Create New Report	Click this button to generate a PDF report of the listed domains.
Certificates	<p>Click this button to access the Certificates Listing page.</p> <p>From this page you can upload one or more certificates to give remote browsers access to the Access Control Manager.</p>

System Settings - External Domains Add Page





When you click **Add New External Domain** from the External Domains Listing page, the External Domain: Add New page is displayed.

Feature	Description
Name	Enter the name of this external domain.
New Server	Enter the IP address or host name of a server in the external domain then click  .
Current Servers	New servers are automatically added to this list of servers in the domain.
	Select a server from the list then click this button to remove the server from the list.
	Click this button to save your changes.
	Click this button to discard your changes.

System Settings - External Domains Edit Page

When you click the name of a domain from the External Domains Listing page, the External Domains: Edit page is displayed.


Make any changes that are required.

Feature	Description
Name	Edit the name of this external domain as required.
New Server	Enter the IP address or host name of a new server in the domain then click  .
Current Servers	The list of servers currently included in this external domain.
	Select a server from the list then click this button to remove the server from the list.
	Click this button to save your changes.
	Click this button to discard your changes.

System Settings - Certificates Listing Page

When you click **Certificates** from the External Domains Listing page, the Certificates Listing page is displayed.

Certificates that have been uploaded to the system are listed on this page. Certificates are used by browsers to confirm that systems are safe for users to access.



Feature	Description
Name	The name of the certificate file.
Size	The size of the certificate file.
Upload Date	The date the file was uploaded.
	Click this button to delete the certificate.
Add New Certificates Listing	Click this button to upload a new certificate for this external domain.

Certificate Upload Page

Use this page to upload an external domain server certificate to the Access Control Manager application. This allows the system to authenticate users through an Active Directory server on an external domain.

The certificates must be in .PEM format, but can be exported from Windows in .CER format then renamed to use the .PEM extension.

There must be a certificate for every server that has been added to the system as part of the external domain.

Feature	Description
Upload Certificate file:	Click Browse to locate and select the certificate in the Choose File to Upload dialog box.
	Click this button to save your changes.
	Click this button to discard your changes.

Badge Templates - Introduction

A badge template is a format designed by a qualified operator that is used to generate a physical badge. Using this procedure, an enrollment officer or administrator can:

- Enroll an employee using the Identities feature.
- Assign the new employee to a specific badge template.
- Generate (print) a badge with 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.

The Avigilon Access Control Manager application automatically supplies such fields as photos and data with the relevant information taken from the Identities database. Other fields, such as backgrounds, graphics, and text are static and are applied to every badge. In addition, the application can change 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.

Once you have created one or more badge templates, you can assign them to a user at **Identities > Badge**.

Using Badge Templates

The Badge Designer is used to design badge templates. You can add photos, logos, text, and database fields to badge templates and define the layout. Once you assign a badge template to an identity, you can create a badge that is auto-populated with the identity's details.

Adding a Badge Template

Badge templates are used to define the layout of badges or cards that are used to access doors within your access control system. Each badge template is filled with placeholders that automatically pull the required information from each identity the template is assigned to.

To add a new badge template to the system, complete the following steps:

1. From the Setup links area, select **Settings > Badge Designer**.
2. On the Badge Templates Listing page, click **Add New Badge Template**.
3. On the following page, give the badge template a name.
4. Enter the size of the badge in pixels.
5. Click the **BG Color** field to select a different background color.

When the color palette is displayed, select a color from the palette or manually enter the color in RGB, HSV or hex code format.

6. In the **Opacity** field, define how opaque you want the background color to be.
7. If the badge or card will be double-sided, check the **Two Sided** check box.

NOTE: Only printers that support double-sided printing will be able to print two-sided cards.

If you selected the Two Sided option, click **Back Side** at any time to add elements to the back of the badge or card.



8. Add the required badge layout elements.

The elements are placeholders that define what type of information will be used for each identity badge or card.


- Click **Add Picture** to add a photograph of the identity to the badge. You can only add one picture to the badge template. For more information, see *Badge Designer - Add Picture* on page 253.
- Click **Add Graphic** to add any other type of image to the badge. This can include a logo or icon. For more information, see *Badge Designer - Add Graphic* on page 256.
- Click **Add DB Field** to add specific information about the identity, like their name or department. For more information, see *Badge Designer - Add DB Field* on page 253.
- Click **Add Text** to add a line of text, like the company name or a slogan. For more information, see *Badge Designer - Add Text* on page 255.

9. Define the size and location of each element.

- If you can adjust the size of the element, manually enter the size in pixels.
- To move the element, you can click and drag the element on the canvas or manually enter the location in pixels. 0 x 0 would place the element in the top left corner.



10. To remove an element from the canvas, click  beside the element details.
11. Click  to save your changes and update the preview.

Editing a Badge Template


1. From the Setup links area, select **Settings > Badge Designer**.
2. On the Badge Template Listing page, click the name of the badge template that you want to edit.
3. Make any changes that are required. For more information, see *Badge Designer - Add and Edit Page* on page 251.
4. Click  to save your changes and update the preview.

Duplicating a Badge Template

You can duplicate an existing badge template instead of creating one from scratch.

1. From the Setup links area, select **Settings > Badge Designer**.
2. On the Badge Template Listing page, click  for the badge template that you want to duplicate.
The Badge Template Listing page refreshes to display a duplicate.
3. Click the name of the duplicate.
4. Rename the badge template.
5. Edit the details as required, then click  to save your changes and update the preview. For more information, see *Badge Designer - Add and Edit Page* on page 251.

Deleting a Badge Template

1. From the Setup links area, select **Settings > Badge Designer**.
2. Click  for the badge template that you want to delete.
3. When the browser displays a pop-up message to ask *Are you sure?*, click **OK**.

Badge Designer - Changing the Badge Background Color

When you open a new badge template or edit an existing one, the canvas background data fields appear at the top of the left column like this example:

Name:

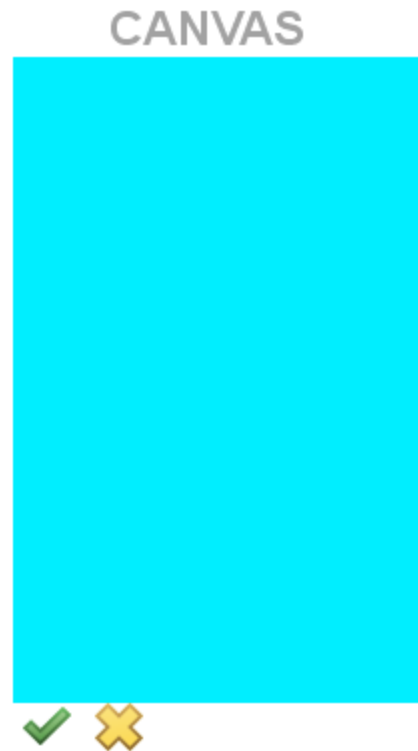
Size: x

BG Color:

Opacity: %

Partitions:

Two Sided:



To change the background color and opacity:

1. Click on the **BG Color** box.
The color palette appears.
2. Change the color as required then click **Close Window** in the upper right corner to return to the canvas.
3. In the **Opacity** text box, enter the percentage of opacity you require for this background color.
4. When you are certain of your color and opacity, click .

The canvas background changes and the preview pane appears with the changes reflected.

Color Palette

When you click a color field, like the Badge Designer background feature, the color palette appears like this example:



To use this palette to select a specific color:

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

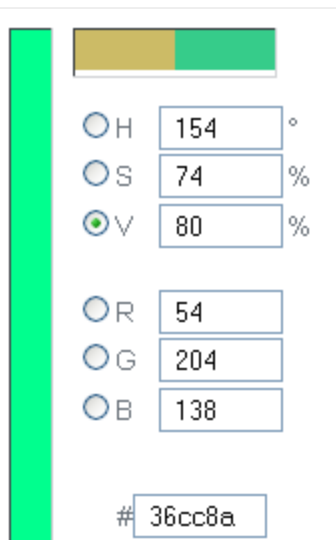
All possible tints and variations of this color appear to the left in the tint area.

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.


2. 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.

3. If required, slide up or down the vertical slide bar to change the color still further.
4. When you're finished with this palette, click **OK**.
5. Click the  icon to impose the new color on the canvas or other element.

Badge Templates - Listing Page

When you select **Settings > Badge Designer** from the Setup links area, the Badge Templates Listing page is displayed.


This page lists all the badge templates that have been added to the system.

Feature	Description
Name	The name of the badge template. Click the name to edit the badge template. For more information, see <i>Editing a Badge Template</i> on page 248.
Commands	Click  to delete the badge template. For more information, see <i>Deleting a Badge Template</i> on page 248. Click  to copy the badge template. The copy of the badge template is automatically added to the top of the list.
Add New Badge Template	Click this button to add a new badge template. For more information, see <i>Adding a Badge Template</i> on page 247.


Badge Designer - Add and Edit Page

When you click the **Add New Badge Template** button or the name of a badge template from the Badge Template Listing page, the Badge Template Edit page is displayed.

Tip: You must save your changes before it is shown in the preview.

Feature	Description
Canvas	This displays the current layout of your badge template. Click and drag elements on the canvas to define their location on the badge.
Preview	The preview below the canvas displays how the badge layout would appear on a finished badge. You must save your changes before some items are displayed in the preview.
Name	Enter a name for this badge template.
Size	Enter the size of this badge template in pixels. The first box defines the width, the second box specifies the length.
BG Color	Click this field to choose a background color for the badge. When the color palette is displayed, select a color from the palette or manually enter the color in RGB, HSV or hex code format.
Opacity	Enter how opaque you want the background color to be. 0% is transparent and 100% is a opaque.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Two Sided	Check this box to set this as a double sided template. Only those badge printers capable of printing on both sides can accommodate this setting.
Back Side Front Side	If this is a Two Sided template, click Back Side at the top of the page to configure the back side of the badge template. To return to the front side of the badge template, click the Front Side button. The front side of the template is displayed by default.
Add Picture	Click this button to add space for a photo on to the badge template. Use this option to add the photo of an identity.
Add DB Field	Click this button to add a database field on to the badge template. Use this option to add an identity detail. For example if you add the First Name data field, the identity's first name is automatically added to the layout location when you print a badge based on this template.
Add Text	Click this button to add display text on to the badge template. Use this option to add a line of text, like the company name or slogan.
Add Graphic	Click this button to add an image to the badge template. Use this option to add any image that is not a photo of an identity, like a logo or emblem.
	Click this button to save your changes. You must save your changes before it is shown in the preview.






Feature	Description
	Click this button to discard your changes.

Badge Designer - Add Picture

When you add a picture to a badge template, you are adding a placeholder for a photo of the identity when this badge template is used.

After you click **Add Picture** on the Badge Designer Edit page, a photo object is added to the canvas and the following options are displayed:



Feature	Description
Photo	Click Photo to show or hide the following options. Click  to delete the object from the canvas.
Layer Order	Enter a number to indicate where the object appears when objects are stacked on top of each other. 1 is the bottom layer, 2 is on top of 1 and so on.
Location	Enter where the object appears on the canvas. 0 x 0 would place the object in the top left corner, while 80 x 160 would place the object in the bottom right corner. You can also set the location by click and dragging the object on the canvas.
Dimensions	Enter the size of the object. The first field is the width and the second field is the height.
Rotation	Select the number of degrees to rotate this object clockwise. The default is 0 degrees.
Maintain Aspect	Check this box to always maintain the aspect ratio of the photo. If this option is disabled, the photo is automatically stretched to fill the object space.
	Click this button to save your changes. You must either press Enter or save your changes before it is reflected in the preview.
	Click this button to discard your changes.


Badge Designer - Add DB Field

When you add a DB field to a badge template, you are adding a placeholder for a information that is supplied by the Identities database.

For example, you place a Full Name database field on this badge template. When a new badge issued, the badge is automatically populated with the identity's full name according to the badge template.

After you click **Add DB Field** on the Badge Designer Edit page, a database field object is added to the canvas and the following options are displayed:


Feature	Description
Data Field	<p>Select a database field from the drop down list.</p> <p>All the system default database fields and any user defined fields are listed.</p> <p>Click Data Field to show or hide the following options.</p> <p>Click  to delete the object from the canvas.</p>
Layer Order	<p>Enter a number to indicate where the object appears when objects are stacked on top of each other.</p> <p>1 is the bottom layer, 2 is on top of 1 and so on.</p>
Location	<p>Enter where the object appears on the canvas. 0 x 0 would place the object in the top left corner, while 80 x 160 would place the object in the bottom right corner.</p> <p>You can also set the location by click and dragging the object on the canvas.</p>
Dimensions	<p>Enter the size of the object.</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.</p> <p>The default is 0 degrees.</p>
BG Color	<p>Click this field to choose a background color for this object. By default, it is set to be the same color as the badge template.</p> <p>When the color palette is displayed, 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.</p> <p>0% is transparent and 100% is opaque.</p>
Font	<p>Select the font you want this object to use.</p> <p>The font list includes text fonts and barcode fonts. Text fonts are listed first (from Arial to Verdana Italic), then barcode fonts are listed (from AusPost 4 State Customer Code to United States Service POSTNET).</p>
Font size	<p>Enter the font size in points.</p>
Auto Resize	<p>Check this box to have the system automatically resize the database information to fit the dimensions of the object.</p>
Alignment	<p>Select how you want the text to align inside the object.</p>
Text Color	<p>Click this field to choose a font color.</p> <p>When the color palette is displayed, 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.</p> <p>0% is transparent and 100% is opaque.</p>
	<p>Click this button to save your changes.</p> <p>You must save your changes before it is reflected in the preview.</p>



Feature	Description
	Click this button to discard your changes.

Badge Designer - Add Text

When you add text to a badge template, you are adding a line of text to the badge template. The same text will appear for all badges that use this template.

After you click **Add Text** on the Badge Designer Edit page, a text object is added to the canvas and the following options are displayed:



Feature	Description
Text	<p>Enter the text you want to appear on this badge template.</p> <p>Click Text to show or hide the following options.</p> <p>Click  to delete the object from the canvas.</p>
Layer Order	<p>Enter a number to indicate where the object appears when objects are stacked on top of each other.</p> <p>1 is the bottom layer, 2 is on top of 1 and so on.</p>
Location	<p>Enter where the object appears on the canvas. 0 x 0 would place the object in the top left corner.</p> <p>You can also set the location by click and dragging the object on the canvas.</p>
Dimensions	<p>Enter the size of the object.</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.</p> <p>The default is 0 degrees.</p>
BG Color	<p>Click this field to choose a background color for this object. By default, it is set to be the same color as the badge template.</p> <p>When the color palette is displayed, 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.</p> <p>0% is transparent and 100% is opaque.</p>
Font	<p>Select the font you want this object to use.</p> <p>The font list includes text fonts and barcode fonts. Text fonts are listed first (from Arial to Verdana Italic), then barcode fonts are listed (from AusPost 4 State Customer Code to United States Service POSTNET).</p>
Font size	Enter the font size in points.
Auto Resize	Check this box to have the system automatically resize the text to fit the dimensions of the object.
Alignment	Select how you want the text to align inside the object.
Text Color	Click this field to choose a font color.


Feature	Description
	When the color palette is displayed, select a color from the palette or manually enter the color in RGB, HSV or hex code format.
Opacity	Enter how opaque you want the font color to be. 0% is transparent and 100% is opaque.
	Click this button to save your changes. You must save your changes before it is reflected in the preview.
	Click this button to discard your changes.

Badge Designer - Add Graphic

When you add a graphic to a badge template, you are adding an image or logo to the badge template. The same image will appear for all badges that use this template.

After you click **Add Graphic** on the Badge Designer Edit page, an image object is added to the canvas and the following options are displayed:

Feature	Description
# or Image File Name	Click this label to show or hide the following options. Click  to delete the object from the canvas.
Layer Order	Enter a number to indicate where the object appears when objects are stacked on top of each other. 1 is the bottom layer, 2 is on top of 1 and so on.
Image	Click the button to locate the image you want to add. You can only choose JPEG images. If an image already appears on the canvas, choosing a new image will replace the current image.
Location	Enter where the object appears on the canvas. 0 x 0 would place the object in the top left corner. You can also set the location by click and dragging the object on the canvas.
Dimensions	Enter the size of the object. The first field is the width and the second field is the height.
Rotation	Select the number of degrees to rotate this object clockwise. The default is 0 degrees.
Maintain Aspect	Check this box to maintain the aspect ratio of the image when the system fits it into the object space. If this option is disabled, the image is automatically stretched to fill the object space.
	Click this button to save your changes.

Feature	Description
	You must save your changes before it is reflected in the preview.
	Click this button to discard your changes.

Badge Designer - Barcodes

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 (from Arial to Verdana Italic) then the barcode fonts (from AusPost 4 State Customer Code to United States Service POSTNET).

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 is invalid, the barcode will not be displayed on the badge.

Badge Designer - Layer Ordering

The badge designer allows you to layer badge objects on top of each other so that certain information can be made more prominent than others, or allow information to stretch over images where appropriate.

For example, you can place an employee photo on a badge with the word "Administration" written across the photo. In this example, the photo would be on the bottom, and the word "Administration" is layered on top.

For each badge object, you have a **Layer Order** option. Enter a number to represent which layer the object should be.

- 1 is the bottom layer
- 2 is on top of 1
- 3 is on top of 2 (etc.)

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.

Supported External Systems

Listed below are all the external systems that are supported by the Access Control Manager system. Some systems may not be available to you if your system does not have the required license.

External Systems - Avigilon™ Server Listing Page



When you select **Settings > External Systems** In the top-right Setup links area, the first page you see is the Avigilon page. Select the **Avigilon** tab to return to this page.

Feature	Description
Name	The name of the ACM 5.6.4 Server.
Address	The IP address of the ACM 5.6.4 Server. Click on the address to edit the server.
Appliance	The appliance this server is connected to.
Cameras	The number of cameras that are currently connected to the server and are accessible to the appliance.
Status	Indicates the current status of the server.
Delete	Click  to delete the server from the system.
Add New Avigilon Server	Click this button to add a new ACM 5.6.4 Server to the system.

External Systems - Avigilon™ Server Add Page

When you click the **Add New Avigilon Server** button, the Avigilon Server Add page is displayed.



Feature	Description
Name	Enter a name for the Avigilon ACM 5.6.4 Server.
Alt Name	An alternative name that is automatically assigned by the Access Control Manager system.
Appliance	If you have more than one appliance in your system, select the appliance the ACM 5.6.4 Server should connect to.
Address	Enter the IP address of the ACM 5.6.4 Server.
Port	Enter the port number used to communicate with the ACM 5.6.4 Server. The default port is 80.
Remote Username	Enter an Avigilon ACM 5.6.4 username for accessing the server.
Remote Password	Enter the password for the username.
Local Username	Enter an Access Control Manager identity username that the external system can use to connect to the appliance.
Local Password	Enter the password for the username.
Installed	Check this box to indicate that the ACM 5.6.4 Server is online and able to communicate with the appliance.

Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.

External Systems - Avigilon™ Server Edit Page


When you click an address from the Avigilon Server Listing page, the Avigilon Server Edit page is displayed.

Make any changes as required.

Feature	Description
Name	The name of the Avigilon ACM 5.6.4 Server.
Alt Name	The alternative name is automatically assigned by the Access Control Manager system.
Appliance	The appliance the ACM 5.6.4 Server is connected to.
Address	The IP address of the ACM 5.6.4 Server.
Port	The port number used to communicate with the ACM 5.6.4 Server.
Remote Username	The Avigilon ACM 5.6.4 username for accessing the server.
Remote Password	The password for the Avigilon username.
Local Username	The Access Control Manager identity username that the external system uses to connect to the appliance.
Local Password	The password for the Access Control Manager username.
Installed	Check this box to indicate that the ACM 5.6.4 Server is online and able to communicate with the appliance.
Cameras	<p>A list of the cameras that are connected to the system. If there are no cameras listed, then no cameras are currently connected to the ACM 5.6.4 Server.</p> <ul style="list-style-type: none"> • Name – the name of the camera. • Disabled – indicates if the camera video is disabled (Yes) or not (No). • PTZ – indicates if the camera has active pan-tilt-zoom capabilities. • Status – indicates if the camera is online or not. • Zoom Capability – indicates if you are able to zoom the camera within the Access Control Manager system.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Avigilon Server	Click this button to add another Avigilon ACM 5.6.4 Server to the system.



External Systems - Dedicated Micros™ Listing Page

When you select the **Dedicated Micros** tab on the External Systems screen, the Dedicated Micros Listing page is displayed.

Feature	Description
Name	The name of the Dedicated Micros server.
Address	The IP address of the Dedicated Micros server. Click on the address to edit the server.
Gateway	The appliance this server is connected to.
Cameras	The number of cameras that is currently connected to the server and is accessible to the appliance.
Status	Indicates the current status of the server.
Delete	Click  to delete the server from the system.
Add New Dedicated Micros Server	Click this button to add a new Dedicated Micros server to the system.

External Systems - Dedicated Micros™ Add Page

When you click **Add New Dedicated Micros Server**, the Dedicated Micros Add page is displayed.



Feature	Description
Name	Enter a name for the Dedicated Micros server.
Alt Name	An alternative name that is automatically assigned by the Access Control Manager system.
Appliance	If you have more than one appliance in your system, select the appliance the server should connect to.
Address	Enter the IP address of the Dedicated Micros server.
Port	Enter the port number used to communicate with the Dedicated Micros server.
Dedicated Micros Login	Enter a Dedicated Micros username for accessing the server.
Dedicated Micros Password	Enter the password for the Dedicated Micros username.
ACM Login	Enter an Access Control Manager identity username that the external system can use to connect to the appliance.
ACM Password	Enter the password for the Access Control Manager username.
VidProxyUrl	Enter the URL used as a translator between the Access Control Manager appliance and the Dedicated Micros server.
Installed	Check this box to indicate that the Dedicated Micros server is installed and able to communicate with the Access Control Manager appliance.
	Click this button to save your changes.
	Click this button to discard your changes.

External Systems - Dedicated Micros™ Edit Page

When you click an address from the Dedicated Micros Server Listing page, the Dedicated Micros Edit page is displayed.

Feature	Description
Name	The name for the Dedicated Micros server.
Alt Name	The alternative name that is automatically assigned by the Access Control Manager system.
Appliance	The Access Control Manager appliance the Dedicated Micros server is connect to.
Address	The IP address of the Dedicated Micros server.
Port	The port number used to communicate with the Dedicated Micros server.
Dedicated Micros Login	The Dedicated Micros username for accessing the server.
Dedicated Micros Password	The password for the Dedicated Micros username.
ACM Login	The Access Control Manager identity username that the external system uses to connect to the appliance.
ACM Password	The password for the Access Control Manager username.
VidProxyUrl	The URL used as a translator between the Access Control Manager appliance and the Dedicated Micros server.
Installed	Check this box to indicate that the Dedicated Micros server is installed and able to communicate with the Access Control Manager appliance.


Cameras – a list of the cameras that are connected to the server. This area is only displayed if there are cameras connected to the server.

Name	The name of the camera.
Camera UUID	The camera's universally unique identifier, or logical ID.
Disabled	Indicates if the camera video is disabled (Yes) or not (No).
Status	Indicates if the camera is online or not.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Dedicated Micros Server	Click this button to add a new Dedicated Micros server.

External Systems - Exacq™ Servers Listing Page



When you select the **Exacq** tab on the External Systems screen, the Exacq Servers Listing page is displayed.

Feature	Description
Name	The name of the Exacq server.
Address	The IP address of the Exacq server. Click on the address to edit the server.

Feature	Description
Appliance	The appliance this server is connected to.
Cameras	The number of cameras that are currently connected to the server and are accessible to the appliance.
Status	Indicates the current status of the server.
Delete	Click  to delete the server from the system.
Add New Exacq Server	Click this button to add a new Exacq server to the system.

External Systems - Exacq™ Server Add Page

If you click the **Add New Exacq Server** button, the Exacq Server Add page is displayed.

Feature	Description
Name	The name of the Exacq server. This field is auto-completed when you save and connect to the server.
Alt Name	An alternative name that is automatically assigned by the Access Control Manager system.
Appliance	If you have more than one appliance in your system, select the appliance the server should connect to.
Address	Enter the IP address of the Exacq server.
Port	Enter the port number used to communicate with the Exacq server.
Username	Enter an Exacq username for accessing the server.
Password	Enter the password for the username.
Motion Smoothing	Select how long, in seconds, the system should wait before reporting the end of a motion event. This feature helps reduce the number of motion events if the camera is recording video of a high traffic area. For more information, see <i>External Systems - Motion Smoothing</i> on the next page.
Pass Through Enabled	Check this box to indicate that pass through is enabled for the input connected to the Exacq server.
Installed	Check this box to indicate that this server is installed and able to communicate with the Access Control Manager appliance.
	Click this button to save your changes.
	Click this button to discard your changes.

External Systems - Exacq™ Server Edit Page



When you click an address from the Exacq Server Listing page, the Exacq Server Edit page is displayed.

Make any changes as required.

Feature	Description
Name	The name of the Exacq server. This field is auto-completed by the Exacq

Feature	Description
	server.
Alt Name	The alternative name that is automatically assigned by the Access Control Manager system.
Appliance	The appliance the server should connect to.
Address	The IP address of the Exacq server.
Port	The port number used to communicate with the Exacq server.
User Name	The Exacq username for accessing the server.
Password	The password for the username.
Motion Smoothing	The amount of time, in seconds, the system should wait before reporting the end of a motion event. This feature helps reduce the number of motion events if the camera is recording video of a high traffic area. For more information, see <i>External Systems - Motion Smoothing</i> below.
Pass Through Enabled	Check this box to indicate that pass through is enabled for the input connected to the Exacq server.
Installed	Check this box to indicate that this server is installed and able to communicate with the Access Control Manager appliance.

Cameras – a list of the cameras that are connected to the server. This area is only displayed if there are cameras connected to the server.

Name	The name of the camera.
Address	The IP address of the camera.
Disabled	Indicates if the camera video is disabled (Yes) or not (No).
PTZ	Indicates if the camera has active pan-tilt-zoom capabilities.
Status	Indicates if the camera is online or not.
Motion Masked During	Select a schedule if motion masking alarms generated by this camera are ever ignored and not reported by the system. Only configured schedules in the system are listed.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Exacq Server	Click this button to add a new Exacq server to the system.

External Systems - Motion Smoothing

Motion smoothing is an algorithm used to minimize the report of motion events that occur in quick succession. Part of the configuration for an Exacq server is the Motion Smoothing value in seconds. When the server detects a motion restored event, the application does not report it until the motion smoothing time expires.


For example, a parade is passing through the scene. A camera connected to the Exacq server is reporting multiple motion detection events as the parade passes through the field of view. If the Motion Smoothing value is set to 30 seconds, the camera must report its last motion restored event and wait for 30 seconds without any new motion activity before it is logged in the Access Control Manager system as the end of the motion event.

Note that the time/clock on the Exacq server and on the Access Control Manager appliance must be the same. If the clocks are not in sync, the motion smoothing algorithm may not function properly.

External Systems - IP-Based Camera Listing Page

When you select the **IP Based** tab on the External Systems screen, the IP Based Camera Listing page is displayed.

This page lists all the cameras that are connected to the appliance by the camera's IP address or displays video streaming via RTSP.



Feature	Description
Name	The name of the camera that has been added to the system. Click the name to edit the camera.
Device IP	The IP address of the camera.
Delete	Click  to remove a camera from the system.
Add New Camera	Click this button to add a new camera for this system.

External Systems - IP-Based Camera Add Page

When you click **Add New Camera** from the IP-Based Camera Listing page, the IP Camera Add page is displayed.

Enter the details as required.



Feature	Description
Name	Enter a name for the camera.
Type	Select one of the following options from the drop down list: <ul style="list-style-type: none"> • Web Camera – The camera is directly connected to the network and is accessible by its IP address. • RTSP – The camera may not be directly connected to the network but live video from the camera is available through the camera's Real Time Streaming Protocol. <p>NOTE: To use RTSP, you must install a plug-in. See <i>External Systems- Enabling RTSP</i> on the next page</p>
Device IP	Enter the IP address for the camera
Still URL	(optional) Enter the URL or web address of the camera's web-based application showing the last still image captured by the camera.
Preview URL	(optional) Enter the URL or web address of the camera's web-based application showing a preview of the finished picture.
Device Login	Enter the login name that is required to access the camera.

Feature	Description
Device Password	Enter the password that is required to access the camera.
	Click this button to save your changes.
	Click this button to discard your changes.

External Systems - IP-Based Camera Edit Page

When you click the name of a camera from the IP-Based Camera Listing page, the IP Camera Edit page is displayed.

Make any changes as required.

Feature	Description
Name	The name of the camera.
Type	The type of connection the appliance uses to stream video from the camera. The options are: <ul style="list-style-type: none"> • Web Camera – The camera is directly connected to the network and is accessible by its IP address. • RTSP – The camera may not be directly connected to the network but live video from the camera is available through the camera's Real Time Streaming Protocol.
Device IP	The IP address of the camera.
Still URL	The URL or web address of the camera's web-based application that shows the last still image captured by the camera.
Preview URL	The URL or web address of the camera's web-based application that shows a preview of the finished picture.
Device Login	The login name that is required to access the camera.
Device Password	The password for the login name.
	Click this button to save your changes.
	Click this button to discard your changes.

External Systems- Enabling RTSP

To view RTSP video in your browser:

1. Install the [VLC Media Player](#).
2. Open the video viewer window. You can access the video viewer window by selecting:
 - **Monitor > Events > Live Video** or
 - **Physical Access > Doors > Cameras**


The video viewer window pops up.

