

# Monitoring Supervisor Guide

Access Control Manager™

Version 6.50.0

© 2016 - 2024, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logos, AVIGILON CONTROL CENTER, ACC, ACCESS CONTROL MANAGER, ACM and ACM VERIFY are trademarks of Avigilon Corporation. HID, HID GLOBAL, and VERTX are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries. Allegion and Schlage are trademarks of Allegion plc, its subsidiaries and/or affiliates in the United States and other countries. Other names or logos mentioned herein may be the trademarks of their respective owners. The absence of the symbols ™ and ® in proximity to each trademark in this document or at all is not a disclaimer of ownership of the related trademark.

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

Avigilon Corporation  
avigilon.com

PDF-ACM-MSG-6.50.0-A

Revision: 1 - EN

20240121

# Revisions

ACM Release	Description
Release 6.50	-

# Table of Contents

Revisions .....	3
Introduction .....	7
Managing Notes .....	8
Monitoring .....	9
Monitoring Events .....	9
Pause/Resume Events .....	10
Clear Events .....	10
View Live Video .....	10
View Recorded Video .....	11
Create Event Notes .....	11
View Event Notes .....	12
View Event Instructions .....	12
View Event Identity Details .....	12
View Event History .....	12
Change Events List Settings .....	13
Reconnect to Events List .....	13
Searching for Events and Alarms .....	14
View Camera (Search) .....	15
View Recorded Video (Search) .....	15
Create Event Notes (Search) .....	15
View Event Notes (Search) .....	16
View Event Instructions (Search) .....	16
View Event Identity Details (Search) .....	16
View Event History (Search) .....	17
Change Transactions List Settings .....	17
Monitoring Alarms .....	18
Acknowledge Alarms .....	19
Assign Alarms .....	19
View Live Video (Alarms) .....	19
View Recorded Video (Alarms) .....	20
Create Event Notes (Alarms) .....	20
View Event Notes (Alarms) .....	21
View Event Instructions (Alarms) .....	21
View Event Identity Details (Alarms) .....	21
View Event History (Alarms) .....	22
Change Alarms List Settings .....	22
Turning Sound On/Off .....	22
Using the Verification page .....	24
Verifying Identities at Doors .....	24
Verification Events List .....	24

Using the Dashboard .....	26
Status Colors .....	27
Appliance Transactions Indicators .....	28
Device Status .....	28
Security Status .....	29
Controlling Doors .....	30
Door Modes .....	31
Using Map Templates .....	33
Adding Maps .....	33
Using a Map .....	33
Viewing a Map .....	33
Hardware Status .....	34
Map Actions .....	35
Monitoring Bosch Intrusion Panels .....	38
Monitor Bosch Intrusion Panel Status .....	38
Monitoring Areas in Bosch Intrusion Systems .....	38
Viewing Areas .....	38
Arming Areas .....	39
Arming Perimeter Areas .....	39
Disarming Areas .....	39
Silencing Keypad Alarms .....	40
Clearing Alarms .....	40
Resetting Sensors .....	40
Monitor Bosch Intrusion Panel Points .....	40
Monitor Bosch Intrusion Panel Outputs .....	41
Monitoring and Controlling DMP Intrusion Systems .....	41
Viewing Panels, Areas, Zones and Outputs .....	41
Silencing Keypad Alarms on Panels .....	42
Resetting Sensors on Panels .....	42
Arming or Disarming Areas .....	42
Bypassing Zones and Resetting Bypassed Zones .....	43
Activating and Deactivating Outputs .....	43
<b>Identities .....</b>	<b>44</b>
Adding an Identity .....	44
Assigning Roles to Identities .....	45
Assigning Tokens to Identities .....	46
Assigning Groups to Identities .....	47
Capturing and Uploading Photos of an Identity .....	47
Creating Badges for Identities .....	51
Searching for an Identity .....	52
Editing an Identity .....	53
Enrolling Identities and Issuing HID Origo Tokens .....	54

Issuing a Token to an Enrolled Identity on a Registered Mobile Device .....	54
Registering a New Mobile Device for an Enrolled Identity .....	54
Searching for HID Origo Tokens .....	54
Setting Up Multi-Factor Authentication .....	55
Add Your MFA Devices .....	55
Add MFA Device .....	55
Delete MFA Device .....	56
Disable MFA .....	56
Logging In .....	56
Reports .....	57
Generating Reports .....	57
Report Preview .....	57
Editing Reports .....	58
Editing Audit Log and Transaction Reports .....	59
Creating Custom Reports .....	60
Scheduling a Custom Report By Batch Job (Specification) .....	60
Creating Custom Audit Log and Transaction Reports .....	61
Identity Correlation Report .....	62
Example uses .....	62
Generating the report .....	62
Generating a report for other identity correlations .....	62
Exporting the report to a spreadsheet .....	63
Setting Personal Preferences .....	64
Changing the Password in My Account .....	64
External Systems - Defining the Badge Camera for the System .....	64
Scheduling Batch Jobs .....	64
Generating a Batch Report .....	65
Applying an Identity Profile to a Group Using a Job Specification .....	66
Applying a Door Template to a Group Using a Job Specification .....	67
Scheduling a Global Action .....	69
Setting Batch Door Modes .....	70
Setting Your Preferred Language .....	71
Permissions and Rights .....	73