3. Right-click inside the video viewer window.
4. Select *Run this plug-in*.

The live video is displayed.



External Systems - LifeSafety Power™ Listing Page

When you select the **LifeSafety** tab on the External Systems screen, the External Systems Listing page is displayed.

Feature	Description
Name	The name of the LifeSafety power supply. Click the name to edit the power supply.
Address	The IP address of the power supply.
Appliance	The appliance this power supply is connected to.
Delete	Click  to delete the power supply from the system.
Add New External System	Click this button to add a new LifeSafety power supply to the system.

External Systems - LifeSafety Power™ Add Page



When you click the **Add New External System** button, the External System Edit page is displayed.

Feature	Description
Name	Enter a name for the LifeSafety power supply.
Alt Name	Enter an alternative name for this power supply as required.
Appliance	If you have more than one appliance in your system, select the appliance the power supply should connect to.
Address	Enter the IP address of the power supply.
Port	Enter the port number used to communicate with the LifeSafety power supply.
User Name	Enter a LifeSafety username for accessing the power supply.
Password	Enter the password for the username.
Installed	Check this box to indicate that the LifeSafety power supply is installed and able to communicate with the Access Control Manager appliance.
	Click this button to save your changes.
	Click this button to discard your changes.

External Systems - LifeSafety Power™ Supply Edit Page


When you click the name of a power supply from the External Systems Listing page, the External Systems Edit page is displayed.

Make any changes as required.

Feature	Description
Name	The name for the LifeSafety power supply.
Alt Name	The alternative name for this power supply.
Appliance	The appliance the power supply should connect to.
Address	The IP address of the power supply.
Port	The port number used to communicate with the LifeSafety power supply.
User Name	The LifeSafety username for accessing the power supply.
Password	The password for the username.
Installed	Check this box to indicate that the LifeSafety power supply is installed and able to communicate with the Access Control Manager appliance.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New External System	Click this button to add a new LifeSafety power supply to the system.

External Systems - Milestone™ Servers Listing Page



When you select the **Milestone** tab on the External Systems screen, the Milestone Servers Listing page is displayed.

Feature	Description
Name	The name of the Milestone server.
Address	The IP address of the Milestone server. Click on the address to edit the server.
Appliance	The appliance this server is connected to.
Cameras	The number of cameras that is currently connected to the server and is accessible to the appliance.
Status	Indicates the current status of the server.
Delete	Click  to delete the server from the system.
Add New Milestone Server	Click this button to add a new Milestone server to the system.

External Systems - Milestone™ Server Add Page

When you click the **Add New Milestone Server** button, the Milestone Server Add page is displayed.



Feature	Description
Name	Enter a name for the Milestone server.

Feature	Description
Alt Name	An alternative name that is automatically assigned by the Access Control Manager system.
Appliance	If you have more than one appliance in your system, select the appliance the server should connect to.
Address	Enter the IP address of the Milestone server.
Port	Enter the port number used to communicate with the Milestone server.
User Name	Enter a Milestone username for accessing the server.
Password	Enter the password for the username.
VidProxyUrl	Enter the URL used as a translator between the Access Control Manager appliance and the Milestone server.
VidProxyImageUrl	Enter the URL used to store the video captured by the Milestone server.
Installed	Check this box to indicate that the Milestone server is installed and able to communicate with the Access Control Manager appliance.
	Click this button to save your changes.
	Click this button to discard your changes.

External Systems - Milestone™ Server Edit Page


When you click an address from the Milestone Server Listing page, the Milestone Server Edit page is displayed. Make any changes as required.

Feature	Description
Name	The name for the Milestone server.
Alt Name	The alternative name that is automatically assigned by the Access Control Manager system.
Appliance	The Access Control Manager appliance the Milestone server is connect to.
Address	The IP address of the Milestone server.
Port	The port number used to communicate with the Milestone server.
User Name	The Milestone username for accessing the server.
Password	The password for the username.
VidProxyUrl	The URL used as a translator between the Access Control Manager appliance and the Milestone server.
VidProxyImageUrl	The URL used to store the video captured by the Milestone server.
Installed	Check this box to indicate that the Milestone server is installed and able to communicate with the Access Control Manager appliance.
Cameras – a list of the cameras that are connected to the server. This area is only displayed if there are cameras connected to the server.	

Feature	Description
Name	The name of the camera.
Camera UUID	The camera's universally unique identifier, or logical ID.
Disabled	Indicates if the camera video is disabled (Yes) or not (No).
PTZ	Indicates if the camera has active pan-tilt-zoom capabilities.
Status	Indicates if the camera is online or not.
Zoom Capability	Indicates if you are able to zoom the camera within the Access Control Manager system.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Milestone Server	Click this button to add a new Milestone server.

External Systems - Salient™ Servers Listing Page



When you select the **Salient** tab on the External Systems screen, the Salient Servers Listing page is displayed.

Feature	Description
Name	The name of the Salient server.
Address	The IP address of the Salient server. Click on the address to edit the server.
Appliance	The appliance this server is connected to.
Cameras	The number of cameras that is currently connected to the server and is accessible to the appliance.
Status	Indicates the current status of the server.
Delete	Click  to delete the server from the system.
Add New Salient Server	Click this button to add a new Salient server.

External Systems - Salient™ Server Add Page

When you click the **Add New Salient Server** button, the Salient Server Add page is displayed.

Feature	Description
Name	Enter a name for the Salient server.
Alt Name	An alternative name that is automatically assigned by the Access Control Manager system.
Appliance	If you have more than one appliance in your system, select the appliance the server should connect to.
Hostname	Enter the network name, URL, or IP address of this Salient server. All Salient servers have a fixed address (assigned when this server was configured) that must be entered here.



Feature	Description
Port	Enter the port number used to communicate with the Salient server.
WebServicePort	Enter the port number that the Salient server uses to communicate with its web service.
User Name	Enter a Salient username for accessing the server.
Password	Enter the password for the username.
VidProxyUrl	Enter the URL used as a translator between the Access Control Manager appliance and the Salient server.
Installed	Check this box to indicate that the Salient server is installed and able to communicate with the Access Control Manager appliance.
	Click this button to save your changes.
	Click this button to discard your changes.

External Systems - Salient™ Server Edit Page

When you click an address from the Salient Server Listing page, the Salient Server Edit page is displayed.

Make any changes as required.

Feature	Description
Name	The name of the Salient server.
Alt Name	An alternative name that is automatically assigned by the Access Control Manager system.
Appliance	The appliance the server is connected to.
Hostname	The network name, URL, or IP address of this Salient server.
Port	The port number used to communicate with the Salient server.
WebServicePort	The port number that the Salient server uses to communicate with its web service.
User Name	The Salient username for accessing the server.
Password	The password for the username.
VidProxyUrl	The URL used as a translator between the Access Control Manager appliance and the Salient server.
Installed	Check this box to indicate that the Salient server is installed and able to communicate with the Access Control Manager appliance.
Cameras	
Name	The name of the camera.
Disabled	Indicates if the camera video is disabled (Yes) or not (No).
PTZ Enabled	Indicates if the camera has active pan-tilt-zoom capabilities.
Status	Indicates if the camera is online or not.
Zoom Capability	Indicates if you are able to zoom the camera within the Access Control Manager system.

Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Salient Server	Click this button to add a new Salient server to the system.



External Systems - Adding

In order to add photos to the Identities database or record video for surveillance, you must first 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. In the top-right Setup links area, select **Settings > External Systems**.
2. Select the tab for the external system you want to add.
3. From the external system 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. In the top-right Setup links area, select **Settings > External Systems**.
2. Select the tab for the type of external system you want to edit.
3. From the external system 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. In the top-right Setup links area, select **Settings > 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 - 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. In the top-left User links area, click **My Account**.
2. Under the Profile tab, select a camera from the **Badge Camera** drop down list.
All the IP cameras that have been added as part of an external system are listed.
3. When you're finished, click .

Next time you create a badge, the selected camera is used to take the identity photo.


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 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 JPG, PNG, GIF or BMP 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 221.




1. In the Setup links area, select **Settings > 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. In the Setup links area, select **Settings > 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

Once a map has been configured, it can be accessed from the Monitor screen and used 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, activate inputs and outputs, control doors and keep track of identities as they arrive at muster stations from the Mustering dashboard. The map also notifies you if there is an alarm by flashing a red icon.







1. From the icon task bar, 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.



Figure 2: Example map


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 more status information.</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 409.</p>
Review an alarm	<p>If you see a flashing red icon, the item on the map is in an alarm state. Click the icon to see the status details.</p>
Control a door	<p>Click  on the map to display the door control menu, then click any of the following:</p> <ul style="list-style-type: none"> • Disable — disable the door. • Unlock — unlock the door. This door will remain unlocked until the Lock command is issued. • Lock — lock the door. This door will remain locked until the Unlock command is issued.

To...	Do this...
	<ul style="list-style-type: none"> • Grant — grant access to the person who is at the door. The door is temporarily unlocked to permit a one time entry through the door. • Restore — reset the door's configuration values to their default value. • Mask Held — mask the Door Held Open Alarm. • Unmask Held — unmask the Door Held Open Alarm. • Mask Forced — mask the Forced Held Open Alarm. • Unmask Forced — unmask the Door Forced Open Alarm. • Trace — display the event transactions for the door. <p>To hide the control menu, click the icon again.</p>
Control a panel or subpanel	<p>Click the  on the map to display the panel control menu, then click any of the following:</p> <ul style="list-style-type: none"> • Panels <ul style="list-style-type: none"> ◦ Download Params — download the latest system configurations to the panel. ◦ Tokens — download the tokens to the panel. ◦ Reset/Download — reset and download the current system configuration to the panel's connected doors. ◦ APB Reset — reset the anti-passback configuration for this panel. ◦ Clock — re-sync the panel time. ◦ Trace — display the event transactions for the panel. • Subpanels <ul style="list-style-type: none"> ◦ Trace — display the event transactions for the subpanel. <p>To hide the control menu, click the icon again.</p>
Control an input	<p>Click the  on the map to display the input control menu, then click any of the following:</p> <ul style="list-style-type: none"> • Mask — mask the input. • Unmask — unmask the input. <p>To hide the control menu, click the icon again.</p>
Control an output	<p>Click the  on the map to display the output control menu, then click any of the following:</p> <ul style="list-style-type: none"> • On — activate the output. • Off — deactivate the output. • Pulse — pulse the output <p>To hide the control menu, click the icon again.</p>
Display video	<p>Click the  on the map to display the Camera Video window. For more information see <i>Monitor Screen - Viewing Camera Video</i> on page 417.</p>
Open a linked	<p>Click  to display a close-up view of the same map, or  to display a expanded view</p>

To...	Do this...
map	of the same map.
Execute a global action	Click  to execute the configured global action.
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 plus the name of the area. In the example image, 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.</p> <p>For more information, see <i>Mustering - Using the Dashboard</i> on page 221.</p>

Map Templates (Settings) - Listing Page



When you select **Settings > Maps** from the Setup links area, the Map Templates Listing page is displayed. This page lists all the maps that have been added to the system.

Feature	Description
Name	The name of the map template. Click the name to edit the map. For more information, see <i>Maps - Creating and Editing a Map</i> on page 272.
	Click this button to delete the selected map template.
Show	Click this button to display a preview of how the map would look in the Monitor screen.
Add New Map Template	Click this button to add a new map template. For more information, see <i>Maps - Creating and Editing a Map</i> on page 272.

Maps - Add Page

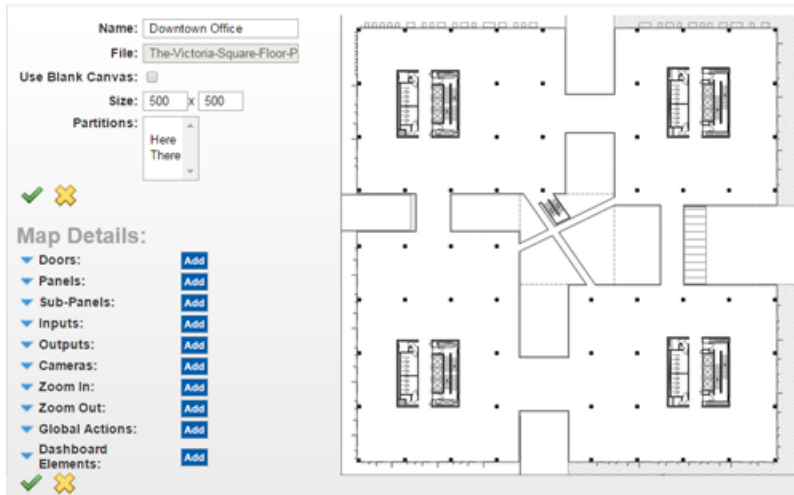
When you click **Add New Map Template** from the Map Templates Listing Page, the Map Template: Add New page is displayed. From this page, select the image that the map would be based on.

Feature	Description
Name	Enter a name for the map.
File:	Click the Browse button to select the image you want to use as the base of the map. You can select any raster image in PNG, JPEG, BMP and GIF format.
Blank Canvas	<p>Check this box to leave the map background white.</p> <p>This option is primarily for setting up Mustering dashboards that do not need to be on a map.</p>
Re-Size To:	<p>Enter the map size in pixels.</p> <p>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.</p>

Feature	Description
	Click this button to save your changes. After you save the map for the first time, you are taken to the Map Template Edit page where you can add doors, panels, shortcuts and dashboard elements.
	Click this button to discard your changes.

Maps - Edit Page

The Map Edit page is displayed after you save a new map for the first time, or when you click the name of the map on the Map Template (Settings) Listing page.





On the right is the base map image. You can move map items anywhere in this work area.

On the left are the map properties, including the name and size. In the Map Details area are a list of all the items that can be added to the map.

Map Properties



Feature	Description
Name	The name of the map
File	The original image filename of the base map image.
Blank Canvas	Check this box to leave the map background white. This option is primarily for setting up Mustering dashboards that do not need to be on a map.
Size	The size of the map. 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.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden. NOTE: It is recommended that you do not assign maps to a partition. If you add a device to the map that is part of multiple partitions, the map may generate an error when a user without the same permissions as the device tries to use the map.
	Click this button to save your changes.
	Click this button to discard your changes.










Map Details



To add an item to the map, click the **Add** button beside the item you want to add. An icon matching the item you added will automatically be added to the top left corner of the map image. Move the icon to where it should appear in the map.

Tip: Map icons are added on top of each other in the top left corner of the map. Move added icons right away or you may lose track of all the items that have been added to the map.

To show or hide the details of each item that has been added to the map, click the  or  beside each item. If any of the item drop down lists are empty, you need to add or configure that item in the system first.

To delete an item that has been added to the map, click  beside the listed item.

Feature	Description	Map Icon
Doors	Select a door from the drop down list.	
Panels	Select a panel from the drop down list.	
Subpanels	Select a subpanel from the drop down list.	
Inputs	Select an input from the drop down list.	
Outputs	Select an output from the drop down list.	
Cameras	Select a camera from the drop down list.	
Zoom In	Select a map that offers a closer view of a specific area in this map.	
Zoom Out	Select a map that offers a wider view of this map area.	
Global Actions	Select a global action from the drop down list.	
Dashboard Elements	Configure a Mustering dashboard element: <ol style="list-style-type: none"> 1. Enter a title for the dashboard element. The map automatically updates with each change that you make. 2. Click the Title Font Color field to change the text color. 3. In the Title Font Size drop down list, select the size. The options are Small, Medium and Large. 4. For the Opacity option, choose how transparent you want the dashboard 	Square, circle or text object

Feature	Description	Map Icon
	<p>element to be. You can enter a percent number, or move the slider to set the opacity. 100% is opaque and 0% is transparent.</p> <ol style="list-style-type: none"> 5. In the Location field, enter where you want the dashboard element to appear on the map. You can also move the dashboard element directly on the map. 6. In the Element Type drop down list, select if you want the dashboard element to appear as Text Only or Graphic & Text. <p>If you choose Graphic & Text, the following options are displayed:</p> <ol style="list-style-type: none"> 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. 	
	Click this button to save your changes.	
	Click this button to discard your changes.	



Identities

The Identities screen gives you access to all the cardholders and operators in the system. You can manually add each identity to the system or you can use the Collaboration feature to transfer identity information from a third party database. For more information, see *Collaboration - Introduction* on page 313.

Identities Overview

From the Identity Search page you can either add or search for identities. Once you have searched you can select an identity to edit, including the following actions:

- assigning roles, tokens, and groups
- capturing images and uploading photos
- creating badges and reports
- deleting

Adding an Identity

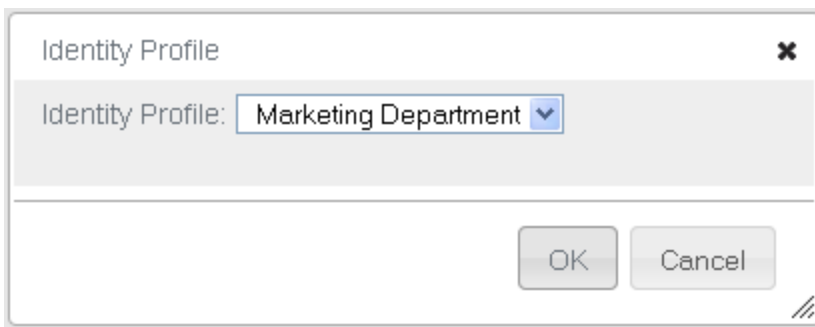
To add a new identity:

1. Click **Identities** from the icon task bar.

The Identities Listing 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:



- 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.

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. For more information, see *Editing a User Defined List*.


4. Click  .

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

5. Assign role(s) 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. Click **Download** to download 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:
 - **Groups:** use this page to assign this identity to a group.
 - **Access:** use this page to view this identity's access privileges including roles, access groups, and doors.
 - **Capture:** use this page to take a photo of the user.
 - **Photos:** use this page to upload an existing photo of the user.
 - **Transactions:** use this page to view past alarms and events that were triggered by this user.
 - **Badge:** use this page to assign a badge to this user.
 - **Audit:** use this page to view a log of all the changes that have been made to this identity.

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.
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**.

NOTE: Only the fields that appear on the Identities page are included in this list. If the search criteria that you want is not listed in the Search Field drop down list, then it can be added, if created as a user defined field. See *User Defined Fields - Adding a Field* on page 235 for more detail.
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: 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. See *Adding an Identity Profile* on page 302 and *Identity Profiles - Batch Update* on page 305 for more detail.

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

5. If you want to delete the identities displayed in the search results, click **Destroy Batch** then click **OK** when the Message from webpage dialog box displays the message 'Number of identities being deleted <number>. Are you sure?'

NOTE: This feature has the potential to erase the entire database and should only be used by a top-level administrator. Only the identities assigned with **Identity Destroy Batch** delegation can use this feature. See *Deleting an Identity* on page 289 for more detail.

Editing an Identity

To edit an existing identity:

1. Click **Identities** from the icon task bar.
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 this identity to a role.
 - Tokens: use this page to create a token for the identity.
 - Groups: use this page to assign this identity to a group.
 - Access: use this page to view this identity's access privileges including roles, access groups, and doors.
 - Capture: use this page to take a photo of the user.
 - Photos: use this page to upload an existing photo of the user.
 - Transactions: use this page to view past alarms and events that were triggered by this user.
 - Badge: use this page to assign a badge to this user.
 - Audit: use this page to view a log of all the changes that have been made to this identity.


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

Identities - Assigning Roles

To assign roles to an identity:

1. Click **Identities** from the icon task bar.
2. From the Identities listing page, click on the name of the identity you want to edit.

The Identity Edit screen appears.

3. Select the **Roles** tab.
4. 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 terms by using the **Ctrl** or **Shift** key.

5. Click .

Identities - Assigning Tokens


To create tokens and assign them to an identity:

1. Click **Identities** from the icon task bar.
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 **Tokens** tab.
4. 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 New Token**.

5. Enter the details as required.
6. Click .
7. Click **Download** to download the token to the connected panels and associated doors.
8. To assign this token to a badge, select the **Badge** tab.
9. From the **Badge Token** drop down list, select the internal number you want to assign to the badge.

10. Click .


Identities - Assigning Groups

To assign groups to an identity:


1. Click **Identities** from the icon task bar.
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 **Groups** tab.

4. 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.

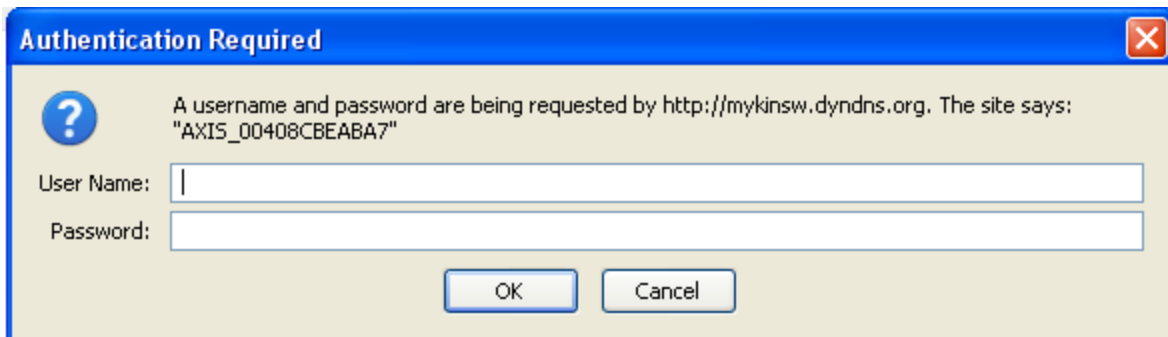
5. Click .

Capturing an Image of an Identity

You can capture an image of a person to display on the Identity page or print on a badge.

NOTE: You must configure a badge camera before you can use this feature. For more information, see *External Systems - Adding* on page 271 and *External Systems - Defining the Badge Camera for the System* on page 272.

1. There are two ways to arrive at the Capture page:
 - From the Identities Listing page, click  from the **Image Capture** column.
 - From the Identities Listing page, click on the name of an identity, then select the **Capture** tab.
2. If the camera requires authentication, this page will not appear until you have entered your login credentials:



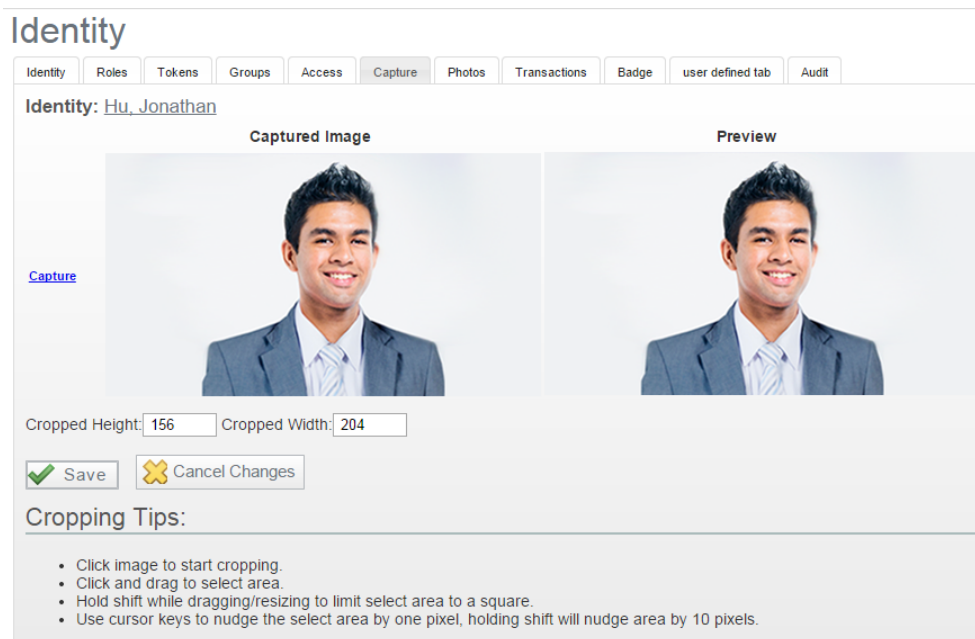
The image shows a Windows-style dialog box titled "Authentication Required" with a blue header and a red close button. The main area has a light beige background. On the left is a blue question mark icon. To its right, text reads: "A username and password are being requested by http://mykinsw.dyndns.org. The site says: 'AXIS_00408CBEABA7'". Below this text are two input fields: "User Name:" and "Password:". At the bottom of the dialog are two buttons: "OK" and "Cancel".

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

The capture page appears.

3. Click **Capture**.

The page refreshes to show the captured image on the left and a preview of the image on the right.



4. To crop the image, click the captured image on the left.
5. Click and drag to select the cropping area.

Hold **Shift** to constrain the area selection to a square.

Use the cursor keys to nudge the area selection by one pixel. Hold **Shift** to nudge the area selection by 10 pixels.

6. Click  .

Identities - Creating Badges

Badges are access cards that you can customize for each user.

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** from the icon task bar.
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 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**.

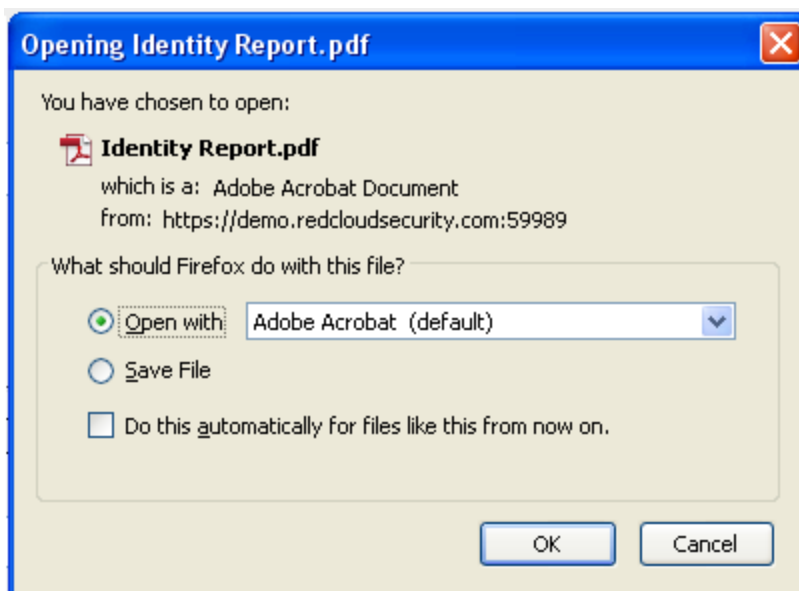
Creating an Identity Report

You can generate two types of PDF reports for an identity. The available reports are:

- Identity report showing all the attributes of the identity.
- Event report indicating the events involving the identity.

To generate an identity report:

1. On the Identities Listing page, select a user.
The Identities Edit screen appears.
2. At the bottom of the Identity page, click **Create New Report**.
A dialog box will popup:

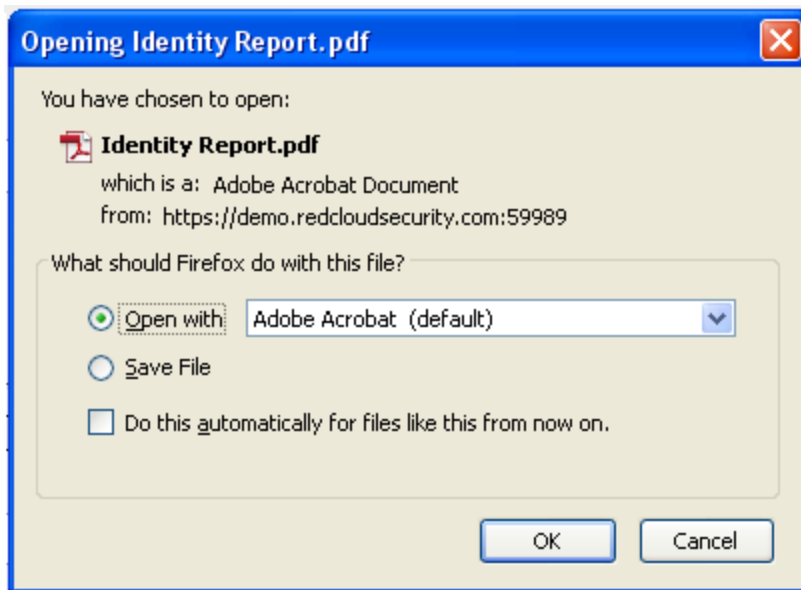


3. Select your preference then click **OK**.
A PDF report is generated.

To generate an event report:

1. On the Identities Listing page, select a user.
The Identities Edit screen appears.
2. At the bottom of the Identity page, click **Event Report**.

A dialog box will popup:



3. Select your preference then click **OK**.

A PDF report is generated.

For more information on generating and customizing reports, see *Generating Reports* on page 421.

Uploading a Photo of an Identity

You can upload images of a person to display on the Identity page or print on a badge.

NOTE: Ensure the image has the appropriate dimensions to fit on the badge. Most badges are approximately 2 x 3 inches in size.


To upload an existing photo:

1. Click **Identities** from the icon task bar.
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 **Photos** tab.
4. Click **Upload Photo**.


The screen expands to include more fields.

5. Click **Choose File** and navigate the directory to find the image you want to upload.

Click **Open** to select the image.

If you want to delete this dialog box, click  .


If you want this image to appear on the Identity page, select the **Primary** check box.

6. When you're finished, click  .

The image is saved to the Photos page.

Deleting an Identity

To delete an existing identity:

1. From the icon task bar, select **Identities**.
2. From the Identities Listing page, click  beside the identity that you want to delete.
3. When the confirmation message is displayed, click **OK**.

Destroy Batch feature

The Destroy Batch feature allows you to delete multiple identities at once.

NOTE: This feature has the potential to erase the entire database and should only be used by a top-level administrator. Only the identities assigned with **Identity Destroy Batch** delegation can use this feature.

To delete multiple identities at once:

1. Perform an advanced search to find all the identities you want to delete from the database.
2. Click **Destroy Batch**.
3. When the confirmation message is displayed, click **OK**.

All of the identities in the list are deleted from the system.




Identities - Identity Search Page

When you click **Identities** from the icon task bar, the Identity Search page is displayed. Select the **Identities** tab to return to this page.

All the identities in the system are hidden by default. Click any letter in the gray alphabet bar to display all the names that are sorted under that letter. Alternatively, you can use the search function to find the identity that you are looking for. See *Searching for an Identity* on page 282 for more detail.

Once you click a letter or perform a search, a list of related identities is displayed with the following details:

Feature	Description
Name	The name of the identity. A photo of the identity may be displayed if the system settings are set to always display identity photos.


Feature	Description
	Click the name to edit the identity details.
Status	The current status of the identity: active (such as full-time and part-time employees) or inactive (such as employees currently on leave).
Last Used	The last date that the identity gained access.
Download	Click  to download the identity's access permissions to all connected panels.
Image Capture	Click  to take a photo of the identity.
Delete	Click  to delete the identity from the database.
Add New Identity	Click this button to add a new identity.
Create New Report	Click this button to generate a report of all the identities in the system.

Identities - Add Page


When you click **Add New Identity** from the Identities Listing page, the Identities Add page appears. Enter the required identity details.


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 239.

Feature	Description
Identity Information:	
Last Name	Enter the last name of this user. This field is required.
First Name	Enter the first name of this user.
Middle Name	Enter the middle name of this user.
External System ID	Enter the ID used by the company or issuer of the badge.
Title	From the drop down list, select the title of this user.
Department	From the drop down list, select the department this user is affiliated with.
Division	From the drop down list, select the company division for this user.
Last Used	Indicates the last time this user accessed an area.
Status	From the drop down list, select the status of this identity.
Type	From the drop down list, select the type of identity.
Issue Date	Specify the date this identity was issued. Click the field to use the calendar.
Last Door	Indicates the last door this identity accessed.
Last Area	Indicates the last area this identity accessed.
Address Information:	
Street Address	Enter the street address where this user lives.

Feature	Description
City	Enter the city where this user lives.
State	Enter the state where this user lives.
Zip Code	Enter the zip code where this user lives.
Site Location	From the drop down list, select the location where this user works.
Building	From the drop down list, select the building where this user works.
Phone	Enter this user's personal phone number.
Work Phone	Enter this user's work phone number.
Email Address	Enter this user's email address.
Account Information:	
Remote Authentication?	<p>Check this box to allow the user to authenticate using remote domain credentials via Active Directory.</p> <p>Important: Do not check this box unless there is already a remote domain configured to authenticate to. If there is no domain available this could result in your account being locked. For more detail on configuring remote authentication, refer to <i>System Settings - Configuring Remote Authentication</i> on page 242</p>
Remote Domain	<p>From the drop down list, select an external domain for this identity to use for authentication.</p> <p>Only the external domains previously defined by the system appear in this list.</p>
Record Modification	Indicates the date and time this identity was modified.
Inactivity Timer	From the drop down list, select the amount of time this user can be inactive before it is logged out of the system.
Maximum Active Token	Specify the maximum number of active tokens this user is allowed to have.
	Above the Login field, this bar indicates the strength of the password you have entered below.
Login	Enter the login name this user will use to log in the application.
Password	Enter the password this user will use to log in the application. A minimum of four characters is required.
Confirm	Re-enter the password to confirm it.
Allow Remote Access?	<p>Check this box to allow this identity remote access to the PostgreSQL transactional database.</p> <p>NOTE: To ensure that the remote access is setup, complete the Transactions Connect Port field on the <i>Appliances - Add Page</i> on page 34 or <i>Appliances - Appliance Page</i> on page 36.</p>

In addition, there are two buttons at the bottom of this page:

Feature	Description
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.


Identities - Identity Page

When you click the name of an identity from the Identities Listing page, the Identity Edit page is displayed. Select the **Identity** tab to return to this page.



On this page, you can edit general information about the identity.

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 239.

Feature	Description
Identity Information:	
Last Name	Enter the last name of this user. This field is required.
First Name	Enter the first name of this user.
Middle Name	Enter the middle name of this user.
External System ID	Enter the ID used by the company or issuer of the badge.
Title	From the drop down list, select the title of this user.
Department	From the drop down list, select the department this user is affiliated with.
Division	From the drop down list, select the company division for this user.
Last Used	Indicates the last time this user accessed an area.
Status	From the drop down list, select the status of this identity.
Type	From the drop down list, select the type of identity.
Issue Date	Specify the date this identity was issued. Click the field to use the calendar.
Last Door	Indicates the last door this identity accessed.
Last Area	Indicates the last area this identity accessed.
Address Information:	
Street Address	Enter the street address where this user lives.
City	Enter the city where this user lives.
State	Enter the state where this user lives.
Zip Code	Enter the zip code where this user lives.
Site Location	From the drop down list, select the location where this user works.
Building	From the drop down list, select the building where this user works.
Phone	Enter this user's personal phone number.
Work Phone	Enter this user's work phone number.
Email Address	Enter this user's email address.
Account Information:	
Remote	Check this box to allow the user to authenticate using remote domain credentials via

Feature	Description
Authentication?	Active Directory. Important: Do not check this box unless there is already a remote domain configured to authenticate to. If there is no domain available this could result in your account being locked. For more detail on configuring remote authentication, refer to <i>System Settings - Configuring Remote Authentication</i> on page 242
Remote Domain	From the drop down list, select an external domain for this identity to use for authentication. Only the external domains previously defined by the system appear in this list.
Record Modification	Indicates the date and time this identity was modified.
Inactivity Timer	From the drop down list, select the amount of time this user can be inactive before it is logged out of the system.
Maximum Active Token	Specify the maximum number of active tokens this user is allowed to have.
	Above the Login field, this bar indicates the strength of the password you have entered below.
Login	Enter the login name this user will use to log in the application.
Password	Enter the password this user will use to log in the application. A minimum of four characters is required.
Confirm	Re-enter the password to confirm it.
Allow Remote Access?	Check this box to allow this identity remote access to the PostgreSQL transactional database. NOTE: To ensure that the remote access is setup, complete the Transactions Connect Port field on the <i>Appliances - Add Page</i> on page 34 or <i>Appliances - Appliance Page</i> on page 36.





In addition, there are five buttons at the bottom of this page:

Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Identity	Click this button to add a new person to the database.
Create New Report	Click this button to generate a PDF report on this identity.
Event Report	Click this button to generate a spreadsheet report on this identity.

Identities - Roles Page

When you select the **Roles** tab, the Roles page is displayed. A role is a container for all the permissions a user would need in order to perform a specific role in the organization. For more information on roles, see *Roles - Introduction*.

This page allows you to assign one or more roles to the user.


Feature	Description
Available	A list of roles that have been configured in the system. To assign a role to this user, select the role from the Available list, then click  to move it to the Members list.
Members	A list of roles that are currently assigned to this user. To remove a role from the user, select the role from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.
	Click this button to discard your changes.

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

Identities - Tokens Listing Page

When you select the **Tokens** tab, the Tokens Listing page is displayed. A token is a card or code that is assigned to a user to give them physical access permissions.

This page displays all the tokens that have been assigned to this identity.



Feature	Description
Internal Number	The number that is encoded on the card. Click the number to edit the token details.
Token Status	Current status option of the token. The options are: <ul style="list-style-type: none"> • Active • Expired • Inactive • Not Yet Active NOTE: Note the following: <ul style="list-style-type: none"> • The status is manually adjusted - it does not automatically update based on the Activate Date. For example, if the Token Status is set to Not Yet Active and the Activate Date is set to 09/13/2015, the status will not automatically update to Active on that date. • In order for a token to be active, the Token Status must be Active and the current date must fall between the Activate date and the Deactivate Date.
Deactivate Date	The date that the token will be deactivated.
Embossed Number	The number that is embossed on the card.
Last Used	The last time this token was used to gain access.
Delete	Click  to delete this token.

Feature	Description
	Click Download to download the token to all connected panels.



Identities - Token: Add New Page

When you click **Add New Token** on the Tokens page, the Token Add page is displayed. Enter the required details.

Feature	Description
Embossed Number	Enter the number to be printed on a badge. This is only required for physical access cards.
Internal Number	Enter the internal number that is assigned to this token. This value will be downloaded to panels to enable this token's access permissions.
PIN	Enter the PIN number that the user will be required to enter at a keypad card reader.
Token Status	From the drop down list, select the current status option of the token. The options are: <ul style="list-style-type: none"> Active Expired Inactive Not Yet Active <p>NOTE: Note the following:</p> <ul style="list-style-type: none"> The status must be manually adjusted - it does not automatically update based on the Activate Date. For example, if the Token Status is set to Not Yet Active and the Activate Date is set to 09/13/2015, the status will not automatically update to Active on that date. In order for a token to be active, the Token Status must be Active and the current date must fall between the Activate date and the Deactivate Date.
Issue Level	Assign a number from 0 to 9 (where 9 is the highest possible issue level).
Last Area	Indicates the last area this token gained access to.
APB Exempt	Check this box to exempt this token from anti-passback. For more information on Anti-Passback modes, see <i>Anti-Passback Modes</i> on page 63.
Trace	Check this box to enable the trace feature for this token. This will generate a trace event each time the token is used to gain access. The event can then be sent to monitoring, reported separately, and used in global I/O configurations.
Download	Check this box to allow this token to be downloaded to panels.
Never Expire	Check this box to prevent this token from expiring.
Extended door times	Check this box to give this token extended access time. Once enabled, the door remains unlocked for a longer period of time than the standard access time to accommodate users that may require more time to enter a door, such as individuals with physical disabilities. Standard and extended access times are specified on the Door Edit page.

Feature	Description
Pin exempt	Check this box to exempt this token from PIN entry at a keypad card reader.
Use/ Lose exempt	Check this box to prevent this token from expiring if you know the identity will return after an extended period of inactivity.
Issue Date	Enter the date this token was issued. Click in the field to use the calendar.
Activate Date	Enter the activation date for this token. Click in the field to use the calendar.
Deactivate Date	Enter the deactivation date for this token. Click in the field to use the calendar.
Last Door	Indicates the last door this token was used to gain access.
Last Used	Indicates the last time this token was used to gain access.
Intrusion Users: Available	List of available intrusion users that may be assigned as members. To assign as a member, select the intrusion user and click  . The intrusion user selected will be moved to the Members list and will be associated to this identity.
Intrusion Users: Members	List of intrusion users assigned to this identity. To unassign a member, select the intrusion user and click  . The intrusion user selected will be moved to the Available list and will no longer be assigned to this identity.


In addition, there are two buttons at the bottom of this page:


Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.

Identities - Token Edit Page




The Token Edit page allows you to edit the token details.

Feature	Description
Embossed Number	Enter the number to be printed on a badge. This is only required for physical access cards.
Internal Number	Enter the internal number that is assigned to this token. This value will be downloaded to panels to enable this token's access permissions.
PIN	Enter the PIN number that the user will be required to enter at a keypad card reader.
Token Status	From the drop down list, select the current status option of the token. The options are: <ul style="list-style-type: none"> • Active • Expired • Inactive

Feature	Description
	<ul style="list-style-type: none"> Not Yet Active <p>NOTE: Note the following:</p> <ul style="list-style-type: none"> The status must be manually adjusted - it does not automatically update based on the Activate Date. For example, if the Token Status is set to Not Yet Active and the Activate Date is set to 09/13/2015, the status will not automatically update to Active on that date. In order for a token to be active, the Token Status must be Active and the current date must fall between the Activate date and the Deactivate Date.
Issue Level	Assign a number from 0 to 9 (where 9 is the highest possible issue level).
Last Area	Indicates the last area this token gained access to.
APB Exempt	Check this box to exempt this token from anti-passback. For more information on Anti-Passback modes, see <i>Anti-Passback Modes</i> on page 63.
Trace	Check this box to enable the trace feature for this token. This will generate a trace event each time the token is used to gain access. The event can then be sent to monitoring, reported separately, and used in global I/O configurations.
Download	Check this box to allow this token to be downloaded to panels.
Never Expire	Check this box to prevent this token from expiring.
Extended door times	Check this box to give this token extended access time. Once enabled, the door remains unlocked for a longer period of time than the standard access time to accommodate users that may require more time to enter a door, such as individuals with physical disabilities. Standard and extended access times are specified on the Door Edit page.
Pin exempt	Check this box to exempt this token from PIN entry at a keypad card reader.
Use/ Lose exempt	Check this box to prevent this token from expiring if you know the identity will return after an extended period of inactivity.
Issue Date	Enter the date this token was issued. Click in the field to use the calendar.
Activate Date	Enter the activation date for this token. Click in the field to use the calendar.
Deactivate Date	Enter the deactivation date for this token. Click in the field to use the calendar.
Last Door	Indicates the last door this token was used to gain access.
Last Used	Indicates the last time this token was used to gain access.
Intrusion Users: Available	List of available intrusion users that may be assigned as members. To assign as a member, select the intrusion user and click  . The intrusion user selected will be moved to the Members list and will be associated to this identity.
Intrusion	List of intrusion users assigned to this identity.

Feature	Description
Users: Members	To unassign a member, select the intrusion user and click  . The intrusion user selected will be moved to the Available list and will no longer be assigned to this identity.





In addition, there are six buttons on this page:

Feature	Description
Download	Click this button to download this token to all connected panels.
1 free pass	From the drop-down list, select a door. Click 1 free pass to allow the user to enter the door without generating an APB error.
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Token	Click this button to create a new token for this user. You can assign more than one token to an identity.
	Click this button to delete the token.

Identities - Groups Page

When you select the **Groups** tab, the Groups page is displayed. Groups are sets of components that can include hardware components (cameras, doors, etc.) and/ or system components (identities, roles, etc.). For more information on groups, see *Groups - Introduction* on page 1.

This page allows you to assign the user to one ore more groups.

Feature	Description
Available	A list of groups that have been configured in the system. To assign this user to a group, select the group from the Available list, then click  to move it to the Members list.
Members	A list of groups that this user is currently assigned to. To remove this user from a group, select the group from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.
	Click this button to discard your changes.

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

Identities - Access Page


When you select the **Access** tab, a list of roles, access groups, and doors associated with this identity is displayed.

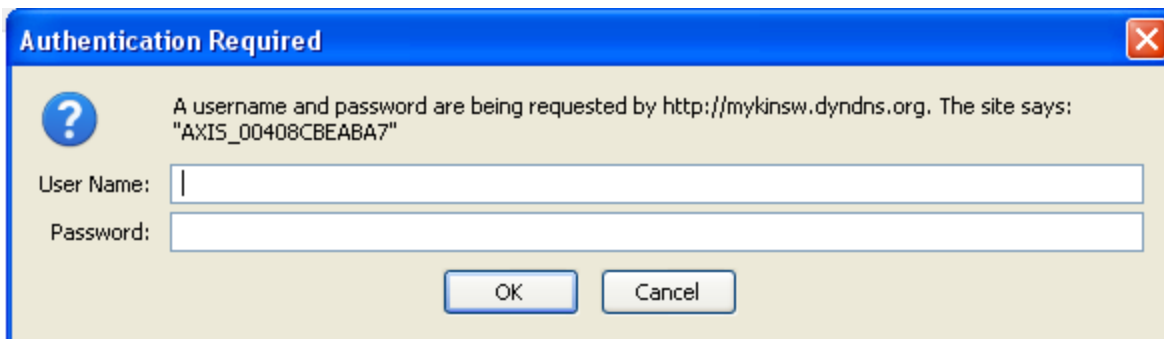
Feature	Description
Identity	The name of this identity. Click on the name to return to the Identity page.
Roles	A list of the identity's roles. Click + or - beside each role to show or hide the access groups and doors that are associated with the identity through the role.
Access Groups	A list of the access groups this identity is a member of.
Doors	A list of doors this identity can access.

Capturing an Image of an Identity

You can capture an image of a person to display on the Identity page or print on a badge.

NOTE: You must configure a badge camera before you can use this feature. For more information, see *External Systems - Adding* on page 271 and *External Systems - Defining the Badge Camera for the System* on page 272.

1. There are two ways to arrive at the Capture page:
 - From the Identities Listing page, click  from the **Image Capture** column.
 - From the Identities Listing page, click on the name of an identity, then select the **Capture** tab.
2. If the camera requires authentication, this page will not appear until you have entered your login credentials:



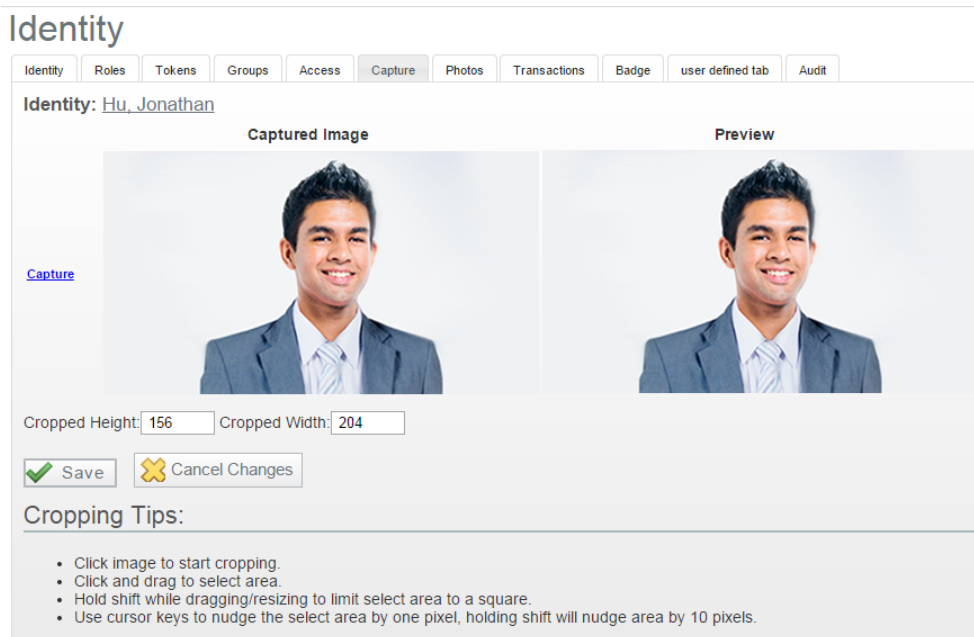
The image shows a dialog box titled "Authentication Required" with a blue header and a close button (X) in the top right corner. The main area has a light beige background. On the left, there is a blue circular icon with a white question mark. To the right of the icon, the text reads: "A username and password are being requested by http://mykinsw.dyndns.org. The site says: 'AXIS_00408CBEABA7'". Below this text are two input fields: "User Name:" followed by a white text box, and "Password:" followed by a white text box. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

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

The capture page appears.

3. Click **Capture**.

The page refreshes to show the captured image on the left and a preview of the image on the right.



4. To crop the image, click the captured image on the left.
5. Click and drag to select the cropping area.

Hold **Shift** to constrain the area selection to a square.

Use the cursor keys to nudge the area selection by one pixel. Hold **Shift** to nudge the area selection by 10 pixels.




6. Click  .

Identities - Photos Page

When you click on the **Photos** tab, the Photos page is displayed. This page allows you to upload photos of the user.

If you have not uploaded any photos yet, the page will only display the **Upload Photo** button.

Once a photo is uploaded, the page will display the image and some additional features:

Feature	Description
Primary File	Check this box to use this image on the badge template. It will also be displayed on the Identity Edit page.
	Click this button to delete the photo.
Upload a Photo	Click this button to upload a photo.
	Click this button to save your changes.
	Click this button to discard your changes.



Identities - Transactions Page

When you select the **Transactions** tab, a list of events that have been triggered by this identity is displayed.

Feature	Description
Panel Date	The date and time when the event occurred.
Priority	The importance of the event.
Event	The name of the event.
Source	The source of the event, such as a door or panel.
Source Location	The location of the event.
Card Number	The internal number of the token that generated the event.
Message	The message associated with the event.

Identities - Badge Page

When you select the **Badge** tab, the Badge page is displayed. This page allows you to create badges for the user.

Feature	Description
Badge Photo	From the drop down list, select a photo to print on the badge. Only the photos that have been previously uploaded appear in this list.
Badge Token	From the drop down list, select a token to associate with the badge. Only the tokens that have been previously defined appear in this list.
Badge Template	From the drop down list, select a badge template. Only the badge templates that have been previously defined appear in this list.
Badge Back Photo	From the drop down list, select a photo to be printed on the back of the badge. Only the photos that have been previously uploaded appear in this list.
Create Badge	Click this button to print the badge. This button is only activated if a badge printer has been configured for this system.
	Click this button to save your changes.
	Click this button to discard your changes.

If you have not created a badge template yet, a message appears: *No badge template exists.*

To create a custom badge template, click **Badge Designer**.

Identities - Audit Page

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

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

Identity Profiles

Defining an identity can take a long time, with over 25 identity fields and additional attributes such as roles, groups, tokens, and badge templates. Identity profiles provide a shortcut that can speed up the process.

Identity profiles are templates that can be applied to identities. The field values assigned in the profile will populate in the same fields for the identities. Profiles can be applied in the following ways:


- Create a new identity using a profile template. For more information, see *Adding an Identity* on page 281
- Use the batch update feature to apply an identity profile to multiple identities in a group. For more information, see *Identity Profiles - Batch Update* on page 305.

Adding an Identity Profile


To add an Identity Profile:

1. Select **Identities > Profiles** from the icon task bar.


The Identity Profiles Listing page appears.

2. Click **Add New Identity Profile**.
3. Fill out the **Name** field, then complete the page with the required details.
4. Click  .

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

3. Assign role(s) to this identity profile as required, then click  .

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

4. Enter the token details as required, then click  .
5. Select the **Groups** tab to assign this identity profile to a group.
6. Select the **Access** tab to view this identity profile's roles, access groups, and the doors it can access.

Editing an Identity Profile

To edit an existing identity profile:

1. Select **Identities > Profiles** from the icon task bar.
2. From the Identity Profiles Listing page, click on the identity profile you want to edit.

The Identity Profile: 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 profile details
 - Roles: use this page to assign this identity profile to a role.
 - Tokens: use this page to create a token template for the identity profile.
 - Groups: use this page to assign this identity profile to a group.
 - Access: use this page to view this identity profile's access privileges including roles, access groups, and doors.

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

Identity Profiles - Assigning Roles


To assign roles to an identity profile:


1. Select **Identities > Profiles** from the icon task bar.
2. From the Identity Profiles Listing page, click on the name of the identity profile you want to edit.

The Identity Profile Edit screen appears.

3. Select the **Roles** tab.

There are three sections on the Roles page:

- **Assign Equal:** When you apply the profile to an identity, they will lose all their previous roles and gain the roles specified in this list.
 - **Add:** When you apply the profile to an identity, they will keep their previous roles and gain the roles specified in this list.
 - **Remove:** When you apply the profile to an identity, they will lose the roles specified in this list.
4. To assign a role to the identity profile, select the role from the **Available** window, then click  to move it to the **Members** window.

To remove a role from the identity profile, select the role from the **Members** window, then click  to move it to the **Available** window.

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

5. When you're finished, click .

Identity Profiles - Defining Token Settings

To define token settings for this identity profile:

1. Select **Identities > Profiles** from the icon task bar.
2. From the Identity Profiles Listing page, click on the name of the identity profile you want to edit.

The Identity Profile Edit screen appears.

3. Select the **Tokens** tab.
4. If no tokens have been created yet, the Tokens Edit page appears.

If one or more tokens have already been created, click **Add New Token**.

5. Enter the details as required.

6. Click  .


For information on how to download tokens and assign badges to users, see *Searching for an Identity* on page 282.


Identity Profiles - Assigning Groups

To assign groups to an identity profile:


1. Select **Identities > Profiles** from the icon task bar.
2. From the Identity Profiles Listing page, click on the name of the identity profile you want to edit.

The Identity Profile Edit screen appears.

3. Select the **Groups** tab.
4. There are three sections on the Groups page:
 - **Assign Equal:** When you apply the profile to an identity, they will be removed from all the groups they were previously assigned to and added to the groups in this list.
 - **Add:** When you apply the profile to an identity, they will remain in all the groups they were previously assigned to and added to the groups in this list.
 - **Remove:** When you apply the profile to an identity, they will be removed from the groups in this list.
5. To assign a group to the profile, select the group from the **Available** window, then click  to move it to the **Members** window.


To remove a group from the profile, select the group from the **Members** window, then click  to move it to the **Available** window.

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

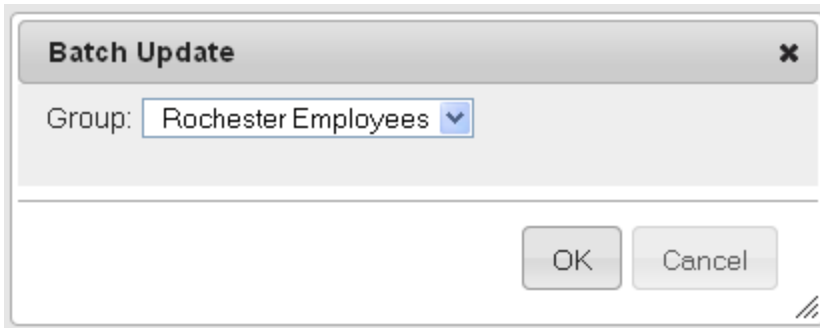
6. When you're finished, click  .

Identity Profiles - Batch Update

The Batch Update feature allows you to assign an identity profile to all members of a group.

1. Select **Identities > Profiles** from the icon task bar.
2. On the Identity Profiles Listing page, click  from the **Batch Update** column beside the identity profile you want to apply to a group.

The Batch Update dialog box popup:




3. From the **Group** drop down list, select a group.
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 identity profile's settings.

NOTE: If there are more than 10 identities in the the update will be scheduled as a batch job. This can be checked at **My Account > Batch Jobs**.


Deleting an Identity Profile


To delete an existing identity profile:

1. From the icon task bar, select **Identities > Profiles**.
2. From the Identity Profiles Listing page, click  beside the identity profile that you want to delete.
3. When the confirmation message is displayed, click **OK**.

Identity Profiles - Listing Page

When you select **Identities > Profiles** from the icon task bar, the Identity Profiles Listing page is displayed. This page lists all identity profiles that have been defined in the system.

Feature	Description
Name	The name of this identity profile. Click the name to edit the identity profile details.
Batch Update	Click  to apply this profile to all members in a group.

Feature	Description
Add New Identity Profile	Click this button to add a new identity profile.
Delete	Click  to delete this profile.

Identity Profiles - Add Page



When you click **Add New Identity Profile**, the Identity Profile Add Page appears. Enter the required identity profile details.

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 239.

Feature	Description
Identity Profile Information:	
Name	Enter a name for this identity profile. This field is required.
Title	From the drop down list, select a title for this profile.
Department	From the drop down list, select a department for this profile.
Division	From the drop down list, select a company division for this profile.
Status	From the drop down list, select the status of this profile. This field is required.
Type	From the drop down list, select the type of profile.
Issue Date	Specify the date this profile was issued. Click in the field to use the calendar.
Address Information:	
Street Address	Enter the street address where this profile lives.
City	Enter the city where this profile lives.
State	Enter the state where the profile lives.
Zip Code	Enter the zip code where the profile lives.
Site Location	From the drop down list, select the location where this profile works.
Building	From the drop down list, select the building where this profile works.
Phone	Enter this profile's personal phone number.
Work Phone	Enter this profile's work phone number.
Email Address	Enter this profile's email address.
Account Information:	
Remote Domain	From the drop down list, select an external domain for this identity to use for authentication. Only the external domains previously defined by the system appear in this list.
Allow Remote Access?	Check this box to allow this profile to access the system remotely.
Maximum Active Token	Specify the maximum number of active tokens this profile is allowed to have.
Inactivity Timer	From the drop down list, select the amount of time this profile can be inactive before it is logged out of the application.

Feature	Description
Defaults:	
Home Page	From the drop down list, select the first page this profile will see when they log into the Access Control Manager.
Items/Page	Enter the number of items this profile will see per page. The default setting is 25 items per page.
Monitor dflt rows	From the drop down list, select the number of rows this profile will see when they use the Monitor feature.
Locale	From the drop down list, select the language for this profile's user interface.
Show Timezone Offset?	From the drop down list, specify whether there is an offset for time zones.
Default Badge Template	From the drop down list, select a badge template for this profile. Only the badge templates that have been previously defined appear in this list.
Badge Camera	From the drop down list, select the camera that will be used to capture photos of members of this profile. Only the devices that have been previously configured appear in this list.
Photo Size	Enter the size you want for photos captured with the badge camera specified above. This size is in picas with the length and width separated by a comma (no spaces required).
Do Not Log REST Command	From the drop down list, specify whether to log all REST commands.

In addition, there are two buttons at the bottom of the page:

Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.

Identity Profiles - Identity Page

When you click the name of an identity profile from the Identity Profile Listing page, the Identity Profile Edit page is displayed. Select the **Identity** tab to return to this page.

On this page, you can edit general information about the identity profile.



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 239

Feature	Description
Identity Profile Information:	
Name	Enter a name for this identity profile. This field is required.
Title	From the drop down list, select a title for this profile.

Feature	Description
Department	From the drop down list, select a department for this profile.
Division	From the drop down list, select a company division for this profile.
Status	From the drop down list, select the status of this profile. This field is required.
Type	From the drop down list, select the type of profile.
Issue Date	Specify the date this profile was issued. Click in the field to use the calendar.
Address Information:	
Street Address	Enter the street address where this profile lives.
City	Enter the city where this profile lives.
State	Enter the state where the profile lives.
Zip Code	Enter the zip code where the profile lives.
Site Location	From the drop down list, select the location where this profile works.
Building	From the drop down list, select the building where this profile works.
Phone	Enter this profile's personal phone number.
Work Phone	Enter this profile's work phone number.
Email Address	Enter this profile's email address.
Account Information:	
Remote Domain	From the drop down list, select an external domain for this identity to use for authentication. Only the external domains previously defined by the system appear in this list.
Allow Remote Access?	Check this box to allow this profile to access the system remotely.
Maximum Active Token	Specify the maximum number of active tokens this profile is allowed to have.
Inactivity Timer	From the drop down list, select the amount of time this profile can be inactive before it is logged out of the application.
Defaults:	
Home Page	From the drop down list, select the first page this profile will see when they log into the Access Control Manager.
Items/Page	Enter the number of items this profile will see per page. The default setting is 25 items per page.
Monitor dfit rows	From the drop down list, select the number of rows this profile will see when they use the Monitor feature.
Locale	From the drop down list, select the language for this profile's user interface.
Show Timezone Offset?	From the drop down list, specify whether there is an offset for time zones.
Default Badge Template	From the drop down list, select a badge template for this profile. Only the badge templates that have been previously defined appear in this list.

Feature	Description
Badge Camera	From the drop down list, select the camera that will be used to capture photos of members of this profile. Only the devices that have been previously configured appear in this list.
Photo Size	Enter the size you want for photos captured with the badge camera specified above. This size is in picas with the length and width separated by a comma (no spaces required).
Do Not Log REST Command	From the drop down list, specify whether to log all REST commands.

In addition, there are three buttons at the bottom of the page:

Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.
Add New Identity Profile	Click this button to add a new identity profile.




Identity Profiles - Roles Page


When you select the **Roles** tab, the Roles page is displayed. A role is a container for all the permissions a user would need in order to perform a specific role in the organization. For more information on roles, see *Roles - Introduction* on page 1.

This page allows you to assign roles to the identity profile.

There are three sections on the Roles page:

- **Assign Equal:** When you apply the profile to an identity, they will lose all their previous roles and gain the roles specified in this list.
- **Add:** When you apply the profile to an identity, they will keep their previous roles and gain the roles specified in this list.
- **Remove:** When you apply the profile to an identity, they will lose the roles specified in this list.

Feature	Description
Available	A list of roles that have been configured in the system. To add a role to the identity profile, select the role from the Available list, then click  to move it to the Members list.
Members	A list of roles that are currently assigned to this identity profile. To remove a role from the identity profile, select the term from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.

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

Identity Profiles - Token Profile: Edit Page

When you select the **Tokens** tab within an Identity Profile, the Tokens page is displayed. A token is a card or code that is assigned to a user to give them physical access permissions.

This page allows you to configure settings that will be applied to all tokens that are created for members of this profile.

Feature	Description
Token Status	<p>From the drop down list, select the current status option of the token. The options are:</p> <ul style="list-style-type: none"> • Active • Expired • Inactive • Not Yet Active <p>NOTE: Note the following:</p> <ul style="list-style-type: none"> • The status must be manually adjusted - it does not automatically update based on the Activate Date. For example, if the Token Status is set to Not Yet Active and the Activate Date is set to 09/13/2015, the status will not automatically update to Active on that date. • In order for a token to be active, the Token Status must be Active and the current date must fall between the Activate date and the Deactivate Date.
Issue Level	Assign a number from 0 to 9 (where 9 is the highest possible issue level).
APB Exempt	Check this box to exempt this token from anti-passback. This is generally used for executive override.
Trace	Check this box to enable the trace feature for this token. This will generate a trace event each time the token is used to gain access. The event can then be sent to monitoring, reported separately, and used in global I/O configurations.
Download	Check this box to enable the download option for this token.
Never Expire	Check this box to indicate that this token never expires.
Extended door times	<p>Check this box to indicate that this token can use extended door times.</p> <p>This feature is useful for token holders with special needs.</p>
Use/ Lose exempt	
Issue Date	Enter the date this token was issued. Click in the field to use the calendar.
Activate Date	Enter the date this token is to be activated. Click in the field to use the calendar.

Feature	Description
Deactivate Date	Enter the date this token is to be deactivated. Click in the field to use the calendar.
Token Expiration Time	Enter the number of days this token will be active before it expires.





Identity Profiles - Groups Page

When you click on the **Groups** tab, the Groups page is displayed. Groups associate policies with users and security devices to establish access regulations.. For more information on policies and groups, see *Policies - Introduction* on page 1 and *Groups - Introduction* on page 1.

This page allows you to assign groups to the identity profile.

There are three sections on the Groups page:

- **Assign Equal:** When you apply the profile to an identity, they will be removed from all the groups they were previously assigned to and they will be added to the groups in this list.
- **Add:** When you apply the profile to an identity, they will remain in all the groups they were previously assigned to and they will be added to the groups in this list.
- **Remove:** When you apply the profile to an identity, they will be removed from the groups in this list.

Feature	Description
Available	A list of groups that have been configured in the system. To assign a group to this identity profile, select the group from the Available list, then click  to move it to the Members list.
Members	A list of groups that are currently assigned to this identity profile. To remove a group from this identity profile, select the group from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.
	Click this button to discard your changes.

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

Identity Profiles - Access Page

When you select the **Access** tab, a list of roles, access groups, and doors associated with this identity profile is displayed.

Feature	Description
Identity	The name of this identity profile. Click on the name to return to the Identity page.

Feature	Description
Roles	A list of the identity profile's roles. Click + or - beside each role to show or hide the access groups and doors that are associated with the identity profile through the role.
Access Groups	A list of the access groups this identity profile is a member of.
Doors	A list of doors this identity profile can access.

Collaboration - Introduction

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.

Collaborations - Adding

To add a collaboration:

1. In the top-right Setup links area, click **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 - Arcsight CEF; Events - Generic XML; Events - Milestone video; Events - Splunk; Events - Syslog	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?
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. See *Collaboration - Edit Screen* on page 324 for more detail.

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. In the top-right Setup links area, click **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 Acknowledgements	Select this checkbox to include acknowledgements.
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 318.

XML	Definition
<code><plasectrxGatewayDN> cn=544de4aa06914073,ou=gateways ,dc=plasec </plasectrxGatewayDN></code>	An internal reference for the ACM/RedCloud 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 ACM history – adjusted for ACM local time.
<code><plasectrxPaneldate>20140610085028-400 </plasectrxPaneldate></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 ACM history.
<code><plasectrxPaneldateUTC>20140610125028Z </plasectrxPaneldateUTC></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 recorded valid access of the card that was used at a door causing a ‘Local Grant’ event.
<code><plasectrxEvtypename> Intrusion</plasectrxEvtypename></code>	ACM event type category for this event. Corresponds to one of the event types defined in ACM in Settings: Event Types.
<code><plasectrxBackgroundColor> </plasectrxBackgroundColor></code>	Color assigned to the event background color (if any) for display in the ACM monitor.
<code><plasectrxForegroundColor> </plasectrxForegroundColor></code>	Color assigned to the event foreground color (if any) for display in the ACM monitor.
<code><plasectrxAckBackgroundColor> </plasectrxAckBackgroundColor></code>	Color assigned to the event background color (if any)

XML	Definition
	for display in the ACM monitor. This color corresponds to an 'acknowledged alarm' on the Alarms page.
<pre><plasectrxAckForegroundColor> </plasectrxAckForegroundColor></pre>	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.
<pre><plasectrxEventname> Input point in alarm </plasectrxEventname></pre>	Name of the event. Corresponds to one of the events defined in ACM in Physical Access: Events.
<pre><plasectrxPanelname>elevator test </plasectrxPanelname></pre>	Name of the panel that the event originated from.
<pre><plasectrxSourcename> Input on subpanel 0 Address 1 </plasectrxSourcename></pre>	Name of the source of the event.
<pre><plasectrxSourcelocation> </plasectrxSourcelocation></pre>	Location of the source of the event, as defined in the 'Location' field on the various hardware property pages.
<pre><plasectrxSourcealtname> </plasectrxSourcealtname></pre>	Applies to doors only - if the event source is a door, this is the Alt. Name as defined on the Door properties Configuration tab.
<pre><plasectrxPointaddress> 750</plasectrxPointaddress></pre>	A reference number for the event e.g. 'Input point in alarm'.
<pre><plasectrxPointDN> cn=750,ou=points,dc=plasec </plasectrxPointDN></pre>	This is the LDAP dn of the 'Input point in alarm' event, for lookup during ACM processing.
<pre><plasectrxEvtypeaddress>5 </plasectrxEvtypeaddress></pre>	This is a reference number for the event type e.g. 'Intrusion'.
<pre><plasectrxSourceDN> cn=100,cn=0,cn=9,ou=panels, cn=544de4aa06914073,ou=gateways, dc=plasec </plasectrxSourceDN></pre>	LDAP dn of the source of the event, used in ACM processing.
<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>	ACM operator that is associated with certain events e.g. an audit event for a record updated by an ACM 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

XML	Definition
	a door causing a 'local grant' event.
<pre><plasectrxCarno>0 </plasectrxCarno></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 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.

XML	Definition
<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</plasectrx
  GatewayDN>
  <cn>38901f4a95d14013</cn>
  <plasectrxRecdate>20140610055028-0700</plasectrxRecdate>
  <plasectrxPaneldate>20140610085028-0400</plasectrxPaneldate>
  <plasectrxRecdateUTC>20140610125028Z</plasectrxRecdateUTC>
  <plasectrxPaneldateUTC>20140610125028Z</plasectrxPaneldateUTC>
  <plasectrxLastacc>19700101000000Z</plasectrxLastacc>
  <plasectrxEvtypename>Intrusion</plasectrxEvtypename>
  <plasectrxBackgroundColor></plasectrxBackgroundColor>
  <plasectrxForegroundColor></plasectrxForegroundColor>
  <plasectrxAckBackgroundColor></plasectrxAckBackgroundColor>
  <plasectrxAckForegroundColor></plasectrxAckForegroundColor>
  <plasectrxEventname>Input point in alarm</plasectrxEventname>
  <plasectrxPanelname>elevator test</plasectrxPanelname>
  <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=gat
  eways,dc=plasec
  </plasectrxSourceDN>
  <plasectrxSourceCtype>40</plasectrxSourceCtype>
  <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 315.

Collaboration - Editing

To edit an existing collaboration:

1. In the top-right Setup links area, click **Collaboration**.
The Collaborations Listing page appears.
2. Click on the name of the collaboration you want to edit.
The Collaboration Edit screen appears. See *Collaboration - Edit Screen* on page 324 for more detail.
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 Server pull	Pull identities, tokens, groups, roles from a Microsoft SQL Server RDBMS store and keep the Access Control Manager identity database in sync with changes.
Events	
Events - Arcsight CEF	Transmit events in real time using the Arcsight CEF format.
Events - Generic XML	Transmit events in real time using XML.
Events - Milestone Video	Transmit events in real time and insert the Milestone video database.
Events - Syslog	Transmit events in real time to a Syslog utility.
Events - Splunk	Produces messages in Splunk format. Splunk is a log aggregation product.


Collaboration - Running

To run a collaboration:

1. In the top-right Setup links area, click **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. In the top-right Setup links area, click **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. In the top-right Setup links area, click **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 event types you want to transfer, then click .

The event type is added to the Members list to show that it is now assigned.

To remove an event type from the collaboration, select the event type from the Members list, then click .

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



5. Click .

Collaboration - Listing Page

When you click **Collaboration** in the top-right Setup links area, the Collaboration Listing page is displayed.

The Collaboration Listing page lists all Collaborations that have been configured in the system.

Feature	Description
Name	The name of this collaboration. Click the name to edit the collaboration details.
Installed	Indicates if this collaboration is active. Check the icon to indicate that this collaboration is currently operational and available to the system.
Type	The collaboration type that is assigned to this collaboration.
Last Transfer	The date and time when the last transfer occurred.
Preview	Click Preview to view this collaboration's log. NOTE: Previews are not available for Identity CSV imports. NOTE: Log files are available on the Appliance: Logs page; for: <ul style="list-style-type: none"> • Imports, the log file is named identity_collab.txt.

Feature	Description
	<ul style="list-style-type: none"> Exports, a log file is created with the same name as the export name.
Run	<p>Click  to run this collaboration.</p> <p>This icon is only displayed for collaboration types that support this operation, such as pulls and uploads.</p>
Delete	Click  to delete this collaboration.
Add New Collaboration	Click this button to create a new collaboration.
Create New Report	Click this button to generate a PDF summary of all the collaborations.

Collaboration - Add Page

When you click **Add New Collaboration** from the Collaborations Listing page, the Collaboration Add page displays.

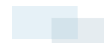
The following features display when you first access the page:



Feature	Description
Name	Enter the name of this collaboration.
Appliance	<p>From the drop down list, select the appliance that will be associated to this collaboration.</p> <p>Only the appliances that have been previously configured appear in this list.</p>
Type	<p>From the drop down list, select the collaboration type.</p> <p>Depending on the type of collaboration you specify, additional fields will appear below.</p>
Installed	Check this box to indicate that this collaboration is currently operational and available to the system.
Partitions	<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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</p>

The following features will display when you select the collaboration type (for more information, refer to *Collaborations - Adding* on page 313):

Feature	Description
Partitions to Export	<p>Filter results by exporting Identities who are members of selected partitions.</p> <p>Displays only for the Identity CSV Export collaboration type.</p>
Host	<p>If you are using Windows Share, enter the host name where the file is located. Separate the directory with a forward slash (/) i.e. host/share.</p> <p>If you are using SCP, enter the host name without the directory.</p>

Feature	Description
	Displays for the following collaboration types: Events - Arcsight CEF; Events - Generic XML; Events - Milestone video; Events - Pelco Digital Sentry; Events - Pelco Endura; Events - Splunk; Events - Syslog; Identity CSV Export; Identity CSV Recurring; Identity LDAP pull; Identity Oracle RDBMS pull and Identity SQL Server pull.
Port Number	Port to which the collaboration will connect on the remote server. If empty, uses known TCP defaults (SMB:445, SCP:22). Displays for the following collaboration types: Events - Arcsight CEF; Events - Generic XML; Events - Milestone video; Events - Pelco Digital Sentry; Events - Pelco Endura; Events - Splunk; Events - Syslog; Identity CSV Export; Identity CSV Recurring; Identity LDAP pull; Identity Oracle RDBMS pull and Identity SQL Server pull.
Require TCP	Check this box to indicate that the transfer occurs over TCP. Displays for the following collaboration types: Events - Arcsight CEF; Events - Generic XML; Events - Milestone video; Events - Pelco Digital Sentry; Events - Pelco Endura and Events - Splunk; Events - Syslog.
Include Primary Photo	Check the box to include the primary photo (or first photo if no primary photo is indicated) in the import/export. For imports, this is only to be used when you are importing data that has been exported using the Identity - CSV Export Collaboration. Displays for the following collaboration types: Identity CSV Export and Identity CSV Recurring.
Include Roles	Check the box to include roles in the export. Displays only for the Identity CSV Export collaboration type.
Location Type	Select the location type for this CSV file. Displays for identity CSV Recurring and Identity CSV Export collaboration types.
User Name	User Name that the collaboration will use to login to the remote server. Displays for the following collaboration types: Identity CSV Export; Identity CSV Recurring; Identity Oracle RDBMS pull; and Identity SQL Server pull.
Password	User password that the collaboration will use to login to the remote server. Displays for the following collaboration types: Identity CSV Export; Identity CSV Recurring; Identity Oracle RDBMS pull; and Identity SQL Server pull.
Location	Click Browse to search for and select the directory to export CSVs to/import CSVs from. NOTE: The export location is a directory, while the import location points to a file. Displays for the following collaboration types: Identity CSV Export and Identity CSV Recurring.
Delimiter	Select the delimiter of the file. NOTE: Delimiter, Text Qualifier and Date Format are used to tell the import how the CSV file has been prepared. When importing data exported from ACM, do not change the default values. Otherwise, a delimiter can be selected. Displays for the following collaboration types: Identity CSV one-time Long format and





Feature	Description
	Identity CSV Recurring.
Text Qualifier	Select the character used to differentiate the data from the delimiter. Displays for the following collaboration types: Identity CSV one-time Long format and Identity CSV Recurring.
CSVFile	Click Browse to search for and select a CSV file. Displays for Identity CSV one-time Long format and Identity CSV one-time Short format.
Date Format	Select date format (e.g. MDY). Displays only for the Identity CSV Recurring collaboration type and Identity CSV one-time Long format.
Bind DN	Enter the distinguished name (DN) used to log in to the server. Displays only for the Identity LDAP pull collaboration type.
SSL	Check this box to indicate that the data transfer is conducted using SSL. Displays only for the Identity LDAP pull collaboration type.
Instance	Enter the instance within the database to connect to. Displays for the Identity Oracle RDBMS pull and Identity SQL Server pull collaboration types.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Edit Screen

When you click on a collaboration from the Collaborations Listing page, the Collaboration Edit screen is displayed.

This screen displays options that are specific to the type of collaboration you are working with. The same collaboration properties appear at the top of each page:

Feature	Description
Name	Enter the name of this collaboration.
Installed	Check this box to indicate that this collaboration is currently operational and available to the system.
Appliance	ACM appliance this applies to. This is a read-only field.
Type	The collaboration type. This is a read-only field.
Installed	Check this box to indicate installation status.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.

Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.

For more information about different collaboration types, see the links below.

Collaboration - ArcSight™ CEF Edit Screen

This collaboration type pushes events from the Access Control Manager using the Arcsight CEF format.

When you select an **Events -ArcSight CEF** collaboration type from the Collaborations Listing page, the Collaboration Edit Screen will have the following tabbed pages:

- ArcSight CEF: use this page to edit general information about the collaboration including the host name and port number.
- Events: use this page to specify which event types to transfer and what time interval to run transfers.

The ArcSight CEF page has the following fields. Edit the details as required.

Feature	Description
Host	Enter the host of the application. Include the domain and computer name where appropriate.
Port Number	Enter the port number of the host that will receive the data.
Require TCP	Check this box to indicate that the transfer occurs over TCP.

Collaboration - CSV One-time Edit screen


This collaboration type pulls identity-related attributes from a CSV file into the Access Control Manager database.


When you select an **Identity - CSV One-Time Short format** or **Identity - CSV One-Time Long format** collaboration type from the Collaborations Listing page, the Collaboration Edit Screen is displayed.

Short Format

If you specified **Identity - CSV One-Time Short format** as the collaboration type, the CSV Upload page will have the following fields. Edit the details as required.



NOTE: The CSV One-Time Short format creates a new identity instance each time it runs. Therefore you must delete the identity that you are updating to avoid duplicates. The long format is recommended because it overwrites previous data without creating duplicates.

Feature	Description
CSV File	Click Choose File and navigate the directory to find the CSV file you want to upload. Click Open to select the file.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.

Long Format

If you specified **Identity - CSV One-Time Long format** as the collaboration type, the edit screen will have the following fields. Edit the details as required.

Feature	Description
Delimiter	Select the delimiter of the file.
Text Qualifier	Select the character used to differentiate the data from the delimiter.
Date Format	Select the date format used in the file.
CSV File	Click Browse and navigate the directory to find the CSV file you want to upload. Click Open to select the file.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Preparing CSV files

It is important to format the data in a CSV file correctly. Data should be entered in a spreadsheet with column headers in the first row that match the name of each field in the Access Control Manager that you want to map to. All values must be an exact match, including spelling, spacing, and case-sensitivity, with the exception of UDF fields which are prefixed with 'UDF_'.

Avoiding Duplicate Identities and Errors

Running the identity CSV upload twice may result in identities being duplicated. Duplicate identities can be deleted in the Identities Listing page. If an error occurs, a message will appear with the approximate CSV line location. This will help locate the error and start the CSV upload at the point where the last record failed.

Do not use the pound symbol (#) in the CSV file, otherwise an error will occur.

Collaboration - Fields

Mandatory Identity Fields

The following fields are mandatory:

Feature	Description
External System ID	Enter the identity's external system ID. Use any combination of alphanumeric characters except the pound sign (#). The External System ID is used as a key to link existing data. Subsequent imports will not duplicate existing identities unless you change their External System ID.
First Name	Enter the identity's last name.

Feature	Description
	Use any combination of alphanumeric characters except the pound sign (#).
Last Name	Enter the identity's first name. Use any combination of alphanumeric characters except the pound sign (#).

Optional Identity Fields

Feature	Description
Middle Name	Enter the identity's middle name. Use any combination of alphanumeric characters except the pound symbol (#).
Title	Enter the identity's title. Use any combination of alphanumeric characters except the pound symbol (#).
Address	Enter the identity's street address. Use any combination of alphanumeric characters except the pound symbol (#).
City	Enter the identity's city. Use any combination of alphanumeric characters except the pound symbol (#).
State	Enter the identity's state. Use any combination of alphanumeric characters except the pound symbol (#). It must be the state's full name starting with a capital letter for each word. For example: North Carolina.
Zip	Enter the identity's zip code. Use any combination of alphanumeric characters except the pound symbol (#).
Phone	Enter the identity's phone number. Use any combination of alphanumeric characters except the pound symbol (#). For Example: (303) 555-1234, 303.555.1234, 303-555-1234, 303 555 1234.
Work Phone	Enter the identity's work phone number. Use any combination of alphanumeric characters except the pound symbol (#). For Example: (303) 555-1234, 303.555.1234, 303-555-1234, 303 555 1234.
Email Address	Enter the identity's email address. Use any combination of alphanumeric characters except the pound symbol (#).
Department	Enter the identity's department. Use any combination of alphanumeric characters except the pound symbol (#).
Division	Enter the identity's division. Use any combination of alphanumeric characters except the pound symbol (#).
Site Location	Enter the identity's site location.

Feature	Description
	Use any combination of alphanumeric characters except the pound symbol (#).
Building	Enter the identity's building. Use any combination of alphanumeric characters except the pound symbol (#).
Type	Enter the identity's type. Use any combination of alphanumeric characters except the pound symbol (#).
Status	Enter the identity's status. Use 1 (for Active) or 2 (for Inactive).
Roles	Enter the identity's role. Use any combination of alphanumeric characters except the pound symbol (#). NOTE: Only one role can be imported
Load Date	Enter the identity's issue date. Use the date format: mm/dd/yyyy.
Partition	Enter the name of a partition. The name must exactly match the name of an existing partition.

Token Fields

Feature	Description
Token Unique	Enter the token's unique ID. Use any combination of alphanumeric characters except the pound sign (#). The Token Unique is used as a key to link existing data. You may re-use the identity's External System ID.
Internal Number	Enter the token's internal number. Use any combination of numbers. Leading zeros are not significant.
Embossed Number	Enter the token's embossed number. Use any combination of alphanumeric characters except the pound sign (#).
Token Status	Enter the token's status. Use 1 (for Active) or 2 (for Inactive).
Issue Level	Enter the token's issue level. Use any combination of numbers. Leading zeros are not significant.
PIN	Enter the token's PIN. Use any combination of numbers. Leading zeros are significant.
Issue Date	Enter the token's issue date. Use the date format: mm/dd/yyyy.

Feature	Description
Activation Date	Enter the token's activation date. Use the date format: mm/dd/yyyy.
Deactivation Date	Enter the token's deactivation date. Use the date format: mm/dd/yyyy.
VIP	Specify if the token is APB exempt. Use 1 or y or t (for True) or any other value (for False).
Never Expire	Specify if the token never expires. Use 1 or y or t (for True) or any other value (for False).
Download	Specify if the token can be downloaded to panels. Use 1 or y or t (for True) or any other value (for False).
Ext Access	Specify if the token has extended door time. Use 1 or y or t (for True) or any other value (for False).

Collaboration - CSV Upload

To create a CSV file:

1. Prepare the data in a spreadsheet.

Column headers must be in the first row and match the name of each field in the Access Control Manager that you want to map to.

2. Export the data as a CSV file.

To upload a CSV file:

1. In the top-right Setup links area, click Collaboration.
2. From the Collaborations Listing page, click Add New Collaboration.
3. Enter a name for the collaboration.
4. In the Type field, select either **Identity CSV One-Time Short format** or **Identity CSV One-Time Long format**.
5. Complete the remainder of the page as required.
6. Click **Choose File** and navigate the directory to find the CSV file you want to upload.

Click **Open** to select the file.

7. Click  .

Collaboration - CSV Upload Template

The comma-separated values (CSV) file must include headers for each attribute you want to include in the database.

CSV One Time Short Format Collaboration

The following columns are included:

Column	Example	Notes
External System ID	1234	
Load Date	06/08/2015	
First Name	John	
Last Name	Smith	
Middle Name	Stout	
Address	123 Pine Hurst	
State	Ohio	State or Province
City	Dayton	
Zip	45323	Zip or postal code
Phone	555-232-1244	
Work Phone	555-100-1356	
Email Address	jsmith@bear.org	
Status	Active	
Title	Staff	
Department	IT	
Division	Federal Sector	
Type	Employee	
Site Location	North	
Building	Main Office	

CSV One Time Long Format Collaboration

The following columns are included:

Column	Example	Notes
External System ID	1234	
Load Date	06/08/2015	Format mm/dd/yyyy.
First Name	John	
Last Name	Smith	
Middle Name	Stout	
Address	123 Pine Hurst	
City	Dayton	
State	Ohio	
Zip	45323	Zip or postal code

Column	Example	Notes
Phone	555-232-1244	
Work Phone	555-100-1356	
Email Address	jsmith@bear.org	
Status	Active	
Title	Staff	
Department	IT	
Division	Federal Sector	
Type	Employee	
Site Location	North	
Role	Admin	
Building	Main Office	
Token Unique	12345678	
Internal Number	9874563221	Internal Number may not be used if the access badge or card does not have an internal number.
Embossed Number	42	Embossed Number may not be used if the access badge or card does not have a separate printed number.
Token Status	Active	
Issue Level	5	
PIN	1234567	
Issue Date	02/28/2012	Format mm/dd/yyyy.
Activation Date	02/28/2012	Format mm/dd/yyyy.
Deactivation Date	12/31/2037	Format mm/dd/yyyy.
VIP	True	VIP defines if the user is exempt from anti-passback.
Never Expire	False	
Download	02/02/2015	When the identity token was last downloaded. Format mm/dd/yyyy.
Ext Access	Active	
Partition	South Region	
UDF_Shift	Night	UDF_ prefixed fields are user defined fields and may be different from system to system.
UDF_DateofBirth	1977-09-08	UDF_ prefixed fields are user defined fields and may be different from system to system.

CSV Recurring Collaborations

Column	Example	Notes
Export UUID	d17c25d2-331f-1035-9345-	



Column	Example	Notes
	4b51cd8b394b	
External System ID	1234	
Status	1	
Type	Employee	
Load Date	06/08/2015	Format mm/dd/yyyy.
Partition	South Region, East Region	If multiples used separate using a comma (,).
First Name	John	
Last Name	Smith	
Middle Name	Stout	
Address	123 Pine Hurst	
City	Dayton	
State	Ohio	
Zip	45323	Zip or postal code
Phone	555-232-1244	
Work Phone	555-100-1356	
Email Address	jsmith@bear.org	
Title	Staff	
Department	IT	
Division	Federal Sector	
Site Location	North	
Building	Main Office	
Roles	Admin, Executive, Remote Worker	If multiples used separate using a comma (,).
Token Unique	12345678	
Internal Number	9874563221	Internal Number may not be used if the access badge or card does not have an internal number.
Embossed Number	42	Embossed Number may not be used if the access badge or card does not have a separate printed number.
Token Status	Active	
Issue Level	5	
PIN	1234567	
Issue Date	02/28/2012	Format mm/dd/yyyy.

Column	Example	Notes
Activation Date	02/28/2012	Format mm/dd/yyyy.
Deactivation Date	12/31/2037	Format mm/dd/yyyy.
VIP	True	VIP defines if the user is exempt from anti-passback.
Never Expire	False	
Download	02/02/2015	When the identity token was last downloaded. Format mm/dd/yyyy.
Trace	False	
Ext Access	Active	
UDF_Shift	Night	UDF_ prefixed fields are user defined fields and may be different from system to system.
UDF_DateofBirth	1977-09-08	UDF_ prefixed fields are user defined fields and may be different from system to system.

Collaboration - LDAP Pull Edit Screen

If you specified **Identity LDAP Pull** as the collaboration type, the Collaboration Edit screen will have multiple tabbed pages.

Collaboration - Milestone™ Edit Screen

This collaboration type pushes events from the Access Control Manager to a Milestone video database.

When you select an **Events - Milestone** collaboration type from the Collaborations Listing page, the Collaboration Edit Screen will have the following tabbed pages:

- Milestone: use this page to edit general information about the collaboration including the host name and port number.
- Events: use this page to specify which event types to transfer and what time interval to run transfers..

The Milestone page has the following fields. Edit the details as required.

Feature	Description
Host	Enter the host of the application. Include the domain and computer name where appropriate.
Port Number	Enter the port number of the host that will receive the data.
Require TCP	Check this box to indicate that the transfer occurs over TCP.

Collaboration - Oracle™ RDBMS Pull Edit Screen

This collaboration type pulls identity-related attributes periodically from an Oracle RDBMS store into the Access Control Manager database .

When you select an **Identity - Oracle RDBMS pull** collaboration type from the Collaborations Listing page, the Collaboration Edit Screen will have the following tabbed pages:

- Source: use this page to edit general information about the collaboration, including host information and login credentials.
- Schedule: use this page to schedule how often you want to run a transfer.
- Identities: use this page to specify which identity attributes to pull from the Oracle database.
- Tokens: use this page to specify which token attributes to pull from the Oracle database.
- Blob: use this page to specify what Binary Large Object (image) data to pull from the SQL database.
- User Defined: use this page to specify which user-defined attributes to pull from the Oracle database.
- Roles: use this page to specify which role attributes to pull from the Oracle database.

Collaboration - SQL Server Pull Edit Screen

This collaboration type periodically pulls identity-related attributes from a Microsoft SQL Server RDBMS store into the Access Control Manager database.

When you select an **Identity - SQL Server pull** collaboration type from the Collaborations Listing page, the Collaboration Edit Screen will have the following tabbed pages:

- Source: use this page to edit general information about the collaboration, including host information and login credentials.

NOTE: Keep Identity data and Token data on separate tables or views in the SQL database.

- Schedule: use this page to schedule how often you want to run a transfer.
- Identities: use this page to specify which identity attributes to pull from the SQL database.
- Tokens: use this page to specify which token attributes to pull from the SQL database.
- Blob: use this page to specify what Binary Large Object (image) data to pull from the SQL database.
- User Defined: use this page to specify which user-defined attributes to pull from the SQL database.
- Roles: use this page to specify which role attributes to pull from the SQL database.

NOTE: Ensure any individual images to be imported are not over 1MB.

Collaboration - Syslog Edit Screen

This collaboration type pushes events from the Access Control Manager to a Syslog utility.

When you select an **Events - Syslog** collaboration type from the Collaborations Listing page, the Collaboration Edit Screen will have the following tabbed pages:

- Syslog: use this page to edit general information about the collaboration including the host name and port number.
- Events: use this page to specify which event types to transfer and what time interval to run transfers.

The Syslog page has the following fields. Edit the details as required.

Feature	Description
Host	Enter the host of the application. Include the domain and computer name where appropriate.
Port Number	Enter the port number of the host that will receive the data.
Require TCP	Check this box to indicate that the transfer occurs over TCP.

Collaboration - XML Edit Screen

This collaboration type pushes events from the Access Control Manager using XML.

When you select an **Events - Generic XML** collaboration type from the Collaborations Listing page, the Collaboration Edit Screen will have the following tabbed pages:

- XML: use this page to edit general information about the collaboration including the host name and port number.
- Events: use this page to specify which event types to transfer and what time interval to run transfers.

The XML page has the following fields. Edit the details as required.

Feature	Description
Host	Enter the host of the application. Include the domain and computer name where appropriate.
Port Number	Enter the port number of the host that will receive the data.
Require TCP	Check this box to indicate that the transfer occurs over TCP.

Collaboration - Identity CSV Export Edit Screen

The identity export collaboration can be used to export all identity data into a common file format (CSV) so it can be used by other applications. Photographs will be exported into a photo folder in the directory specified in the collaboration. The export can also be used by a separate Access Control Manager to keep identity data synchronized using the Recurring CSV import (see *Collaboration - Identity CSV Recurring Edit Screen* on the next page).



When you select an **Identity - CSV Export** collaboration type from the Collaborations Listing page, the Collaboration Edit screen will have the following tabbed pages:

- CSV Export: use this page to edit general information about the collaboration, including location type, login credentials, and host/domain.
- Schedule: use this page to schedule how often you want to run the export.

Important: Data exported from one ACM instance will be considered the Master Data when imported into another ACM. Any manual updates made to previously imported identities will be overwritten during the import.

The Identity CSV Export Collaboration: Edit page has the following fields. Edit the details as required.

Feature	Description
Name	Name of the export.
Appliance	ACM appliance this applies to. This is a read-only field.
Type	Collaboration type. This is a read-only field.
Installed	Check the box for collaborations to run. If this is not checked then the collaboration is disabled.
Partitions	Users who have access to selected partitions, will also have access to the collaboration. For further information on partitions, refer to Partitions - Introduction.
Partitions to Export	Filter results by exporting identities who are included in selected partitions.

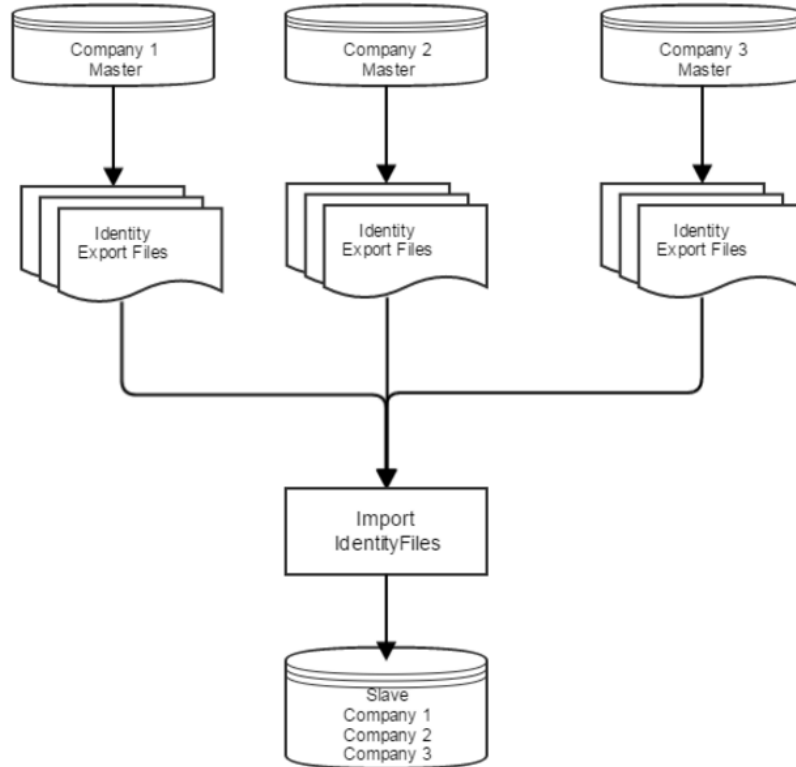
Feature	Description
Include Primary Photo	Check the box to include the primary photo (or first photo if no primary photo is indicated) as part of the export.
Include Roles	Check the box to include roles as part of the export.
Location Type	Select the location type (either Windows Share or SCP) for the CSV file.
Host	If you are using Windows Share , enter the host name where the file is located. Separate the directory with a forward slash (/). If you are using SCP , enter the host name without the directory.
Domain name	Domain for the export destination. Only displays if Windows Share is selected as the host.
Port Number	Port to which the collaboration will connect on the remote server. If empty, uses known TCP defaults (SMB:445, SCP:22).
User Name	User Name that the collaboration will use to login to the remote server.
Password	User password that the collaboration will use to login to the remote server.
Location	Click Browse to search for and select the location to export to. NOTE: You cannot export to the same remote directory specified in an already existing export collaboration. The location must be unique as the export file always has the same name. If the location entered does not already exist, it will be created by the export.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Identity CSV Recurring Edit Screen

This collaboration type imports identity and token data via a CSV file into the Access Control Manager database. This can be either:

- **CSV Recurring Standard Import:** A standard CSV import can be done by preparing the CSV file with the identity data to be imported. If you wish to include photos with a standard import, contact Technical Support.
- **CSV Recurring from an ACM Identity Export:** To synchronize identity data between multiple disparate installations of ACM.

For example:



To import identity data and/or photos that were previously exported from separate ACM. Note that while the CSV file format is similar, a new field, Export UUID (Universally Unique Identifier) has been introduced to ensure uniqueness across multiple ACM installations. The standard import only requires the External Id to be unique, but that cannot be enforced in this scenario. The Export UUID field will appear as the first column in the exported CSV file. For more information, refer to:

- *Collaboration - Preparing CSV files* on page 326
- *Collaboration - CSV Upload Template* on page 329

It is important to note that if the identity already exists in the importing ACM, a duplicate identity will be created the first time the collaboration is run. If you are using this feature, it is recommended you first delete those identities before you proceed with the import. This can be done using the “Destroy Batch” feature or the delete feature on the Identity listings page. Once the UUID has been established for an identity, any ensuing imports will simply update the identity data.

NOTE: If user defined fields (UDFs), roles or partitions are included in the CSV file, then these should exist in ACM prior to importing. If they do not exist then they will not be populated.



NOTE: There are limits relating to imports:

- When importing identities there is a 49 character limit for the each of the identity name fields (i.e. first, middle and last name). If the name exceeds 49 characters then it will be truncated after being imported.
- There is a limit for large UDF integer values. The maximum supported integer value is 999999999999999999. Any values higher than this will be truncated after being imported.

When you select an **Identity - CSV Recurring** collaboration type from the Collaborations Listing page, the Collaboration Edit screen will have the following tabbed pages:



- CSV Recurring: use this page to edit general information about the collaboration, including location type, login credentials, and host/domain.
- Schedule: use this page to schedule how often you want to run the import.

The Identity CSV Recurring Collaboration: Edit page has the following fields. Edit the details as required.

Feature	Description
Name	Name of the import.
Appliance	ACM appliance this applies to. This is a read-only field.
Type	Collaboration type. This is a read-only field.
Installed	Check the box for collaborations to run. If this is not checked then the collaboration is disabled.
Include Primary Photo	Check the box to include the primary photo (or first photo if no primary photo is indicated) in the import/export. For imports, this is only to be used when you are importing data that has been exported using the Identity - CSV Export Collaboration. NOTE: Pictures should be in JPEG format.
Location Type	Select the location type for this CSV file.
Host	If you are using Windows Share , enter the host name where the file is located. Separate the directory with a forward slash (/). If you are using SCP , enter the host name without the directory.
Domain name	Domain for the import location. Only displays if Windows Share is selected as the location type.
Port Number	Port to which the collaboration will connect on the remote server. If empty, uses known TCP defaults (SMB:445, SCP:22).
User Name	User Name that the collaboration will use to login to the remote server.
Password	User password that the collaboration will use to login to the remote server.
Location	Click Browse to search for and select the CSV file to import from.
Delimiter	Delimiter of the file. NOTE: Delimiter, Text Qualifier and Date Format are used to tell the import how the CSV file has been prepared. When importing data exported from ACM, do not change the default values. Otherwise, a delimiter can be selected.
Text Qualifier	Character used to differentiate the data from the delimiter. NOTE: If this field is left blank, the default qualifier is " .
Date Format	Date format used in the file.
	Click this button to save your changes.
	Click this button to discard your changes.


Collaboration - Source Page


When you select the **Source** tab from the Collaboration Edit screen, the Source page is displayed. Depending on the type of collaboration, this page may have any of the following fields:

Feature	Description
Host	Enter the host name of the external database. Include the domain and computer name where appropriate.
Port Number	Enter the port number where data will be pulled from the external database.
User Name	Enter the user name that is required to access the external database. This is SQL or Oracle only.
Password	Enter the password that is required to access the external database.
Instance	Enter the instance within the database to connect to. This is Oracle only.
SSL?	Check this box to indicate that the data transfer is conducted using SSL. This is LDAP only.
Bind DN	Enter the distinguished name (DN) used to log in to the server. This is LDAP only.
Database	Select the name of the external database that you want to transfer. This is SQL only.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Schedule Page



When you click the **Schedule** tab from Collaboration Edit screen, the Schedule page is displayed. This page allows you to specify how often you want transfers to occur.

Feature	Description
Every	Specify how often you want the transfer to occur. Enter the value and select the appropriate units. NOTE: Transfers will only take place between the Start and Ending dates specified (inclusive of the actual dates).
Start date	Enter the date that you want transfers to begin. Click this field to use the calendar.
Ending date	Enter the date that you want transfers to end. Click this field to use the calendar.
Last transfer	A read-only field that shows the date/time of the last successful transfer.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.

Collaboration - Identity CSV Export Schedule Page



When you click the **Schedule** tab from Collaboration Edit screen when editing a CSV Export, the Schedule page is displayed. This page allows you to specify how often you want transfers to occur.

Feature	Description
Name	Name of the export.
Appliance	ACM appliance this applies to. This is a read-only field.
Type	Collaboration type. This is a read-only field.
Installed	Check the box for collaborations to run. If this is not checked then the collaboration is disabled.
Partitions	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 appear in this list. If no partitions are defined for this system, this pane is hidden.
Every	Specify how often you want the transfer to occur. Enter the value and select the appropriate units. NOTE: Transfers will only take place between the Start and Ending dates specified (inclusive of the actual dates).
Start date	Enter the date that you want transfers to begin. Click this field to use the calendar.
Ending date	Enter the date that you want transfers to end. Click this field to use the calendar.
Last transfer	The date the last successful export occurred.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Identity CSV Recurring Schedule Page



When you click the **Schedule** tab from Collaboration Edit screen when editing a CSV recurring import, the Schedule page is displayed. This page allows you to specify how often you want transfers to occur.

Feature	Description
Name	Name of the import.
Appliance	ACM appliance this applies to. This is a read-only field.
Type	Collaboration type. This is a read-only field.
Installed	Check the box for collaborations to run. If this is not checked then the collaboration is disabled.
Every	Specify the frequency of the transfer. Enter the value and select the appropriate units.

Feature	Description
	NOTE: Transfers will only take place between the Start and Ending dates specified (inclusive of the actual dates).
Start date	Enter the date that you want transfers to begin. Click this field to use the calendar.
Ending date	Enter the date that you want transfers to end. Click this field to use the calendar.
Last transfer	The date the last successful import occurred.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Identities Page



When you select the **Identities** tab from the Collaboration Edit screen, the Identities page is displayed. This page allows you to specify how to map the data to identity attributes in the Access Control Manager.

Feature	Description
Table	Select the external database table to pull data from.
Filter	Enter the criteria for selecting attributes within the scope of available identities.
Attributes	Specify which identity attributes you want to pull. <ul style="list-style-type: none"> If the fields are drop down lists, select the option you want to map to each field. If the fields accept strings, enter the value you want to map to each field. Ensure that your entry is identical to the value in the external database, including spelling, spacing, and case-sensitivity.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Tokens Page



When you select the **Tokens** tab from the Collaboration Edit screen, the Tokens page is displayed. This page allows you to specify how to map the data to token attributes in the Access Control Manager.

Feature	Description
Table	Select the external database table to pull data from.
Base DN	Enter the distinguished name (DN) of the entry where you want the search to start from. This is LDAP only.
Filter	Enter the criteria for selecting attributes within the scope of available tokens.
Attributes	Specify which token attributes you want to pull. <ul style="list-style-type: none"> If the fields are drop down lists, select the option you want to map to each field.

Feature	Description
	<ul style="list-style-type: none"> If the fields accept strings, enter the value you want to map to each field. Ensure that your entry is identical to the value in the external database, including spelling, spacing, and case-sensitivity.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Blob Page



When you select the **Blob** tab from Collaboration Edit screen, the Blob page is displayed. This page allows you to specify how to import image data to the Access Control Manager.

Feature	Description
Base DN	Enter the distinguished name (DN) used to log in to the server. This is LDAP only.
Table	Select the external database table to pull data from.
Filter	Enter the criteria for selecting elements within the scope of available blobs (binary large objects).
Attributes:	
Primary Image	Check this box to select this image as the primary image.
Identity	Select the same option that you mapped to the Identity Unique field on the Identities page.
Image	Select the option you want to import into the identity images.
Type	Select the criteria for selecting the type of images to be transferred.
Last Update	Select the criteria for the last update.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - User Defined Page



When you select the **User Defined** tab from the Collaboration Edit screen, the User Defined page is displayed. This page allows you to specify how to import user-defined data into the Access Control Manager.

Feature	Description
Table	Select the external database table to pull data from.
Filter	Enter the criteria for selecting elements within the scope of available user definitions.
Attributes	Specify which user-defined attributes you want to pull: <ul style="list-style-type: none"> If the fields are drop down lists, select the option you want to map to each field. If the fields accept strings, enter the value you want to map to each field. Ensure that your

Feature	Description
	entry is identical to the value in the external database, including spelling, spacing, and case-sensitivity.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Roles Page





When you select the **Roles** tab from Collaboration Edit screen, the Roles page is displayed. This page allows you to specify how to map the data to role attributes in the Access Control Manager.

Feature	Description
Table	Select the external database table to pull data from.
Filter	Enter the criteria for selecting elements within the scope of available roles.
Create Access Group	Check this box to create a new access group for this role.
Attributes	Specify which role attributes you want to pull: <ul style="list-style-type: none"> • If the fields are drop down lists, select the option you want to map to each field. • If the fields accept strings, enter the value you want to map to each field. Ensure that your entry is identical to the value in the external database, including spelling, spacing, and case-sensitivity.
	Click this button to save your changes.
	Click this button to discard your changes.

Collaboration - Events Page

When you select the **Events** tab from the Collaborations Edit screen, the Events page is displayed. This page allows you to specify which event types to transfer and what time interval to run transfers. Depending on the type of collaboration, this page may have any of the following fields:

Feature	Description
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed. Events will be pushed during the time interval specified by this schedule.
Send Acknowledgments	Check this box to send notifications when alarms have been acknowledged.
Send Clears	Check this box to send notifications when events have been cleared.
Send Notes	Check this box to send notes along with event transfers.









Feature	Description
Available	<p>A list of event types that have been configured in the system.</p> <p>To push an event type, select the event type from the Available list, then click  to move it to the Members list.</p>
Members	<p>A list of event types that are currently being pushed by this collaboration.</p> <p>To remove an event type from the list, select the event type from the Members list, then click  to move it to the Available list.</p>
	Click this button to save your changes.
	Click this button to discard your changes.

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

Roles - Main Screen

The Roles feature allows you to define the access control permissions and application permissions that are available in the system.

When you click on Roles from the icon task bar, a row of sub-options appears below the icon:

-  — Click this icon to display the Roles Listing page.
-  — Click this icon to display the Policies Listing page.
-  — Click this icon to display the Groups Listing page.
-  — Click this icon to display the Access Groups Listing page.
-  — Click this icon to display the Delegations Listing page.
-  — Click this icon to display the Partitions Listing page.
-  — Click this icon to display the Routing Groups Listing page.
-  — Click this icon to display the Elevator Access Levels Listing page.

Configuring Roles

This section describes how to configure roles. A role is a container for all the permissions a person would need in order to perform a specific role in the organization. Each role can include access groups, delegations, routing groups, and role-assignment privileges.

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

Once you have defined access groups, delegations, routing groups, and role-assignment privileges, you must assign them to the appropriate roles, and then assign the roles to people in the system.

Adding a Role

It is recommended that you define your required access groups, delegations, and routing groups before you configure roles.

To add a new role:

1. Click **Roles** from the icon task bar.

The Roles Listing page is displayed.

2. Click **Add New Role**.

The Role Add page appears.

3. Enter a name for the role.

4. Complete the remainder of the page with the required details.

5. Click .

The Role Edit screen is displayed.

6. Select the **Access Groups** tab to assign access groups to the role.

7. Select the **Delegate** tab to assign delegations to the role.

8. Select the **Routing** tab to assign routing groups to the role.

9. Select the **Asgn Roles** tab to specify role-assignment privileges. Operators with this role can only assign the specified roles in this list to other people in the system.

10. Select the **Access** tab to view access groups, doors, and identities associated with this role.

11. Select the **Audit** tab to view a log of all the changes that have been made to this role.

12. Click .

Editing a Role

To edit an existing role:

1. Click **Roles** from the icon task bar.

2. From the Roles Listing page, click on the role you want to edit.

The Role Edit screen appears.

3. Navigate through the tabbed pages and edit the details as required. The tabbed pages include:

- Role Edit: use this page to edit general settings for the role.
- Access Groups: use this page to assign access groups to the role.
- Delegate: use this page to assign delegations to the role.
- Routing: use this page to assign routing groups to the role.
- Asgn Roles: use this page to specify role-assignment privileges. Operators with this role can only assign the specified roles in this list to other people in the system.
- Access: use this page to view access groups, doors, and identities associated with this role.
- Audit: use this page to view a log of all the changes that have been made to this role.

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


Assigning an Access Group to a Role


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

1. Click **Roles** from the icon task bar.
2. From the Roles Listing page, click on the role you want to edit.

The Role Edit screen appears.

3. Select the **Access Groups** tab.
4. Select the access groups that you want to add to the role.

To add an option, select the option from the Available list then click .

To remove an option, select the option from the Members list and click .

Tip: Use Shift + Click to select multiple options in sequence. Use Ctrl + Click to select multiple individual options.

5. Click .


All the people with this role now have the access permissions defined by the access group.

Roles - Assigning Delegations

To assign delegations to a role:

1. Click **Roles** from the icon task bar.
2. From the Roles Listing page, click on the role you want to edit.

The Role Edit screen appears.

3. Select the **Delegate** tab.
4. From the Available list, select all the delegations that should be part of the role then click .

The delegation is added to the Members list to show that it is now part of the role.

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

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


5. Click .

Roles - Assigning Routing Groups

To assign routing groups to a role:

1. Click **Roles** from the icon task bar.
2. From the Roles Listing page, click on the role you want to edit.

The Role Edit screen appears.

3. Select the **Routing** tab.
4. From the Available list, select all the routing groups that should be part of the role, then click .

The routing group is added to the Members list to show that it is now part of the role.

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


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

5. Click .

Roles - Assign Roles

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

To specify these permissions:

1. Click **Roles** from the icon task bar.
2. From the Roles Listing page, click on the role you want to edit.
The Role Edit screen appears.
3. Select the **Asgn Roles** tab.
4. From the Available list, select all the roles you want to allow members of this role to assign to others, then click .

The role is added to the Members list.

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

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

5. Click .

Deleting a Role

To delete an existing role:




1. From the icon task bar, select **Roles**.
2. From the Roles Listing page, click  beside the role that you want to delete.
3. When the confirmation message is displayed, click **OK**.

Roles - Listing Page

When you select **Roles** from the Roles sub-options task bar, the Roles screen is displayed. This screen has two tabbed pages: Roles and Default Roles (see *Roles - Default Roles Page* on the facing page for more detail).





The first page you see is the Roles Listing page. Select the Roles tab to return to this page. This page lists all the Roles that have been configured in the system.

Feature	Description
Name	The name of this role. Click the name to edit the role.
Parent	Indicates the parent of this role.

Feature	Description
Child Roles	Indicates the number of children of this role.
Installed	Indicates if this role is communicating with the appliance. Yes () or No (). Click the icon to change the status.
Start Date	Indicates the activation date of this role.
Stop Date	Indicates the deactivation date of this role.
Delete	Click  to delete this role from the database. NOTE: Default roles cannot be deleted.
Add New Role	Click this button to add a new role.
Create New Report	Click this button to generate a report of all the roles in the system.

Roles - Default Roles Page

When you select the **Default Roles** tab from the **Roles Listing** page, the **Role: Default Roles** page displays.

Feature	Description
Available	A list of available roles. Select a role and click  to move a role from the Available list to the Members list.
Members	Roles that have been assigned as default roles. Select a role and click  to move a role from the Members list to the Available list.
Search	Enter a search term to find related roles then click Filter to search. Click in the Case-sensitive check-box so that a check mark displays to restrict the search to be case sensitive. Click Clear to clear the search and start again.
	Click this button to save your changes.
	Click this button to discard your changes.



Roles - Add New Page

When you click **Add New Role** from the Roles Listing page, the Role Add page appears. Enter the required details.

Feature	Description
Name	Enter the name of this role.
Parent	From the drop down list, select the parent of this role. Only the roles that have been defined in the system appear in the drop down list. The child role will inherit all the access permissions defined in the parent role. Also, you cannot delete a parent role until you delete all its children. NOTE: This is an advanced feature and is only recommended for experienced operators.

Feature	Description
Start Date	Specify the activation date for this role. Click the field to use the calendar.
Stop Date	Specify the deactivation date for this role. Click the field to use the calendar.
Installed	Check this box to indicate that this role is currently operational and available to the system.
Partitions	<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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.</p>

In addition, there are two buttons at the bottom of the page:

Feature	Description
	Click this button to save your changes.
	Click this button to discard your changes.

Roles - Role Edit Page



When you click the name of a Role from the Roles Listing page, the Role Edit page is displayed. Select the **Role Edit** tab to return to this page.

This page allows you to edit general settings for the role. Make any changes that may be required.

Feature	Description
Name	Enter the name of this role.
Parent	<p>From the drop down list, select the parent of this role.</p> <p>Only the roles that have been defined in the system appear in the drop down list. The child role will inherit all the access permissions defined in the parent role. Also, you cannot delete a parent role until you delete all its children.</p> <p>NOTE: This is an advanced feature and is only recommended for experienced operators.</p>
Start Date	Specify the activation date for this role. Click the field to use the calendar.
Stop Date	Specify the deactivation date for this role. Click the field to use the calendar.
Installed	Check this box to indicate that this role is currently operational and available to the system.
Partitions	<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 appear in this list. You can only see the</p>

Feature	Description
	partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.





In addition, there are three buttons at the bottom of the page:

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 role.

Roles - Access Groups Page

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

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


Feature	Description
Available	A list of access groups that have been configured in the system. To assign an access group to this role, select the access group, then click  .
Members	A list of access groups that have been assigned to this role. To remove an access group from this role, select the access group, then click  .
	Click this button to save your changes.
	Click this button to discard your changes.




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

Roles - Delegate Page

When you select the **Delegate** tab, the Delegate page is displayed. Delegations are sets of permitted commands within the Access Control Manager application. For more information on Delegations, see *Delegations - Introduction*.

This page allows you to assign delegations to the role.

Feature	Description
Available	A list of delegations that have been configured in the system. To add a delegation to this role, select the delegation from the Available list, then click  to move it to the Members list.





Feature	Description
Members	A list of delegations that have been assigned to this role. To remove a delegation from this role, select the delegation from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.
	Click this button to discard your changes.

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

Roles - Routing Page

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


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




Feature	Description
Available	A list of routing groups that have been defined in the system. To assign a routing group to this role, select the routing group, then click  .
Members	A list of routing groups that have been assigned to this role. To remove a routing group from this role, select the routing group, then click  .
	Click this button to save your changes.
	Click this button to discard your changes.

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

Roles - Assign Roles Page

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

Feature	Description
Available	A list of roles that have been configured in the system. To allow members of this role to assign a specific role to other identities, select the role, then click  .
Members	A list of roles that the user is allowed to assign to others.

Feature	Description
	To remove a role from this list, select the role, then click  .
	Click this button to save your changes.
	Click this button to discard your changes.

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

Roles - Access Page

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

Feature	Description
Child Roles	A list of the child roles of this role. Click + or - beside each role to show or hide the identities that are associated with that role.
Identities	A list of the identities that are members of the role.
Parent	The parent of this role. Click + or - beside the parent role to show or hide the access groups and doors that are assigned to that role.
Access Groups	A list of access groups that are assigned to the role.
Doors	A list of doors that are assigned to the role.

Roles - Audit Page

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

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

Managing Policies

You can use policies to override settings on a group of doors, inputs, and outputs. This feature is useful if you want to quickly change security settings on many components or do a full system lock-down.


After you have created a policy, you must assign it to a group of hardware components to make it effective.

Adding a Policy

To add a new policy:

1. From the icon task bar, select **Roles > Policies**.
2. Click **Add New Policy**.

The Policy Add page appears.

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

When the page refreshes, the Policy Edit screen is displayed.

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

Editing a Policy

To edit an existing policy:

1. From the icon task bar, select **Roles > Policies**.

The Policies Listing page appears.

2. Click on the policy you want to edit.

The Policy Edit screen appears.

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

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




Deleting a Policy

To delete an existing policy:

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

Policies - Listing Page



When you select **Roles > Policies** from the icon task bar, the Policies Listing Page is displayed. This page lists all the Policies that have been configured in the system.

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

Policies - Policy Add Page

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



Feature	Description
Name	Enter the name of this policy.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Installed	Check this box to indicate that this policy is currently operational and available to the system.
Door	Check this box to affect doors with this policy.
Input	Check this box to affect inputs with this policy.

Feature	Description
Output	Check this box to affect outputs with this policy.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	Click this button to save your changes.
	Click this button to discard your changes.

Policies - Policy Page

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

Make any changes that may be required.



Feature	Description
Name	Enter the name of this policy.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Installed	Check this box to indicate that this policy is currently operational and available to the system.
Door	Check this box to affect doors with this policy.
Input	Check this box to affect inputs with this policy.
Output	Check this box to affect outputs with this policy.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	Click this button to save your changes.
	Click this button to discard your changes.

Policies - Mercury page

When you select the **Mercury** tab, the Mercury page is displayed. This page allows you to configure a policy for any door connected to a Mercury Security panel.

Feature	Description
Name	Enter the name of this door policy.
Access Type	Select the access type for this door policy.
Door Mode	Select the entry mode for the door when the door controller is online and communicating with the panel.
Offline Door Mode	Select the entry mode used for the door if the door controller is no longer communicating with the panel. 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 Mode option is Facility code only .
Custom mode	Select an additional door mode that will be active during the time specified in the Custom Schedule field.
Custom Schedule	Define when the Custom Mode would be active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
APB mode	Select the Anti-Passback (APB) mode for this door policy. For more information on Anti-Passback modes, see <i>Anti-Passback Modes</i> on page 63.
APB delay	Enter the number of seconds before another APB entry is allowed.
Into Area	Select the area that the user enters by passing through a door. Only the areas that have been previously configured in the system appear in this list.
Out of Area	Select the area that the user exits by passing through a door. Only the areas that have been previously configured in the system appear in this list.
PIN timeout	Enter the number of seconds that is allowed for a user to enter a PIN before it times out.
PIN attempts	Enter the number of times a user can attempt to enter a PIN before an Invalid PIN event is generated.
LED mode	Select the LED mode to specify how the reader LEDs are displayed. For more information on LED modes, see <i>LED Modes</i> on page 1.
Held pre-alarm	Enter the number of seconds a door can be held open before a pre-alarm is issued. Instead of generating an alarm, it sends a warning signal to the Access Control Manager host.
Access time when open	Enter the number of seconds a door remains unlocked after a card has been swiped.
Standard access time	Enter the number of seconds a door remains unlocked after access has been granted. If the door is not opened within this time, it will automatically lock.



Feature	Description
Held open	Enter the number of seconds a door can be held open before a Door Held Open event is generated.
Extended access	<p>Enter the number of seconds a 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, such as individuals with physical disabilities.</p>
Extended held	<p>Enter the number of seconds a 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, such as individuals with physical disabilities.</p>
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.
Mask Forced During	<p>Specify when Forced Door events are masked.</p> <p>Select a schedule from the drop down list.</p> <p>Only schedules that have been defined in the system are listed.</p>
Mask Held During	<p>Specify when Door Held Open events are masked.</p> <p>Select a schedule from the drop down list.</p> <p>Only schedules that have been defined in the system are listed.</p>
Always Mask Forced	From the drop down box, select TRUE to mask all Forced Door events.
Always Mask Held	From the drop down box, select TRUE to mask all Door Held Open events.
Door Processing Attributes	
Enable cipher mode	Select TRUE to allow the user to enter their card number digits at the a keypad entry.
Deny duress	Select TRUE to deny access to a user that indicates duress at a door.
Don't pulse door strike on REX	Select TRUE to disable the pulse of the door strike when request-to-exit is activated .
Require two card control	Select TRUE to specify that two tokens are required to open a door. This enforces two-person entry rule.
Door forced filter	Select TRUE to filter Forced Door events.

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

Policies - Input Page



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

Feature	Description
Name	Enter the name of this input.
Debounce	Select the number of units (approximately 16 ms each) allowed for debouncing.
Entry Delay	Enter the number of seconds allowed for entry before this input issues an alarm.
Exit Delay	Enter the number of seconds allowed for exit before this input issues an alarm.
Hold Time	Set the amount of time that the alarm will stay in alarm after returning to normal. For example, if the input point goes into alarm, then restores, it will hold it in that alarm state for 1 to 15 seconds after it returns to normal before reporting the normal state.
Logging	Enter the type of logging you need for this input. Valid values are: <ul style="list-style-type: none"> • Log all changes: Log all changes affecting this input. • Do not log CoS if masked: Log all changes except change of state events if the input is currently masked.

Feature	Description
	<ul style="list-style-type: none"> • Do not log CoS of masked & no trouble CoS: Log all changes except change of state events if the input is currently masked and there are no trouble CoS events.
Schedule	<p>Define when this input is active.</p> <p>Select a schedule from the drop down list.</p> <p>Only schedules that have been defined in the system are listed.</p>
Mode	<p>Enter the mode used for this input. The available options are:</p> <ul style="list-style-type: none"> • Normal: The door input is a normal door contact. • Non-latching: The door input is a non-latching contact. • Latching: The door input is latching contact.
EOL resistance	<p>Select the EOL resistance value you need for this input.</p> <p>Only those EOL resistance values previously defined for this system appear in this list.</p>
Enabled	<p>Check this box to indicate that this input is connected and ready to communicate with the Access Control Manager host.</p>
Masked	<p>Select TRUE to indicate that this input is normally masked.</p>
	<p>Click this button to save your changes.</p>
	<p>Click this button to discard your changes.</p>

Policies - Output Page

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

Feature	Description
Name	<p>Enter the name of the output.</p>
Enabled	<p>Check this box to indicate that this output is connected and ready to communicate with the Access Control Manager host.</p>
Mode	<p>Select the output mode.</p>
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.NOTE: This field is only available on outputs not associated with doors (e.g. auxiliary relays).</p>
Schedule	<p>Select a schedule from the drop down list.</p> <p>Only schedules that have been defined in the system are listed.</p>
	<p>Click this button to save your changes.</p>
	<p>Click this button to discard your changes.</p>

Policies - Audit Page

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

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

Configuring Groups

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

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


NOTE: Groups should not be confused with Access Groups. For more information on Access Groups, see *Adding Access Groups* on page 1.

Adding a Group

To add a new group:

1. Select **Roles > Groups** from the icon task bar.
2. Click **Add New Group**.

The Group Add page appears.

3. Fill out the **Name** field.
4. Click  .

When the page refreshes, the Group Edit screen is displayed.

5. Select the **Policies** tab to assign policies to the group. For more information on policies, see *Managing Policies* on page 354.
6. Select the **Members** tab to add components to the group.
7. Select the **Audit** page to view a log of all the changes that have been made to this group.

Editing a Group

To edit an existing group:

1. Select **Roles > Groups** from the icon task bar.

The Groups Listing page is displayed.

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

The Group Edit page appears.

3. Navigate through the tabbed pages and make the required changes. The tabbed pages include:
 - Group: use this page to edit the group name and view the current policies and members in the group.
 - Policies: use this page to select the policies in the group.
 - Members: use this page to select the components in the group.
 - Audit: use this page to view a log of all the changes that have been made to this group.

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

Assigning Policies to Groups

To assign policies to a group:

1. Select **Roles > Groups** from the icon task bar.
2. From the Groups Listing page, click on the name of the group you want to edit.

The Group Edit page appears.

3. Select the **Policies** tab.

4. From the Available list, select all the policies that you want to assign to the group, then click .

The policy is added to the Members list to show that it is now assigned.

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

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

5. Click .

Assigning Components to Groups

To assign members to a group:

1. Select **Roles > Groups** from the icon task bar.
2. From the Groups Listing page, click on the name of the group you want to edit.


The Group Edit page appears.

3. Select the **Members** tab.


4. From the **Type** drop down list, select the type of item you want to add to the group.

Once you select a type, the relevant terms will appear in the Available window.

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

5. From the Available list, select all the items that you want to assign to the group, then click .

The item is added to the Members list to show that it is now assigned.

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

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

6. Click .

Creating a Hardware Group for Routing

To use routing groups, you must create a group that contains the event sources of interest. The event sources must be hardware components. For more information on routing groups, see *Routing Events to the Monitor Screen* on page 380

1. Select **Roles > Groups** from the icon task bar.

The Groups listing page is displayed.

2. Click **Add New Group**.

The Group Add page is displayed.

3. Fill out the **Name** field.

4. Select a partition for the hardware group.

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

5. Click .

The Group Edit screen is displayed.

6. Select the **Members** tab.

7. From the **Type** drop-down list, select a type of hardware component.

NOTE: Do not select **Identity** or **Role**, since they are not routable.

8. Select the hardware components that you want to add to the group.

9. Repeat the previous two steps if you want to add different types of hardware components to the group.

10. Click .

Using Policies to Override Hardware Settings

1. Select **Roles > Policies** from the icon task bar.
2. Create a policy. For more information on how to create a policy, see *Adding a Policy* on page 354.
3. Select **Roles > Groups** from the icon task bar.

The Groups Listing page is displayed.


4. Click **Add New Group**.

The Group Add page appears.

5. Fill out the **Name** field, then click .

When the page refreshes, the Group Edit screen is displayed.

6. Select the **Policies** tab.

7. Select the policy that you want to assign to the group, then click .

8. Select the **Members** tab.

9. From the **Type** drop-down list, select a type of hardware component.

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

10. Select the hardware components that you want to override, then click .

The hardware in the group are now overridden by the specified policy.

Performing an Identity Batch Update

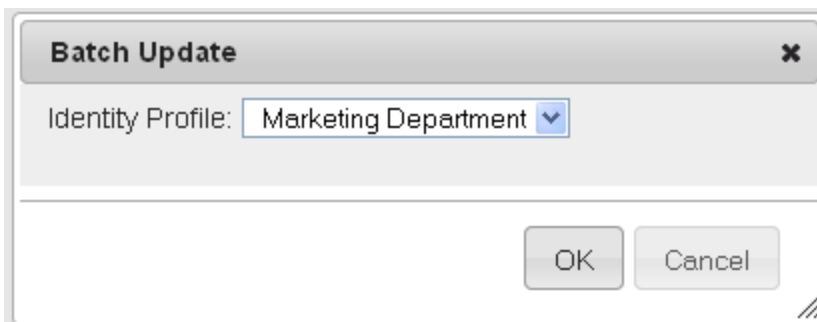
The Batch Update feature allows you to assign an identity profile to all members of a group.

1. Select **Roles > Groups** from the icon task bar.

The Groups Listing page is displayed.

2. From the **BatchUpdate** column, click  beside the group that you want to edit.

The Batch Update dialog box pops up:



3. From the **Identity Profile** drop down list, select the identity profile you want to apply to members of this

group.

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

4. Click  .

All users in this group now have the field values defined by the identity profile.

Scheduling an Identity Batch Update

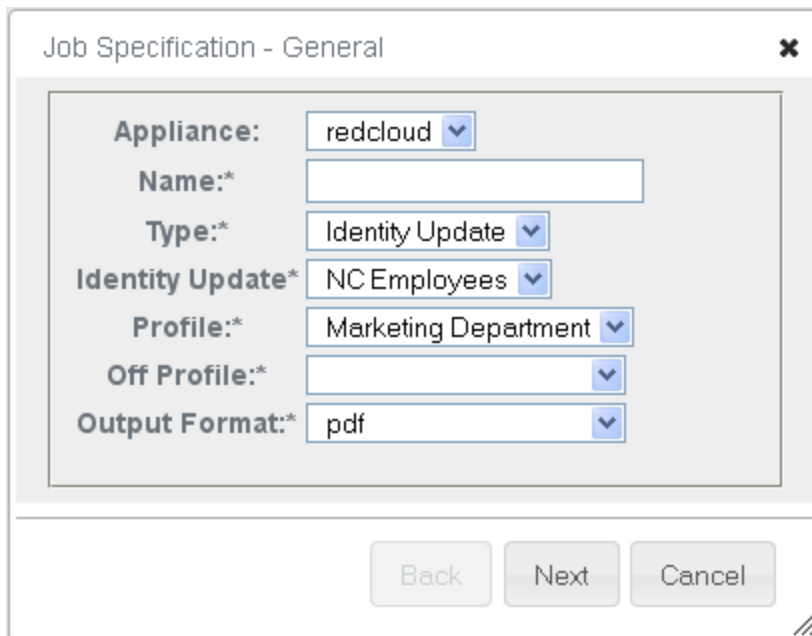
To schedule a batch update:

1. Select **Roles > Groups** from the icon task bar.

The Groups Listing page is displayed.

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

A dialog box pops up:



The dialog box is titled "Job Specification - General" and contains the following fields:

- Appliance:** redcloud (dropdown)
- Name:*** (text input)
- Type:*** Identity Update (dropdown)
- Identity Update:*** NC Employees (dropdown)
- Profile:*** Marketing Department (dropdown)
- Off Profile:*** (dropdown)
- Output Format:*** pdf (dropdown)

At the bottom of the dialog box are three buttons: Back, Next, and Cancel.

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

The Schedule dialog box pops up:

Job Specification - Schedule

Repeat:

Back Next Cancel

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

Depending on the value you select, additional fields appear.

- Fill out the details as required.
- Click **Next**.

The Summary dialog box pops up:

Job Specification - Summary

Batch Job Specification: NC Employees

Type: 2

According to schedule: 00 00 05 12 *

According to schedule:

Back Submit Cancel

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

The job is scheduled.




Deleting a Group

To delete an existing group:

- From the icon task bar, select **Roles > Groups**.
- From the Groups Listing page, click  beside the group that you want to delete.
- When the confirmation message is displayed, click **OK**.



Groups - Listing Page

When you select **Roles > Groups** from the icon task bar, the Groups Listing page is displayed. This page lists all the Groups that have been configured in the system.

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

Groups - Group Add Page

When you click **Add New Group** from the Groups Listing page, the Group Add page appears. Enter the required details.

Name	Enter the name of this group.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Policies	All the policies that are currently associated with this group.
Members	All the identities that are currently associated with this group.
	Click this button to save your changes.
	Click this button to discard your changes.





Groups - Group Edit page

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

Groups - Policies Page

When you select the **Policies** tab, the Policies page is displayed. Policies are access regulations that you can establish for doors, inputs, and outputs. For more information on policies, see *Policies - Introduction*.

This page allows you to assign policies to this group.





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

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

Groups - Members page

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

This page allows you to assign components to the group.

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

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

Groups - Audit Page

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

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

Managing Door Access

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

You must configure doors before you can create access groups. If you want to control access to the floors of a building, you should configure elevator access levels beforehand as well. For more information on elevator access levels, see *Managing Elevator Access* on page 384.

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


Adding an Access Group

If you want to control access to the floors of your building, you must create elevator access levels. For more information on elevator access levels, see *Managing Elevator Access* on page 384. It is recommended that you configure doors and elevator access levels before you create access groups.

To add a new access group:


1. Select **Roles > Access Groups** from the icon task bar.
2. On the Access Groups listing page, click **Add New Access Group**.

The Access Group Add page is displayed.

3. Enter a name for the new access group.
4. Select an appliance to manage the access group.
5. Complete the remainder of the page with the required details.
6. Click  .


The Access Group Edit page is displayed.

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

To add an option, select the option from the Available list then click .

To remove an option, select the option from the Members list and click .

Tip: Use Shift + Click to select multiple options in sequence. Use Ctrl + Click to select multiple individual options.

8. Click  .
9. After you have created an access group, you must assign it to a role to make it effective. For more information, see *Assigning an Access Group to a Role* on page 346.

Editing an Access Group


1. From the icon task bar select **Roles > Access Groups**.
The Access Groups Listing page appears.
2. Click the name of the access group that you want to edit.
The Access Group Edit page appears.
3. Navigate through the tabbed pages and make the required changes. The tabbed pages include:
 - Edit: use this page to edit the access group
 - Access: use this page to view the doors, roles, and identities that are in this access group
 - Audit: use this page to view a log of all the changes that have been made to this access group.

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

Deleting an Access Group

NOTE: You can only delete access groups that are not linked to any roles.

Before you can delete an access group, you must remove the access group from the associated role. For more information, see *Assigning an Access Group to a Role* on page 346.

1. From the icon task bar, select **Roles > Access Groups**.
2. From the Access Groups listing page, click  beside the access group that you want to delete.
3. When the confirmation message is displayed, click **OK**.

Access Groups - Example

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

A working example is:

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

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

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


Assigning an Access Group to a Role


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

1. Click **Roles** from the icon task bar.
2. From the Roles Listing page, click on the role you want to edit.

The Role Edit screen appears.

3. Select the **Access Groups** tab.
4. Select the access groups that you want to add to the role.

To add an option, select the option from the Available list then click .

To remove an option, select the option from the Members list and click .

Tip: Use Shift + Click to select multiple options in sequence. Use Ctrl + Click to select multiple individual options.



5. Click .


All the people with this role now have the access permissions defined by the access group.

Access Groups - Listing Page

When you select **Roles > Access Groups** from the icon task bar, the Access Groups Listing page is displayed.





This page lists all the Access Groups that have been configured in the system.

Feature	Description
Name	The name of the access group. Click the name to edit the access group.
Appliance	Identifies the name of the appliance that maintains this access group.
Installed	Indicates if this access group is communicating with the appliance. Click  for yes or  for no.
# Doors	Specifies the number of doors associated with this access group.
Roles	A list of roles that this access group is a member of.

Feature	Description
Delete	Click  to delete the access group. NOTE: You cannot delete access groups that have been assigned to specific roles.
Add New Access Group	Click this button to add a new access group.
Create New Report	Click this button to generate a report of all the access groups in the system.

Access Groups - Access Group Add page





When you click **Add New Access Group** from the Access Groups Listing page, the Access Group Add page appears. Enter the required details.

Feature	Description
Name	Enter the name of this access group.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Appliance	From the drop down list, select the appliance that manages this access group.
Schedule	Specify when the access group is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Elevator Access level	Select the elevator access level that applies to this access group. Only the elevator access levels that have been defined in the system appear in this list.
Installed	Check this box to indicate that this access group is currently operational and available to the system.
Available	A list of available doors that are associated with the specified appliance. To add a door to this access group, select the door from the Available list, then click  to move it to the Members list.
Members	A list of doors that are members of this access group. To remove a door from this access group, select a door from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.
	Click this button to discard your changes.

Access Groups - Edit Page

When you click the name of an Access Group from the Access Groups Listing page, the Access Group Edit page is displayed. Click on the **Edit** tab to return to this page.

This page allows you to edit general settings for the access group. Make any changes that may be required.

Feature	Description
Name	Enter the name of this access group.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Appliance	The appliance that manages this access group. This is a read-only field.
Schedule	Specify when the access group is active. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Elevator Access level	Select the elevator access level that applies to this access group. Only the elevator access levels that have been defined in the system appear in this list.
Installed	Check this box to indicate that this access group is currently operational and available to the system.
Available	A list of available doors that are associated with the specified appliance. To add a door to this access group, select the door from the Available list, then click  to move it to the Members list.
Members	A list of doors that are members of this access group. To remove a door from this access group, select a door from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.
	Click this button to discard your changes.

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

Access Groups - Access Page

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

Feature	Description
Access Group	The name of this access group.

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

Access Groups - Audit Page

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

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


Managing Access in the Application

A delegation is a list of permissions within the Access Control Manager application that allows an operator to configure settings and monitor events.


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

Adding a Delegation

To add a new delegation:


1. Select **Roles > Delegations** from the icon task bar.
The Delegations listing page is displayed.
2. Click **Add New Delegation**.
The Delegation Add page appears.
3. Enter a name for the new delegation, then click .
The Delegation Edit page appears.

4. Select the permissions you want to include in the delegation.

To add an option, select the option from the Available list then click .


To remove an option, select the option from the Members list and click .

Tip: Use Shift + Click to select multiple options in sequence. Use Ctrl + Click to select multiple individual options.

5. Click .
6. After you have created a delegation, you must assign it to a role to make it effective. For more information, see *Adding a Delegation to a Role* below

Editing a Delegation


To edit an existing delegation:


1. Select **Roles > Delegations** from the icon task bar.
The Delegations Listing page appears.
2. Click the name of the delegation you want to edit.
The Delegation Edit page appears.
3. Make the required changes.
4. Click .

Adding a Delegation to a Role

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

1. Click **Roles** from the icon task bar.
2. From the Roles Listing page, click on the role you want to edit.
The Role Edit screen appears.
3. Select the **Delegate** tab.
4. Select the delegations that you want to add to the role.

To add an option, select the option from the Available list then click .

To remove an option, select the option from the Members list and click .


Tip: Use Shift + Click to select multiple options in sequence. Use Ctrl + Click to select multiple individual options.

5. Click .

All the people with this role now have the access permissions defined by the delegation.


Deleting a Delegation

To delete an existing delegation:

1. From the icon task bar, select **Roles > Delegations**.
2. From the Delegations Listing page, click  beside the delegation that you want to delete.
3. When the confirmation message is displayed, click **OK**.

Delegations Listing Page



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



Feature	Description
Name	The name of this delegation. Click the name to edit the delegation.
Members	The number of tasks that are permitted in this delegation.
Delete	Click  to delete this delegation.
Add New Delegation	Click this button to add a new delegation.
Create New Report	Click this button to generate a report of all the delegations in the system.

Delegations - Edit Page

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

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

Feature	Description
Name	Enter the name of the delegation.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Available	A list of available tasks in the Access Control Manager application. To add a task to the delegation, select the term from the Available list, then click  to move it to the Members list.
Members	A list of tasks that are members of this delegation. To remove a task from this delegation, select the term from the Members list, then click  to move it to the Available list.

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

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

Partitioning the System

The Access Control Manager system allows you to assign operators to specific partitions. When a feature is assigned to a partition, the feature can only be edited by an operator that has access to that partition. If the feature is not assigned to a partition, it can be edited by any operator in the system.

If you are using partitions, it is recommended that you create partitions before you configure the rest of the system.


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

NOTE: The **Partition** field only appears as a configuration option after you have defined one or more partitions in the system. Also, an operator can only see the partitions they have access to.

Adding a Partition

This is a basic procedure on how to add a partition. For a more advanced procedure on how to partition the Access Control Manager system, see *Configuring Partitions* on the next page.

To add a new partition:

1. Select **Roles > Partitions** from the icon task bar.
The Partitions listing page is displayed.
2. Click **Add New Partition**.
The Partition Add page appears.
3. Enter a name for the new partition, then click .
The Partition Edit page appears.

4. Select the operators that you want to include in the partition.

To add an option, select the option from the Available list then click .

To remove an option, select the option from the Members list and click .

Tip: Use Shift + Click to select multiple options in sequence. Use Ctrl + Click to select multiple individual options.

5. Click .

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

Editing a Partition

To edit an existing partition:

1. Select **Roles > Partitions** from the icon task bar.

The Partitions Listing page appears.

2. Click the name of the partition you want to edit.

The Partition Edit page appears.

3. Make the required changes.

4. Click .

Configuring Partitions

It is recommended that you use the default Admin account to configure partitions.

1. Select **Roles > Partitions** from the icon task bar.
2. Create the partitions that you require.
3. Select **Identities** from the icon task bar.
4. Create one or more operators for each partition.
 - If you do not want the operators to be viewed by other operators in the system, go to the Account Information section at the bottom of the Identity Edit page and assign them to the appropriate partition.
 - For now, assign the Super Admin role to each operator. You can change this later if you are partitioning the system for routing groups.
5. Select **Roles > Partitions** from the icon task bar.
6. Add the appropriate operators to each partition.

Each operator will only be able to view and edit the system features that are assigned to their partition, or features that are not assigned to any partition.


7. Partition the system as required by editing each feature individually. For example, to add a door to a partition:
 - a. Select **Physical Access > Doors**.
 - b. Select a door.
 - c. From the Door Edit page, select a partition.

Repeat this procedure to other features as required.

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


Deleting a Partition

To delete an existing partition:

1. From the icon task bar, select **Roles > Partitions**.
2. From the Partitions Listing page, click  beside the partition that you want to delete.
3. When the confirmation message is displayed, click **OK**.

Partitions - Listing Page





When you select **Roles > Partitions** from the icon task bar, the Partitions Listing page is displayed. This page lists all partitions that have been configured in the system.

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

Partitions - Partition Edit Page

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

This page allows you to add users to the partition.

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

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

Routing Events to the Monitor Screen

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

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

You must set up partitions and groups before you can use routing groups. For more information on partitions, see *Partitioning the System* on page 377. For more information on groups, see *Configuring Groups* on page 361.

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

Adding a Routing Group

To add a new routing group:

1. Configure partitions for the routing group. For more information on configuring partitions, see *Configuring Partitions* on page 378.
2. Create a hardware group that contains the event sources of interest. For more information on creating a hardware group for routing, see *Creating a Hardware Group for Routing* on page 363.
3. If you want to route events for specific time intervals, set up one or more schedules. For more information on adding a schedule, see *Adding Schedules* on page 225.
4. Select **Roles > Routing Groups** from the icon task bar.


The Routing Groups listing page is displayed.


5. Click **Add New Routing Group**.

The Routing Group Add page is displayed.

6. Enter a name for the routing group.
7. Complete the remainder of the page with the required details.


Important: Select the appropriate partition for this routing group.


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

To add an option, select the option from the Available list then click .

To remove an option, select the option from the Members list and click .

Tip: Use Shift + Click to select multiple options in sequence. Use Ctrl + Click to select multiple individual options.

When you're finished, click .

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

Editing a Routing Group

To edit an existing routing group:

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

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


Assigning a Routing Group to a Role

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

1. Click **Roles** from the icon task bar.
2. From the Roles Listing page, click on the role you want to edit.

The Role Edit screen appears.

3. Select the **Routing** tab.
4. Select the routing groups that you want to add to the role.

To add an option, select the option from the Available list then click .

To remove an option, select the option from the Members list and click .


Tip: Use Shift + Click to select multiple options in sequence. Use Ctrl + Click to select multiple individual options.

5. Click .

All the operators with this role can now monitor the events defined by the routing group.


Deleting a Routing Group

To delete an existing routing group:

1. From the icon task bar, select **Roles > Routing Groups**.
2. From the Routing groups Listing page, click  beside the routing group that you want to delete.
3. When the confirmation message is displayed, click **OK**.

Routing Groups - Listing Page



When you select **Roles > Routing Groups** from the icon task bar, the Routing Groups Listing page is displayed. This page lists all routing groups that have been configured in the system.

Feature	Description
Name	The name of the routing group. Click the name to edit the routing group details.
Schedule	Indicates when this routing group is active.
Event Type	The number of event types that are in this routing group.
Group	The number of groups that are in this routing group.
Delete	Click  to delete this routing group.
Add New Routing Group	Click this button to create a new routing group.
Create New Report	Click this button to generate a report of all the routing groups in the system.

Routing Groups - Add Page



When you click **Add New Routing Group** from the Routing Groups Listing page, the Routing Group Add page appears. Enter the required details.

Feature	Description
Name	Enter the name of this routing group.
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Schedule Qualifier	From the drop down list, select the option that qualifies the schedule. <ul style="list-style-type: none">• Appliance : Relative to the local time on the appliance when the transaction was created within the Access Control Manager system.• Event: Relative to the local time when the originating event occurred.
Installed	Check this box to indicate that this routing group is currently operational and available to the system.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	Click this button to save your changes.
	Click this button to discard your changes.


Routing Groups - Schedule Page




When you click the name of a Routing Group from the Routing Groups Listing page, the Routing Group Schedule page is displayed. Click on the **Schedule** tab to return to this page.

Feature	Description
Name	Enter the name of this routing group.
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Schedule Qualifier	From the drop down list, select the option that qualifies the schedule. <ul style="list-style-type: none"> • Appliance : Relative to the local time on the appliance when the transaction was created within the Access Control Manager system. • Event: Relative to the local time when the originating event occurred.
Installed	Check this box to indicate that this routing group is currently operational and available to the system.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	Click this button to save your changes.
	Click this button to discard your changes.

Routing Groups - Event Types Page





When you select the **Event Types** tab from the Routing Groups Edit screen, the Event Types page is displayed. This page allows you to specify which event types should be routed in this routing group.

Feature	Description
Routing Group	The name of this routing group. Click this name link to return to the Schedule page.
Available	A list of event types configured in the system. To add an event type to the routing group, select the term from the Available list, then click  to move it to the Members list.

Feature	Description
	A list of event types that are in this routing group.
Members	To remove an event type from the routing group, select the term from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.
	Click this button to discard your changes.

Routing Groups - Groups Page

When you select the **Groups** tab from the Routing Groups Edit screen, the Groups page is displayed. This page allows you to add groups to this routing group.

Feature	Description
Routing Group	The name of this routing group. Click this name link to return to the Schedule page.
Available	A list of groups configured in the system. To add a group to the routing group, select the term from the Available list, then click  to move it to the Members list.
Members	A list of groups that are in this routing group. To remove a group from the routing group, select the term from the Members list, then click  to move it to the Available list.
	Click this button to save your changes.
	Click this button to discard your changes.

Managing Elevator Access

An Elevator Access Level defines a cardholder's elevator access to the floors in a building.

For example, you can create an elevator access level that contains Floor 1 and Floor 3. When you add this elevator access level to an access group, all users in that access group will have access to Floor 1 and Floor 3.


If you want to control elevator access during specified time intervals, you must set up schedules prior to creating the elevator access level. For more information on schedules, see *Adding Schedules* on page 225. After you have created an elevator access level, you must assign it to an access group to make it effective.

NOTE: This feature currently applies to Mercury Security elevator transactions in floor tracking mode.

Adding an Elevator Access Level


If you want to control elevator access during specified time intervals, you must set up schedules prior to creating the elevator access level. For more information on schedules, see *Adding Schedules* on page 225.

To add a new elevator access level:

1. Select **Roles > Elevator Access Levels** from the icon task bar.
The Elevator Access Levels listing page is displayed.
2. Click **Add New Elevator Access Level**.
3. Enter a name for the elevator access level in the **Description** field.
4. Select an appliance to manage the elevator access level.
5. Complete the remainder of the page with the required details.
5. Click  .
6. After you have created an elevator access level, you must assign it to an access group to make it effective. For more information, see *Assigning an Elevator Access Level to an Access Group* below


Editing an Elevator Access Level

To edit an elevator access level:

1. Select **Roles > Elevator Access Levels** from the icon task bar.
The Elevator Access Levels Listing page appears.
2. Click on the elevator access level you want to edit.
The Elevator Access Level Edit screen appears.
3. Make the required changes.
4. Click  .

Assigning an Elevator Access Level to an Access Group


You must assign an elevator access level to an access group to make it effective.

1. Select **Roles > Access Groups** from the icon task bar.
The Access Groups listing page is displayed.
2. Click the name of the access group you want to edit.
3. From the **Elevator Access Level** drop down list, select the elevator access level.
4. Click  .

All users in that access group now have access to the floors in the elevator access level.


Deleting an Elevator Access Level

To delete an existing elevator access level:

1. From the icon task bar, select **Roles > Elevator Access Levels**.
2. From the Elevator Access Level listing page, click  beside the elevator access level that you want to delete.
3. When the confirmation message is displayed, click **OK**.


Elevator Access Levels - Listing Page


When you select **Roles > Elevator Access Levels** from the icon task bar, the Elevator Access Levels listing page is displayed. This page lists all elevator access levels that have been configured in the system.

Feature	Description
Description	The name of this elevator access level. Click on the name to edit the elevator access level details.
Delete	Click  to delete this elevator access level.
Add New Elevator Access Level	Click this button to add a new elevator access level.

Elevator Access Levels - Add Page



When you click **Add New Elevator Access Level** from the Elevator Access Level Listing page, the Elevator Access Level Add page appears. Enter the required details.

Feature	Description
Description	Enter the name of this elevator access level.
Appliance	From the drop down list, select the appliance that manages this elevator access level.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Output	Indicates the default output number.
Description	The name of each floor. The floors are named by default, but you can rename them.
Schedule	Indicate when a card/code has free access to the specified floor, meaning a valid card/code is not required to access this floor. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.

Elevator Access Levels - Edit Page

When you click the name of an elevator access level from the Elevator Access Level Listing page, the Elevator Access Level Edit page is displayed. Make any changes that may be required.

Feature	Description
Description	Enter the name of this elevator access level.
Appliance	From the drop down list, select the appliance that manages this elevator access level.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
Output	Indicates the default output number.
Description	The name of each floor. The floors are named by default, but you can rename them.
Schedule	Indicate when a card/code has free access to the specified floor, meaning a valid card/code is not required to access this floor. Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
	Click this button to save your changes.
	Click this button to discard your changes.

Monitor - Introduction

The Monitor screen allows you to monitor and verify events throughout the Access Control Manager system.

Users with the appropriate permissions can review transaction events, monitor alarms, verify user access and confirm hardware status.

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** from the icon task bar, 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

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

Follow the steps below to view live video.

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

Only events or alarms with an  icon will have video.

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


The **Monitor Screen - Live Video window** displays. View the live video in this window. For more information, see *Monitor Screen - Live Video Window* on page 413.

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

Follow the steps below to view live video.

1. Click **Monitor**. The Monitor Events page displays (for more information, see *Monitoring Events* on page 388).
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. For more information, see *Monitor Screen - Recorded Video Window* on page 414.

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

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 (for more information, see *Monitor Screen - Notes Window* on page 415).

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

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 388).
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 (for more information, see *Monitor Screen - Notes Window* on page 415). 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

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 388).
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 (for more information, see *Monitor Screen - Instructions Window* on page 416). 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 388).
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 (for more information, see *Monitor Screen - Identity Window* on page 416).

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 388).
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. For more information, see *Monitor Screen - History Window* on page 416.

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 its 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.

For more information on column management, see Monitor Screen - Column Management.

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 388).

If your browser loses connectivity with Access Control Manager 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.

1. From the Monitor screen, click the **Search** sub-option.

The Events Search (Transactions) page appears.

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

The Search area is displayed:

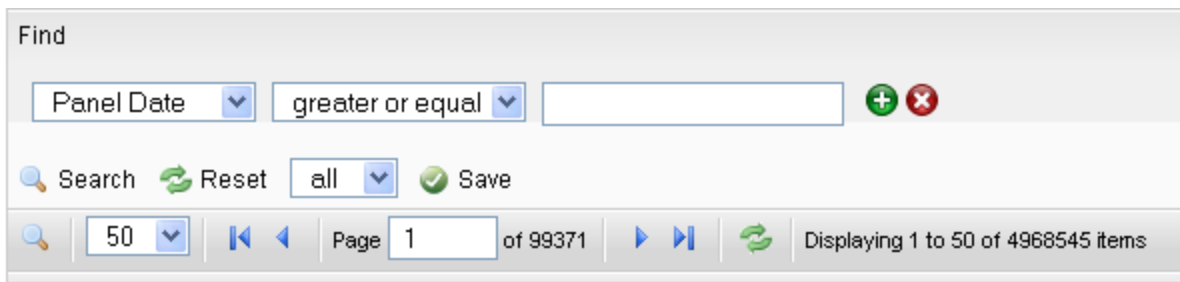


Figure 3: Search options

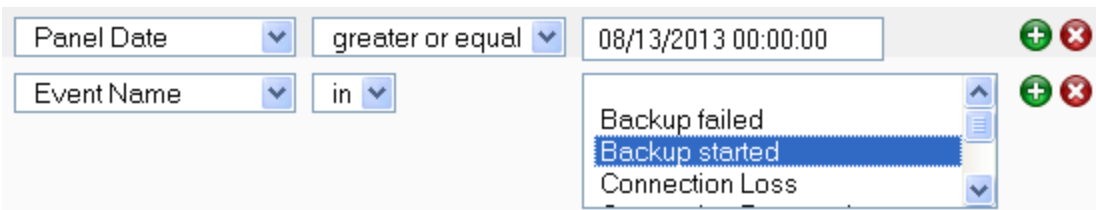
3. From the first drop down list, select the data type that you want to search. The options are:
 - Panel Date
 - Last Name
 - Card Number
 - Message
 - Event Name
 - Event Type
 - Source
4. From the second drop down list, select the appropriate argument for your search. The available arguments change depending on the selected data type.
5. In the text field, enter any text that you want to find in the selected data type. For example, you may enter "forced door" when performing an Event Type search.


You can enter any number or letter combination and you can use wildcards. The wildcard * character can be used to help you find events that you do not have all the details for.

For example:

- s* — will find any word that starts with an "s".
- *s — will find any word that ends with an "s".
- *s* — will find any word that has an "s" in the middle.

6. If you want to narrow your search further, 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 search result and use the action buttons at the top of the page to see the details of the event.

View Camera (Search)

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.

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. For more information see *Monitor Screen - Live Video Window* on page 413.

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)

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.

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

The **Monitor Screen - Recorded Video window** displays.

4. View the video in this window. For more information see *Monitor Screen - Recorded Video Window* on page 414.

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)

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 (for more information see *Monitor Screen - Notes Window* on page 415).

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)

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 (for more information see *Monitor Screen - Notes Window* on page 415). 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)

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 (for more information see *Monitor Screen - Instructions Window* on page 416). View the instructions in the table that displays.

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 (for more information see *Monitor Screen - Identity Window* on page 416).

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. For more information see *Monitor Screen - History Window* on page 416.

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 its new location.

For more information on column management see *Monitor Screen - Column Management*.

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**).

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.
- **In Process** — Click this button to monitor the selected alarm status in real-time.
- **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.

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


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)

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 396.
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. For more information see *Monitor Screen - Live Video Window* on page 413.

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)

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 396).
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. For more information see *Monitor Screen - Recorded Video Window* on page 414.

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)

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 396.
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. For more information see *Monitor Screen - Notes Window* on page 415.

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)

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 396.

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. For more information see *Monitor Screen - Notes Window* on page 415. 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)

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 396.
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. For more information see *Monitor Screen - Instructions Window* on page 416. 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 396.
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. For more information see *Monitor Screen - Identity Window* on page 416.

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** to access the Monitor Alarms page displays. For more information see *Monitor Alarms* on page 396.
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. For more information see *Monitor Screen - History Window* on page 416.

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 396.

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.

For more information on column management, see *Monitor Screen - Column Management*.

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.'.

Monitor Screen - Verification

When you click the **Verification** sub-option from the Monitor screen, 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.

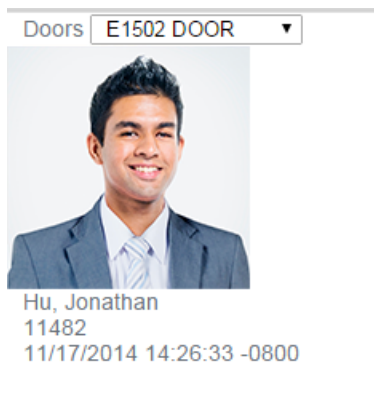
- At the top of the page are four door panes that allow you to select and monitor four doors at a time. After you assign a door to each pane, you can monitor live event transactions as they occur at each door.
- Underneath is a list of all the live door transactions displayed like the Events page. For more information, see *Monitor Screen - Events* on page 412.

Verifying Cardholders at Doors

On the Monitor screen, select the **Verification** sub-option to open the Verification page in order to verify and confirm the identity of any cardholder who passes through the selected doors:

1. From one of the **Doors** drop down lists, select a door.
2. To activate 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 cardholder attempts to enter this door using a card or code, the person's identity information is displayed:



The window includes the card holder's name, internal token number and the time and date of entry. A photo is displayed if there is one stored in the Identity record.

At the bottom of the screen are the detailed entry and exit events generated by the cardholders.

Verification Events List

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

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

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

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 its 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.

For more information on column management see *Monitor Screen - Column Management*.

6. Click **Save Settings** if you want to save the new settings.

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

Monitor Page - Hardware Status

When you click the **HW Status** sub-option from the Monitor screen, the Hardware Status page is displayed.

This page displays the current status of all connected panels, doors, inputs, outputs and associated security devices. You can also use this screen to control doors in the system.

The current status of the device is indicated by the background color. For more information, see *Status Colors* on page 409.

- *System Status* on the next page
- *Door Actions* on page 404
- *Door Status* on page 404
- *Panel Status* on page 405
- *Subpanel Details* on page 406
- *Input / Output Details* on page 407
- *LifeSafety Panels* on page 407

System Status










redcloud 10/18/2012 18:23:31 **Up:** 1 days 7 hours 10 minutes 45 seconds **Port** **Link** **Rx** **Tx**
RAM (%free): 45 **Programs:** 27 **Database:** 83 **Load:** 0.0 1 **Normal** 678033 677511
Doors Off-Line: 1 Active: 0 Masked: 0 **Panels** Off-Line: 0 Active: 0
Inputs Off-Line: 0 Active: 0 Masked: 0 **SubPanels** Off-Line: 0 Active: 0

The System Status details are described starting from the top-left corner, then continues row by row.




Feature	Description
Appliance Name	At the top-left corner is the unlabeled name of the current appliance.
Timestamp	Beside the Appliance Name is the date and time when the appliance initially came online.
Up	Displays the time this Access Control Manager appliance has been running.
RAM	Displays the percentage of installed RAM in the Access Control Manager appliance that is currently unused.
Programs	Displays the number of programs currently running on the appliance.
Database	Displays the free space currently available on the data (writable) portion of the disk.
Load	Indicates the current compute load the Access Control Manager appliance is experiencing.
Disk	Indicates the total number of MB the Access Control Manager appliance hard driver contains.
Port	Indicates the port number the appliance is currently using to connect to the network.
Link	Indicates the current state of the network link to the appliance. This is either Normal or None .
Rx	Indicates the number of received data packets by the port.
Tx	Indicates the number of transmitted data packets by the port.
Doors	The status of connected doors in these three categories: <ul style="list-style-type: none"> • Offline • Active • Masked
Panels	The status of connected panels in these categories: <ul style="list-style-type: none"> • Offline • Active
Inputs	The status of connected inputs in these three categories: <ul style="list-style-type: none"> • Offline • Active • Masked
Subpanels	The status of connected subpanels in these categories: <ul style="list-style-type: none"> • Offline • Active







Door Actions

To use the Door Action buttons, you must select a door before you click the action button.

Feature	Description
	Click this button to disable the specified door. This keeps it from operating and allows no access.
	Click this button to unlock the specified door. This door will remain unlocked until the Lock command is issued, or until another change of state is directed, either via operator override or scheduled action.
	Click this button to lock the specified door. This door will remain locked until the Unlock command is issued, or until another change of state is directed, either via operator override or scheduled action.
	Click this button to grant the current user access to the specified door. The door will be momentarily unlock to permit single time entry through the door.
	Click this button to reset the door's configuration values to their default value.
	Click this button to mask the Door Held Open Alarm for this door.
	Click this button to unmask the Door Held Open Alarm for this door.
	Click this button to mask the Forced Held Open Alarm for this door.
	Click this button to unmask the Door Forced Open Alarm for this door.

























































Door Status

Feature	Description
All / None	Check the box beside the door you want to control through the Door Action buttons. If you click on All in the title line, it automatically selects all listed doors; the word changes to None . If all doors are currently listed, click None to deselect all listed doors.
Name	The name assigned to this door.
Installed	The status of the door's installation:  (installed) or  (uninstalled). Click the icon to change the door status.
Manuf	The vendor or manufacturer of the panel that the door is connected to.
Panel	The name of the panel to which this door is connected.
	Status of communications between the door and specified panel. The color below indicates the current status.

Feature	Description
Communications	
 Lock	Indicates whether this door is locked or not. See the color legend at the bottom of the page for the correct status reference.
 Power	Indicates the status of the power on the door. See the color legend at the bottom of the page for the correct status reference.
 Tamper	Indicates the status of the tamper switch on the door. See the color legend at the bottom of the page for the correct status reference.
 Battery	Indicates the status of the battery backup on the door. See the color legend at the bottom of the page for the correct status reference.
 Forced	Indicates whether this door is currently in a forced state. See the color legend at the bottom of the page for the correct status reference.
 Held	Indicates whether this door is currently in a held open state. See the color legend at the bottom of the page for the correct status reference.

Panel Status

As you click the name of each panel, a list of the connected devices is displayed until you see the last input or output down the line.

Feature	Description																
Name	The name of the panel.																
	Click the name of the panel to see the status of the connected subpanels.																
	<table border="1"> <thead> <tr> <th>Name</th> <th>Installed</th> <th>   </th> <th>Sub-Panel Status</th> </tr> </thead> <tbody> <tr> <td>1501 w down test1</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Subpanel</th> <th>   </th> <th>Installed</th> </tr> </thead> <tbody> <tr> <td>0 - 1501 w down test1 - 1501 Internal SIO-0</td> <td>   </td> <td></td> </tr> <tr> <td>1 - 1501 w down test1 - Two door module-1</td> <td>   </td> <td></td> </tr> </tbody> </table>	Name	Installed	   	Sub-Panel Status	1501 w down test1				Subpanel	   	Installed	0 - 1501 w down test1 - 1501 Internal SIO-0	   		1 - 1501 w down test1 - Two door module-1	   
Name	Installed	   	Sub-Panel Status														
1501 w down test1																	
Subpanel	   	Installed															
0 - 1501 w down test1 - 1501 Internal SIO-0	   																
1 - 1501 w down test1 - Two door module-1	   																
	Click the name of the following subpanel to see the status of the connected inputs and outputs.																

Feature	Description




Installed	<p>The status of the panel's installation: (installed) or (uninstalled).</p> <p>Click the icon to change the panel status.</p>
	Status of communications between the panel and subpanels. See the color legend at the bottom of the page for the correct status reference.
	Indicates the status of the power on this panel. See the color legend at the bottom of the page for the correct status reference.
	Indicates the status of the tamper switch on this panel. See the color legend at the bottom of the page for the correct status reference.
	Indicates the status of the battery backup on the door. See the color legend at the bottom of the page for the correct status reference.

Subpanel Status	Indicates the number of the subpanels attached to this panel. Each relevant subpanel is displayed together with its current status. The color indicates the current status.
------------------------	---

Subpanel Details

Click the name of a panel to display the connected subpanel details.

Feature	Description
Subpanel	The name of this subpanel. To drill down into the inputs and outputs associated with this subpanel, click this link.
	Status of communications between the panel and this subpanel. See the color legend at the bottom of the page for the correct status reference.
	Indicates the status of the power on this panel. See the color legend at the bottom of the page for the correct status reference.

Feature	Description
	Indicates the status of the tamper switch on this panel. See the color legend at the bottom of the page for the correct status reference.
Installed	The status of the subpanel's installation:  (installed) or  (uninstalled). This field is selectable and can be toggled.



Input / Output Details

Click the name of a subpanel to display the connected inputs and outputs.

Feature	Description
Input	This column lists all the inputs controlled by this subpanel, with the name and address of each input.
Cmd	The commands available to control the input: <ul style="list-style-type: none"> • Mask — Click this button to mask the specified input. • UnMask — Click this button to unmask a previously masked input.
Output	This column lists all the outputs (including relays and locks) controlled by this subpanel, with name and address of each output.
Cmd	The commands available to control the output: <ul style="list-style-type: none"> • On — Click this button to power the output. If this output is a door, it energizes the circuit. • Off — Click this button to turn off the power to this output. If this output is a door, it de—energizes the circuit. • Pulse — Click this button to alternately energize and de—energize this output. The pulse interval is determined by the output's settings.

LifeSafety Panels

The following options are only displayed if you have a LifeSafety Power panel installed in your system.










Feature	Description
Name	The name of the LifeSafety Power panel. Click this name to display the panel details.
Installed	The status of the panel's installation:  (installed) or  (uninstalled). This field is selectable and can be toggled.
Commands	The commands available to control the LifeSafety Power panels: <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

Feature	Description
	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 HW Status page of the Monitor screen.

1. From the icon task bar, select **Monitor > HW Status**.
2. To control a door:
 - a. In the Doors section of this page, check the box beside each door you want to control.
 - b. Click the appropriate button Door Action button.





-  — Click this button to disable the specified door. This keeps it from operating and allows no access.
-  — Click this button to unlock the specified door. This door will remain unlocked until the Lock command is issued, or until another change of state is directed, either via operator override or scheduled action.
-  — Click this button to lock the specified door. This door will remain locked until the Unlock command is issued, or until another change of state is directed, either via operator override or scheduled action.
-  — Click this button to grant the current user access to the specified door. The door will be momentarily unlock to permit single time entry through the door.
-  — Click this button to reset the door's configuration values to their default value.
-  — Click this button to mask the Door Held Open alarm for this door.
-  — Click this button to unmask the Door Held Open alarm for this door.
-  — Click this button to mask the Forced Held Open alarm for this door.
-  — Click this button to unmask the Door Forced Open alarm for this door.

The action is performed on the specified device.

3. To control an input:
 - a. In the Panel Status area, click the name of the connected panel then click the name of the connected subpanel.
 - b. 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.
4. To control an output:
 - a. In the Panel Status area, click the name of the connected panel then click the name of the connected subpanel.
 - b. When the required output is displayed, click one of the following buttons:
 - **On** — Click this button to power the output. If this output is a door, it energizes the circuit.
 - **Off** — Click this button to turn off the power to this output. If this output is a door, it de-energizes the circuit.
 - **Pulse** — Click this button to alternately energize and de-energize this output. The pulse interval is determined by the output's settings.
5. 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).

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.
 Masked	The specified Access Control Manager input is currently masked.

Monitor Screen - Map Templates Page

When you click the **Maps** sub-option from the Monitor screen, a list of all the configured maps is displayed. Also included in the list are configured Mustering dashboards.

Click the name of the map template to display the configured map or dashboard.

Using a Map

Once a map has been configured, it can be accessed from the Monitor screen and used 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, activate inputs and outputs, control doors and keep track of identities as they arrive at muster stations from the Mustering dashboard. The map also notifies you if there is an alarm by flashing a red icon.

1. From the icon task bar, 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.

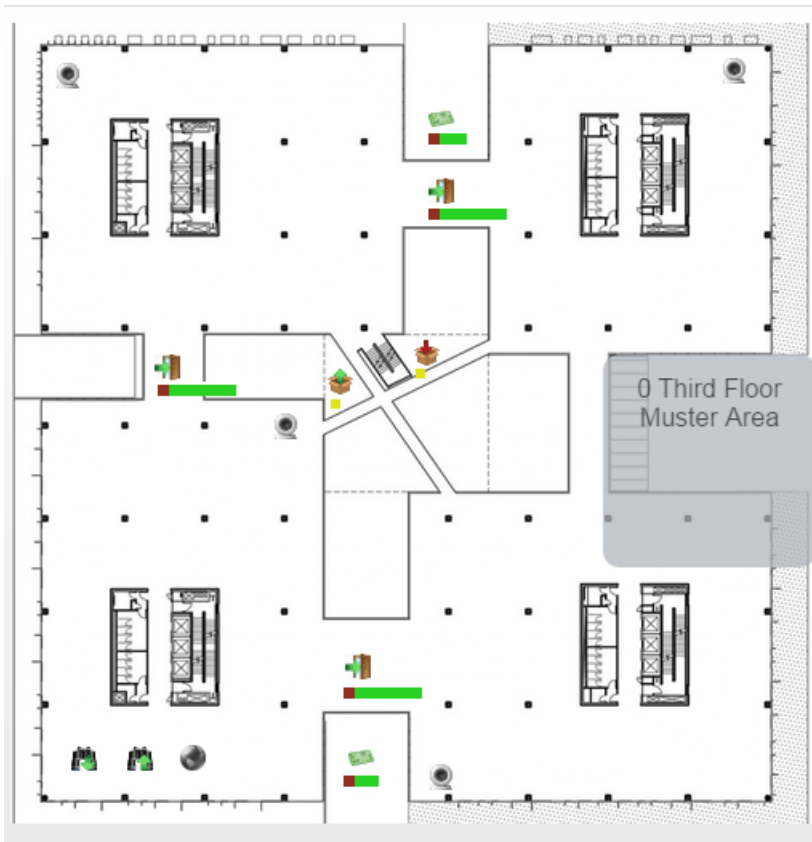










Figure 4: Example map

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 more status information.</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 the previous page.</p>
Review an alarm	<p>If you see a flashing red icon, the item on the map is in an alarm state. Click the icon to see the status details.</p>

To...	Do this...
Control a door	<p>Click  on the map to display the door control menu, then click any of the following:</p> <ul style="list-style-type: none"> • Disable — disable the door. • Unlock — unlock the door. This door will remain unlocked until the Lock command is issued. • Lock — lock the door. This door will remain locked until the Unlock command is issued. • Grant — grant access to the person who is at the door. The door is temporarily unlocked to permit a one time entry through the door. • Restore — reset the door's configuration values to their default value. • Mask Held — mask the Door Held Open Alarm. • Unmask Held — unmask the Door Held Open Alarm. • Mask Forced — mask the Forced Held Open Alarm. • Unmask Forced — unmask the Door Forced Open Alarm. • Trace — display the event transactions for the door. <p>To hide the control menu, click the icon again.</p>
Control a panel or subpanel	<p>Click the  on the map to display the panel control menu, then click any of the following:</p> <ul style="list-style-type: none"> • Panels <ul style="list-style-type: none"> ◦ Download Params — download the latest system configurations to the panel. ◦ Tokens — download the tokens to the panel. ◦ Reset/Download — reset and download the current system configuration to the panel's connected doors. ◦ APB Reset — reset the anti-passback configuration for this panel. ◦ Clock — re-sync the panel time. ◦ Trace — display the event transactions for the panel. • Subpanels <ul style="list-style-type: none"> ◦ Trace — display the event transactions for the subpanel. <p>To hide the control menu, click the icon again.</p>
Control an input	<p>Click the  on the map to display the input control menu, then click any of the following:</p> <ul style="list-style-type: none"> • Mask — mask the input. • Unmask — unmask the input. <p>To hide the control menu, click the icon again.</p>
Control an output	<p>Click the  on the map to display the output control menu, then click any of the following:</p> <ul style="list-style-type: none"> • On — activate the output.


To...	Do this...
	<ul style="list-style-type: none"> • Off — deactivate the output. • Pulse — pulse the output <p>To hide the control menu, click the icon again.</p>
Display video	Click the  on the map to display the Camera Video window. For more information see <i>Monitor Screen - Viewing Camera Video</i> on page 417.
Open a linked map	Click  to display a close-up view of the same map, or  to display a expanded view of the same map.
Execute a global action	Click  to execute the configured global action.
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 plus the name of the area. In the example image, 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.</p> <p>For more information, see <i>Mustering - Using the Dashboard</i> on page 221.</p>

Add Map

Follow the steps below to add maps.

1. Click **Monitor > Maps**. The Map Templates (Monitor) Listing page displays. For more information see *Monitor Screen - Map Templates Page* on page 409.
2. Click **Add New Map Template**.

The **Map Template: Add New** page displays. For more information see *Maps - Add Page* on page 420.

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. For more information see *Maps - Edit Page* on page 278.

Monitor Screen - Events

When you select Monitor from the icon task bar or click the **Events** sub-option, the Monitor Events page is displayed.

This page lists all system activity as it occurs, including doors access.

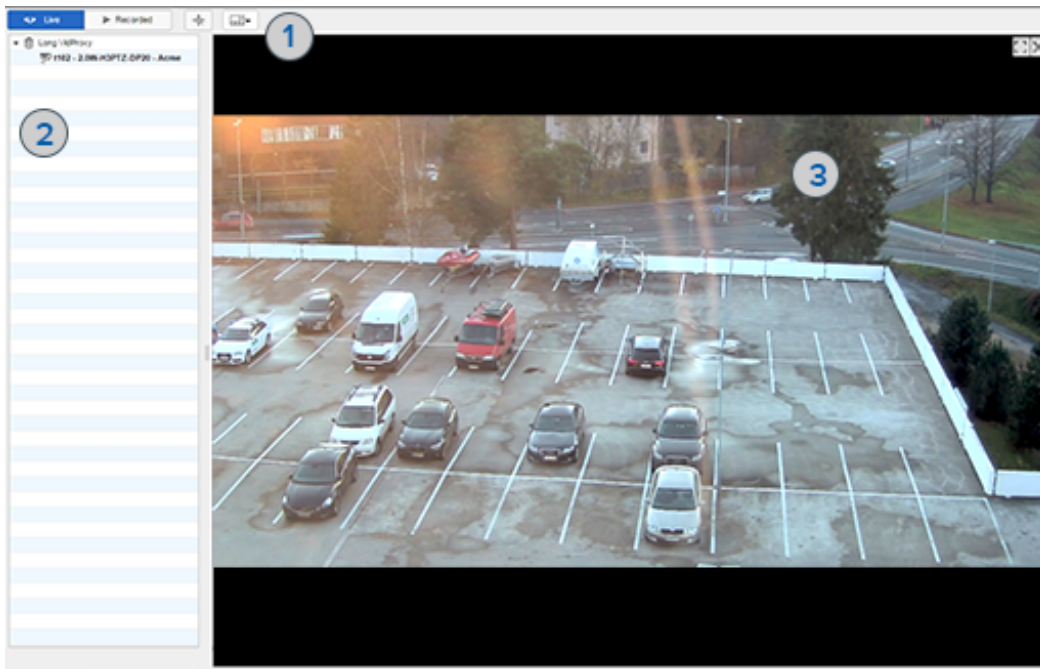
The event transactions are listed with the following information by default:

Feature	Description
Icon	Displays a row of icons to indicate if there are extra details linked to the event. <ul style="list-style-type: none">• : This indicates the event has live video associated with it.• : This indicates the event contains notes that were added by an operator.• : This indicates the event contains instructions that should be completed when the event occurs.
Priority	Displays the urgency of this event where 1 is the most urgent and 999 is the least urgent. Priorities are normally assigned to a specific event using the Priority field on the Event Add page.
Panel Time	Displays the date and time when the source panel issued this event.
Event Name	Displays the name of this event.
Source	Displays the source of the event. Can be a door, reader or system user.
Last Name	Displays the last name of the person responsible for triggering the event. This is almost always the person who used a card or code to enter or exit a supervised area.
First Name	Displays the first name of the person responsible for triggering the event. This is almost always the person who used a card or code to enter or exit a supervised area.
Internal Token No	Displays the internal token number that caused the event to occur. This is usually the number of the card used to enter or exit a supervised area.
Messages	Displays a system message associated with this event.

Monitor Screen - Live Video Window

When you select an event or alarm then click the **Live Video** button, 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.



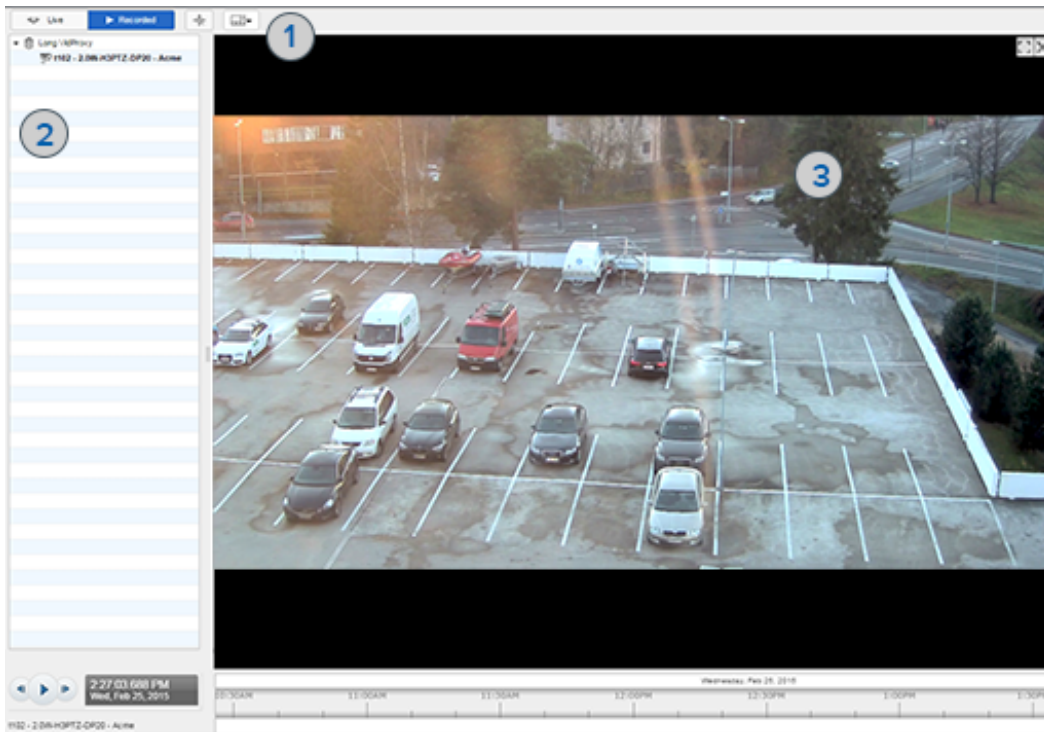
Typically, the Live Video window will include the following elements:

	Feature	Description
1	Camera Controls Tool Bar	This area includes all the features that you would need to view and control the related camera video. Options typically include switching from live to recorded video, PTZ controls for PTZ cameras, and changing the video display layout.
2	Camera List	This area lists all the cameras that are linked to the event. Click the name of a camera to display the video. Use one of the multi-video layouts to display more than one camera at a time.
3	Image Panel	This area displays the video stream from the connected cameras. In the top-right corner, you can minimize and maximize the display or close the video.

Monitor Screen - Recorded Video Window

When you select an event or alarm then click the **Recorded Video** button, the Recorded 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 Recorded Video window will include the following elements:

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

Monitor Screen - Notes Window


When you click the **Notes** button for a selected event transaction, the Notes popup window is displayed.

This Notes window allows you to add notes to the event transaction.

Feature	Description
Event	At the top of the window is a brief summary of the event that you've selected. The provided information includes the date of the event, where it originated, plus the event name and type.
Notes	In the text box, enter any notes you have about the event. Click  to save your note to the event.
Operator	After a note has been saved, it is added to the Operator Notes List.

Feature	Description
Notes List	This list displays all the notes for the event. The list includes the note itself, the name of the operator wrote the note and when the note was saved.

Monitor Screen - Instructions Window

When you select an event with this  icon then can click the **Instructions** button, the Instructions window is displayed.

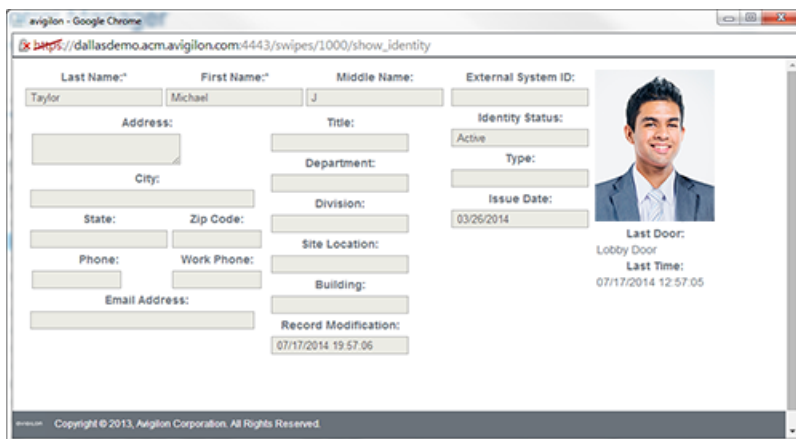
The Instructions window displays any details that you should follow when responding to the selected event. You cannot edit the instructions from this window.

The instructions are added to the event from the *Events - Editing* on page 198 page.

Monitor Screen - Identity Window

When you click the **Identity** button for a selected event transaction, the Identity popup window is displayed.

Many events and alarms occur because of someone using a card or PIN code to access an entry or exit point. To help you identify the person who is accessing the door, the Identity window gives a summary of the person's details.



Notice that this screen includes the same information as the Identity page.

Underneath the identity photo, the last door accessed by this person is displayed, including the time/date when the door was accessed.

Monitor Screen - History Window

When you click the **History** button for a selected event transaction, the History popup window is displayed.


The History window is divided into two halves. The top half displays the event details, and the bottom half displays the history of the event.

Feature	Description
Event	
Panel Date	The date and time of the original event.

Feature	Description
Source	The source of the event.
Event Name	The name of the event that was detected.
History	
Date	The date and time when someone responded to the event.
Action	The action that was performed in response to the event.
Operator	The operator who performed the action.
Notes	The note entered about this action or about the event.

Monitor Screen - Viewing Camera Video

1. From one of the Monitor pages (Events, Alarms, or Search), select an event or alarm that includes a camera.

Only events or alarms with an  icon will have video.

2. Click the **Live Video** or **Recorded Video** button.

The video popup window is displayed.

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.

Monitor Screen - Search


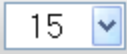


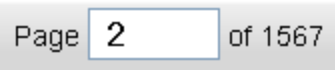



When you click the **Search** sub-option from the Monitor screen, the Events Search (Transactions) page is displayed.

When you first display the Search page, all event transactions are displayed. After you perform a search, the Transactions list updates to only show the events that meet your search criteria.

Scroll to the bottom of the screen and use the search filter to locate specific events. For more information go to *Search Bar* on the facing page.

To perform a event transaction search, see *Searching for Events and Alarms* on page 392

Feature	Description
Transactions	
By default, the following columns are displayed.	
To display additional column options, hover over a column heading then click the down arrow that appears on the right side of the column. A list of all the available options is displayed. Select the check box beside all the headings you want displayed.	
To move a column, click and drag the column to the location of your choice.	
To re-size a column, click and drag the column edges until the columns are the right size.	

Feature	Description
Panel Date	Displays the date and time when the source panel issued this event.
Priority	Displays the urgency of this event where 1 is the most urgent and 100 is the least urgent. Priorities are normally assigned to a specific event using the Priority field on the Event Add page.
First Name	Displays the first name of the person responsible for triggering the event. This is almost always the person who used a card or code to enter or exit a supervised area.
Last Name	Displays the last name of the person responsible for triggering the event. This is almost always the person who used a card or code to enter or exit a supervised area.
Card Number	Displays the internal token number that caused the event to occur. This is usually the number of the card used to enter or exit a supervised area.
Message	Displays a system message associated with this event.
Event Name	Displays the name of this event.
Event Type	Displays the event type.
Source	Displays the source of the event. Can be a door, reader or system user.
Search Bar	
	Click this icon to display the search filters. For more information, see <i>Searching for Events and Alarms</i> on page 392.
	Select the number of items you want to display on a single page.
	Click this button to return to the start of the list.
	Click this button to return to the previous page of the list.
	Enter the page number you want to review. The total number of pages is shown to the right.
	Click this button to go to the next page.
	Click this button to go to the last page.
	Click this button to refresh the search results.

To review the search results, use any of the following buttons:

- **Camera** — Click this button to display live video that is associated with the selected event. For more information, see *Monitor Screen - Viewing Camera Video* on the previous page.
- **Recorded Video** — Click this button to display recorded video that is associated with the selected event. For more information, see *Monitor Screen - Recorded Video Window* on page 414.

- **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, widths, order for this page.

Wildcard Characters

The arguments you can use to search lists include four wildcards.

The asterisk (*) question mark (?) percentage (%) and underscore (_) characters are reserved as wildcard characters.

- The asterisk and question mark characters are for case-sensitive searching where the question mark indicates one character and the asterisk indicates multiple characters.
- The percentage and underscore marks are case-insensitive where the percentage mark indicates one character and the underscore can indicate two or more characters.

Symbol	Description
*	Case-sensitive one character only.
?	Case-sensitive two or more characters.
%	Case-insensitive one character only.
_	Case-insensitive two or more characters.

For example:

- s* - any name starting with "s" and is case-sensitive.
- ?s - any name of three or more characters ending with "s" which is case-sensitive.
- _str% - any name that begins with two or more case-insensitive characters, followed by an "str" and ending with one case-insensitive character.

Monitor Screen - Alarms

When you click the **Alarms** sub-option from the Monitor screen, the Alarms page is displayed.

Alarms are events that are configured to report an alarm when it is triggered. You can configure alarms by assigning events to an alarmed event type. For more information, see *Event Types - Add New Page* on page 233.

This page is divided into two halves — the top Unacknowledged Alarms section and the Acknowledged Alarms section.



- Alarms are automatically added to the Unacknowledged Alarms list as they are triggered. Depending on your alarm settings, you may hear a different sound as different alarms occur.
- The Unacknowledged Alarms list includes all the alarms recorded by the system that have not yet been acknowledged or addressed.

- The Acknowledged Alarms list includes all the alarms that have been acknowledged.
- Alarm events may be highlighted in different colors depending on their alarm state. For more information, see *Events - Colors Listing Page* on page 202.

For more information about the columns that appear on each list, see *Monitor Screen - Events* on page 412.

Maps - Add Page

When you click **Add New Map Template** from the Map Templates Listing Page, the Map Template: Add New page is displayed. From this page, select the image that the map would be based on.



Feature	Description
Name	Enter a name for the map.
File:	Click the Browse button to select the image you want to use as the base of the map. You can select any raster image in PNG, JPEG, BMP and GIF format.
Blank Canvas	Check this box to leave the map background white. This option is primarily for setting up Mustering dashboards that do not need to be on a map.
Re-Size To:	Enter the map size in pixels. 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.
	Click this button to save your changes. After you save the map for the first time, you are taken to the Map Template Edit page where you can add doors, panels, shortcuts and dashboard elements.
	Click this button to discard your changes.

Generating Reports

The Access Control Manager system offers many detailed reports of the current system status. You can generate reports about identities, panels, access details and more.



You have the option of using the default system reports or customizing the reports to fit your needs.

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.




Depending on your web browser, the file may be auto-downloaded or you will be prompted to save the file to your local computer.

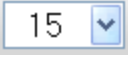





Reports - Report Preview

When you click the name of a report from the Report Listing page, a preview of the selected report is displayed.

You can use the following options to control what is displayed:

Tip: Click  to filter the report. The preview bar expands to display search criteria.

Feature	Description
Generate Report	
The generate report options are displayed in the top left corner of the report preview.	
	Click this button to generate a PDF copy of the current report.
	Click this button to generate a CSV or spreadsheet copy of the current report.
Preview Bar	
The preview options are displayed at the bottom of the report page.	
	Click this icon to filter the report. The report filter options are displayed. The options change depending on the

Feature	Description
	report. <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 data-bbox="237 701 354 751" 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 447.

1. Display the Reports Listing page.
 - To display the system reports page, click **Reports** from the icon task bar.
 - 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* on the facing page.

3. On the following page, select your preferences for the report. The options for each report is different, see the specific Report Edit page for more details.
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.

NOTE: For more details on the individual reports, refer to:


- *Reports - Audit Log* on page 430
- *Reports - Transaction* on page 445

Follow the steps below to edit these reports.


1. Display the Reports Listing page.
 - To display the system reports page, click **Reports** from the icon task bar.
 - 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).


5. Click  to add more search fields, if required.

Complete step 4 above for each additional field added.

6. Click  to save your changes.

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

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




NOTE: Click  if you want to reset the search criteria.

Reports - Listing Page

When you click **Reports** from the icon task bar, the Reports Listing page is displayed.

This page lists all the default system reports and provides the following options for each report:

Feature	Description
Report Name	The name of the report. Click the name to display a preview of the current report.


Feature	Description
Filters	Indicates if there are any filters applied to the report.
Edit	Click  to edit the report options.
PDF	Click  to generate a PDF copy of the report.
Spreadsheet	Click  to generate a CSV or spreadsheet copy of the report.




Listed below are some of the reports that are available:

Reports - Access Grant via Operator

When you click  for the Access Grant via Operator Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Panel Date UTC	In the first row, select the starting date and time of the report. In the second row, select the ending date and time. From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
Door	Select the door that the report should focus on.
Door Location	Enter the door's location.
Operator Name	Enter the name of the operator who performed the action. As you start entering the name, the system performs a search and lists the most similar names in the system. Select the required names.
Card Number	Enter the internal token number related to the event. As you start entering internal token numbers, the system performs a search and lists the closest internal numbers in the system. Select the required internal token numbers.
Search Notes	Enter the notes you want to filter for. The report will only generate the items have the same note text.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.





Reports - Access Groups

When you click  for the Access Group Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.

Criteria





Name	Enter the name of the access group that you want the report to focus on.
Schedule	Select a schedule from the drop down list. Only schedules that have been defined in the system are listed.
Partitions	Select the partition that the access group is part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Action Audit

When you click  for the Action Audit Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.




Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.


Feature	Description
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Panel Date UTC	In the first row, select the starting date and time of the report. In the second row, select the ending date and time. From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
Event Type Name	Enter the name of the event type. As you start entering the name, the system performs a search and lists the most similar event types in the system. Select the required event types.
Event Name	Enter the name of the specific event. As you start entering the name, the system performs a search and lists the most similar events in the system. Select the required events.
Operator	Enter the name of the operator who performed the action. As you start entering the name, the system performs a search and lists the most similar names in the system. Select the required names.
Message	If required, enter the message that may be associated with the event.
Source	Enter the name of the device that is the source of the event. As you start entering the source name, the system performs a search and lists the most similar source names in the system. Select the required items.
Card Number	Enter the internal token number related to the event. As you start entering internal token numbers, the system performs a search and lists the closest internal numbers in the system. Select the required internal token numbers.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Alarm

When you click  for the Alarm Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	<p>Check this box to create a customized copy of this report.</p> <p>Any changes made on this page are automatically applied to the new report.</p>
Report Name	<p>The name of the report.</p> <p>If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.</p>
Criteria	
Panel Date	<p>In the first row, select the starting date and time of the report.</p> <p>In the second row, select the ending date and time.</p> <p>From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.</p>
Source Name	<p>Enter the name of the device that is the source of the event.</p> <p>As you start entering the source name, the system performs a search and lists the most similar source names in the system. Select the required items.</p>
Event Type	<p>Enter the name of the event type.</p> <p>As you start entering the name, the system performs a search and lists the most similar event types in the system. Select the required event types.</p>
Event	<p>Enter the name of the specific event.</p> <p>As you start entering the name, the system performs a search and lists the most similar events in the system. Select the required events.</p>
Operator Name	<p>Enter the name of the operator who performed the action.</p> <p>As you start entering the name, the system performs a search and lists the most similar names in the system. Select the required names.</p>
Card Number	<p>Enter the internal token number related to the event.</p> <p>As you start entering internal token numbers, the system performs a search and lists the closest internal numbers in the system. Select the required internal token numbers.</p>
Search Notes	<p>If required, enter the search term that will identify the alarms you want a report of, according to their included notes.</p>
Operator	<p>Enter the name of the operators that may be involved with the alarm.</p>
Action	<p>Select a specific alarm action.</p>
Message	<p>If required, enter the message that may be associated with the event.</p> <p>You can select one of the Boolean options from the drop down list to narrow your report search.</p>
	<p>Click this button to save your changes.</p>
	<p>Click this button to discard your changes.</p>
	<p>Click this button to generate a PDF version of the report.</p>

Feature	Description
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Appliance

When you click  for the Appliance Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the appliance name.
Host Name	Enter the name of the host computer that is connected to the appliance.
Name Server	Enter the name of the domain server that controls the local network.
Hardware Type	Select the appliance model: Professional or Enterprise .
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Area Identity

When you click  for the Area Identity Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.

Feature	Description
Criteria	
Area Group/Area	Select the area or group of areas that you want the report to focus on.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.


Reports - Area


When you click  for the Area Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.


Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the name of the area you want this report to focus on.
Maximum	Enter the maximum occupancy number for the area.
Log Min	Enter the minimum log value.
Log Max	Enter the maximum log value.
Enable Area	Check this box to only report areas that have been enabled.
Two Persons	Check this box to only report areas that are using the two-person rule.
Partitions	Select the partition the area may be part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Audit Log

When you click **Audit Log Report**, an empty Report Preview page is displayed. Click  to generate a list of all the recorded system transactions.

In the bottom left corner, click  to expands the report criteria. The report search criteria is laid out in this format: *search type + search operator + search value*.



Select a search type and search operator in the **Find** section. In the third field, enter the specific search value that you want to include in the report.

Click  to add more search fields, if required.

Search Type	Search Operator	Search Values
Panel Date	<ul style="list-style-type: none"> greater or equal less or equal 	<p>Select the starting date and time of the report.</p> <p>You have the option of selecting to only show items that are Less than (or equal) or Greater than (or equal) the selected date.</p>
Panel Date UTC	<ul style="list-style-type: none"> greater or equal less or equal 	<p>Select the ending date and time.</p> <p>You have the option of selecting to only show items that are Less than (or equal) or Greater than (or equal) the selected date.</p>
Event	<ul style="list-style-type: none"> in 	<p>Select an event from the list.</p> <p>Shift + click to select multiple items in sequence.</p> <p>Ctrl + click to select multiple items out of sequence.</p>
Operator	<ul style="list-style-type: none"> in 	<p>Enter the name of the operator who performed the action.</p> <p>As you start entering the name, the system performs a search and lists the most similar names in the system. Select the required names.</p>
Event Type	<ul style="list-style-type: none"> in 	<p>Select an event type from the list.</p> <p>Shift + click to select multiple items in sequence.</p> <p>Ctrl + click to select multiple items out of sequence.</p>
Message	<ul style="list-style-type: none"> equal begins with ends with contains 	<p>Enter text of a system generated message.</p>
Source	<ul style="list-style-type: none"> in 	<p>Enter the name of the device that is the source of the event. As you start entering the source name, the system performs a search and lists the most similar source names in the system. Select the required items.</p>
Before	<ul style="list-style-type: none"> contains 	<p>Entry before the change.</p>
After	<ul style="list-style-type: none"> contains 	<p>Entry after the change.</p>
Card Number	<ul style="list-style-type: none"> equal 	<p>Enter the internal token number related to the event.</p>

Search Type	Search Operator	Search Values
		As you start entering internal token numbers, the system performs a search and lists the closest internal numbers in the system. Select the required internal token numbers.





After you've set the filters for the report, you can use any of the following options:

Feature	Description
	Click this button to add a new line of search criteria.
	Click this button to delete the line of search criteria.
Save	Click this button to save your changes. The default system report will use the updated report criteria.
Create Custom Report	Enter a name then click this button to save your changes as a custom report.

Reports - Cameras

When you click  for the Camera Report, the Report Edit page is displayed.





Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the name of the camera that you want the report to focus on.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Collaboration

When you click  for the Collaboration Report, the Report Edit page is displayed.


Edit any of the following options to filter the report, or create a customized version of the report.




Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the name of the collaboration that you want the report to focus on.
Type	Select the collaboration type.
Appliance	Select the appliance that manages the collaboration.
Installed	Check this box to indicate that only the collaborations that are currently connected and communicating on the system should be part of this report.
Partitions	Select the partition the collaboration is part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Delegation Comparison

When you click  for the Delegation Comparison Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Select two or more delegations from the list to compare and report. <ul style="list-style-type: none"> • Shift + click to select multiple delegations in sequence. • Ctrl + click to select multiple delegations out of sequence.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Delegation

When you click  for the Delegation Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Select one or more delegations for the report to focus on.
Partitions	Select the partition the delegation is part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Door Configuration

When you click  for the Door Config Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.





Feature	Description
Criteria	
Name	Enter the full name of the door the report should focus on.
Door	If you do not know the full name of the door, select the door from the list.
Location	Enter the location of the door.
Appliance	Select the appliance the door is connected to.
Vendor	Select the type of panel the door is connected to.
Partitions	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 appear in this list. You can only see the partitions that you are a member of. If no partitions are defined for this system, this pane is hidden.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Door/Identities with Access

When you click  for the Door/Identities with Access Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.


Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the name of the door the report will focus on.
Access Group Key	Enter the access group name. As you start entering the name, the system performs a search and lists the most similar access groups in the system. Select the required access groups.
Schedule	Select the schedule used by the door or related access group.
Token	Select the token status.




Feature	Description
Status	
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Event

When you click  for the Event Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the event name.
Return Name	Enter the return name for the event.
Event Type	Select the event type.
Source Type	Select the source of the event.
Priority	Enter the priority number for the event. The range is 1 - 999 where 1 is the highest priority and 999 is the lowest.
Suppress Time	Select the schedule that is used when event alarms are not reported.
Return Event	Select the return event type.
Return Priority	Enter the priority number for the return event.
Has On/Off	Check this box to indicate that the event uses an on/off mode.
Masked	Check this box to indicate that event is masked.
Logged	Check this box to indicate that the event is logged.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.





Reports - Event Type

When you click  for the Event Type Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.





Criteria

Name	Enter the name of the event type.
Suppress Schedule	Select the schedule used to define when the event type is inactive.
Priority	Enter the priority assigned to this event type.
Masked	Check this box to specify that the event type is masked.
Logged	Check this box to specify that the event type is logged.
Alarm	Check this box to specify that the event type is alarmed.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Group

When you click  for the Group Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the group name.
Policy	Select the policy that is associated with the group.
Members	Select an identities that may be part the group.
Partitions	Select the partition that the group may be part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Holiday


When you click  for the Holiday Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the name of the holiday.
Date	Click the left field to select the specific date of the holiday. If you are unsure of the date, use the drop down list to filter the holidays that are Less than or Greater than the date you entered on the left.
Additional Days	Enter the number of additional days that have been configured for the holiday.
Type	Select the holiday type number.

Feature	Description
Partitions	Select the partition that the holiday may be part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Identity Photo Gallery

When you click  for the Identity Photo Gallery Report, the Report Edit page is displayed.


Edit any of the following options to filter the report, or create a customized version of the report.




Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Role	Select the role that the identity may be part of.
Department	Select the department.
Login	Enter the identity's login name.
Type	From the drop down option list, select the type of identity (e.g. employee).
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report. NOTE: This version of this report does not include photos.

Reports - Identity Summary

When you click  for the Identity Summary Report, the Report: Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter a name using any combination of letters, numbers, and wild cards required to specify the required identity.
Last name	Enter a last name for this identity using any combination of letters, numbers, and wild cards required to specify the required identity.
First name	Enter a first name for this identity using any combination of letters, numbers, and wild cards required to specify the required identity.
Middle Name	Enter a middle initial for this identity using any combination of letters, numbers, and wild cards required to specify the required identity.
Status	From the drop down option list, select the current status of the person you want to report. There are currently four status options available: Active , Expired , Lost , and Stolen .
Role	From the drop down option list, select a role to which this person is assigned. Only those can appear in this list.
Group	From the drop down option list, select a group to which this person is assigned. Only the option Everyone is available by default. All other for this system.
Login	Enter the identity's login name.
Type	From the drop down option list, select the type of identity (e.g. employee).
Issue Date	In the first row, select the starting date and time of the report. In the second row, select the ending date and time. From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
Active Date	In the first row, select the starting date and time of the report. In the second row, select the ending date and time. From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
Deactivate	In the first row, select the starting date and time of the report. In the second row, select the ending date and time. From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
	Click this button to save your changes.

Feature	Description
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Identity/Doors with Access

When you click  for the Identity/Door with Access Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Identity	Enter the name of the identity the report will focus on.
Token Status	Select the token status.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Panel

When you click  for the Panel Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot

Feature	Description
	be edited.
Criteria	
Name	The name of the panel that the report will focus on.
Appliance	Select the appliance the panel is connected to.
Installed	Check this box to indicate the appliance can communicate with the connected device.
Partitions	Select the partition the panel is part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Policy

When you click  for the Policy Report, the Report Edit page is displayed.





Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	The name of the policy the report will focus on.
Installed	Check this box to indicate that the policy is assigned, communicating with the host and active.
Partition	Select the partition the policy is part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Role

When you click  for the Role Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.





Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Name	Enter the name of the role the report will focus on.
Parent Role	Select the parent role if required.
Start Date	In the first row, select the starting date and time of the report. In the second row, select the ending date and time.
Stop Date	From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
Installed	Check this box to indicate that the role is active.
Partitions	Select the partition the role is part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Schedule

When you click  for the Schedule Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot





Feature	Description
	be edited.
Criteria	
Name	Enter the name of the schedule the report will focus on.
Mode	Select the schedule mode.
Partitions	Select the partition the schedule is part of.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Token

When you click  for the Token Report, the Report Edit page is displayed.

Edit any of the following options to filter the report, or create a customized version of the report.


Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Token Status	Select the current status of the token. The options are: <ul style="list-style-type: none"> Active Expired Inactive Not Yet Active
Embossed Number	Enter the number that is printed or embossed on the card or badge.
Internal Number	Enter the internal card or badge number if it is different from the embossed number.
Issue Date	Specify the time and date when this token was issued, or specify a range during which this token might have been issued. In the first row, select the starting date and time of the report. In the second row, select the ending date and time.




Feature	Description
	From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
Activate Date	Specify the time and date during which this token was active or specify a range during which this token was active. In the first row, select the starting date and time of the report. In the second row, select the ending date and time. From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
Deactivate Date	Specify the time and date during which this token was deactivated or specify a range during which this token was deactivated. In the first row, select the starting date and time of the report. In the second row, select the ending date and time. From the drop down list at the end of each row, you have the option of selecting to only show items that are Less than or Greater than the selected date.
	Click this button to save your changes.
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Tokens Pending Expiration Date


When you click  for the Token Report, the Report Edit page is displayed.


Edit any of the following options to filter the report, or create a customized version of the report.

Feature	Description
Copy Report	Check this box to create a customized copy of this report. Any changes made on this page are automatically applied to the new report.
Report Name	The name of the report. If you've chosen to copy this report, you can change the report name. Otherwise, this field cannot be edited.
Criteria	
Expires in	Enter the number of days before a token expires.
	Click this button to save your changes.


Feature	Description
	Click this button to discard your changes.
	Click this button to generate a PDF version of the report.
	Click this button to generate a CSV or spreadsheet version of the report.

Reports - Transaction

When you click **Transaction Report**, an empty Report Preview page is displayed. Click  to generate a list of all the recorded system transactions.

In the bottom left corner, click  to expand the report criteria. The report search criteria is laid out in this format: *search type + search operator + search value*.

Select a search type and search operator in the **Find** section. In the third field, enter the specific search value that you want to include in the report.



Click  to add more search fields, if required.

Search Type	Search Operator	Search Values
Panel Date	<ul style="list-style-type: none"> greater or equal less or equal 	Click the field then select the transaction date and time.
Source	<ul style="list-style-type: none"> in 	Enter the name of the device that is the source of the event. As you start entering the source name, the system performs a search and lists the most similar source names in the system. Select the required items.
Event	<ul style="list-style-type: none"> in 	Select an event from the list. Shift + click to select multiple items in sequence. Ctrl + click to select multiple items out of sequence.
Event Type	<ul style="list-style-type: none"> in 	Select an event type from the list. Shift + click to select multiple items in sequence. Ctrl + click to select multiple items out of sequence.
Card Number	<ul style="list-style-type: none"> Equal 	Enter an internal token number.
Last Name	<ul style="list-style-type: none"> equals begins with ends 	Enter the surname name of an identity.

Search Type	Search Operator	Search Values
	<ul style="list-style-type: none"> with contains 	
First Name	<ul style="list-style-type: none"> equals begins with ends with contains 	Enter the first name of an identity.
Message	<ul style="list-style-type: none"> equals begins with ends with contains 	Enter text of a system generated message.
Full Name	<ul style="list-style-type: none"> equals begins with ends with contains 	<p>Enter the full name of an identity.</p> <p>As you start entering the name, the system performs a search and lists the most similar names in the system. Select the required identities.</p>
Embossed Number	<ul style="list-style-type: none"> equals 	Enter the number that is printed or embossed on a card or badge.
Department	<ul style="list-style-type: none"> in 	<p>Select the department the related transaction identity is assigned to.</p> <p>Shift + click to select multiple items in sequence.</p> <p>Ctrl + click to select multiple items out of sequence.</p>
Building	<ul style="list-style-type: none"> in 	<p>Select the building.</p> <p>Shift + click to select multiple items in sequence.</p> <p>Ctrl + click to select multiple items out of sequence.</p>
Division	<ul style="list-style-type: none"> in 	<p>Select the division.</p> <p>Shift + click to select multiple items in sequence.</p> <p>Ctrl + click to select multiple items out of sequence.</p>
Site Location	<ul style="list-style-type: none"> in 	<p>Select the site location.</p> <p>Shift + click to select multiple items in sequence.</p> <p>Ctrl + click to select multiple items out of sequence.</p>
Identity Type	<ul style="list-style-type: none"> in 	<p>Select the identity type.</p> <p>Shift + click to select multiple items in sequence.</p>



Search Type	Search Operator	Search Values
		Ctrl + click to select multiple items out of sequence.
Notes	<ul style="list-style-type: none"> • equals • begins with • ends with • contains 	<p>Enter the event note details that you want to filter for.</p> <p>The report will only generate the items that have the same note text.</p>
Panel Date Range	• number of days	Enter a number. The report will filter for transactions that occurred in the last # <i>number of days</i> starting from today.

After you've set the filters for the report, you can use any of the following options:

Feature	Description
	Click this button to add a new line of search criteria.
	Click this button to delete the line of search criteria.
Save	<p>Click this button to save your changes.</p> <p>The default system report will use the updated report criteria.</p>
Create Custom Report	Enter a name then click this button to save your changes as a custom report.



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.


1. Click **Reports** from the icon task bar.
2. Click  for the report you want to base the custom report on.
3. On the following Report Edit page, select the **Copy Report** check box.
4. Give the new report a name.
5. Edit the report options to meet your requirements.
6. 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 Transaction Reports

1. Click **Reports** from the icon task bar.
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.

Reports - Custom Reports Listing Page

When you select **Reports > Custom Reports** from the icon task bar, the Custom Reports Listing page is displayed.


This page lists all the custom reports that have been added to the system and provides the following options for each report:










Feature	Description
Name	The name of the custom report. Click the name to display a preview of the report.
Edit	Click  to edit the report options.
Schedule	Click Schedule to create a batch job to generate the report. For more information, see <i>Scheduling Batch Jobs</i> on page 8. The batch report options automatically include the custom report details.
Filters	Indicates the filters that are used in the custom report.
Export PDF	Click  to generate a PDF copy of the report.
Export Spreadsheet	Click  to generate a CSV or spreadsheet copy of the report.
Delete	Click  to delete the custom report.

Reports - Custom Report Preview

When you click the name of a report from the Custom Report Listing page, a preview of the selected report is displayed.

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 data-bbox="240 1234 363 1281" 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.