# Introduction

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

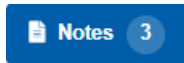
Monitoring Supervisors oversee the Enrollment and Monitoring Operators. They are responsible for responding to events and alarms, monitoring the hardware status of the system, adding and maintaining identities, creating reports, and scheduling and running batch jobs. For more information, see *Permissions and Rights* on page 73.

**Note:** This guide does not define the role of a Monitoring Supervisor on all sites. Please contact your System Administrator for more details.

# Managing Notes

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

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



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



# Monitoring

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

Monitoring Supervisors are responsible for:


- Monitoring system events
- Monitoring alarms
- Monitoring hardware status
- Responding to alarms
- Controlling hardware

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

## Monitoring Events

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

To view the events:

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

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


- **Pause** button — Pauses the flow of events that are displayed on the page.  
The flow of events does not actually stop, the system simply pauses the display of live updates until you click **Resume**.
- **Resume** button — Restarts the flow of events that are displayed on the page.  
This button only appears when the flow of events is paused.
- **Clear** button — Temporarily clear all events from the screen. New events automatically begin to populate the list. To restore the cleared events, refresh the page.
- **Live Video** button — Displays live video that is associated with the selected event.
- **Recorded Video** button — Displays recorded video that is associated with the selected event.
- **Notes** button — Enter a new note or displays any previously saved notes for the selected event.

- **Instructions** button — Displays any instructions that should be completed when the event occurs. The instructions were added when the event was created.
- **Identity** button — Displays details about the person that triggered the selected event.
- **History** button — Displays a detailed history of this event.
- **Save Settings** button — Saves your current settings for this page. For example, the columns and order for this page.
- **Select Columns** button — Choose the information that you want displayed.  
Check the box for each column that you want to see, and clear the box for each column that you want hidden.  
Click and drag the columns to move them into the order you want.
- **Reconnect** button — Reconnects to the appliance.  
This button only appears if your browser has become disconnected from the appliance and an error is displayed.

## Pause/Resume Events


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

Follow the steps below to pause and resume events.

1. Click  **Monitor** to access the Monitor Events page. For more detail see *Monitoring Events* on the previous page.
2. Click **Pause** to pause the flow of events that are displayed on the page.  
The flow of events does not actually stop, the system simply pauses the display of live updates until you click **Resume** (this button only appears when the flow of events is paused).
3. Click **Resume** to restart the flow of events that are displayed on the page.  
The list of events will resume updating.

## Clear Events

Follow the steps below to clear all displayed events.



1. Click  **Monitor** to access the Monitor Events page.
2. Click **Clear** to temporarily clear all events from the screen.  
The list will be cleared. New events automatically begin to populate the list.

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

## View Live Video

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



Follow the steps below to view live video.

1. Click  **Monitor**. The Monitor Events page displays (for more information, see *Monitoring Events* on page 9).
2. Select an event from the list.  
Only events or alarms with an  icon will have video.
3. Click **Live Video** to display live video that is associated with the selected event. (This button only displays if video is available for this event.)  
The Monitor Screen - Live Video window displays. View the live video in this window.  
If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## View Recorded Video

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



Follow the steps below to view live video.

1. Click  **Monitor**. The Monitor Events page displays (for more information, see *Monitoring Events* on page 9).
2. Select an event from the list.  
Only events or alarms with an  icon will have video.
3. Click **Recorded Video** to display recorded video that is associated with the selected event. (This button only displays if video is available for this event.)  
The Monitor Screen - Recorded Video window displays. View the video in this window.  
If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## Create Event Notes

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




Follow the steps below to create event notes.

1. Click  **Monitor** to access the Monitor Events page.
2. Select the event that you want to create notes for.
3. Click **Notes** to create notes for the selected event.  
The Monitor Screen - Notes Window will display.
4. Enter text in the **New Note** field.
5. Click  to save the new note.  
The note will display in the list below the **New Note** section. The date, Operator and note will display in this list.
6. Close the dialog box.

## View Event Notes

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



Follow the steps below to view event notes.

1. Click  **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 9).
2. Select the event that you want to view notes for. (Events with notes will display with  in the **Icon** column.)
3. Click **Notes** to view notes for the selected event. (Alternatively clicking  will do the same thing.) The Monitor Screen - Notes Window will display. Existing notes will display as a list below the **New Note** section. The date, Operator and note will display in this list.

## View Event Instructions


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

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

1. Click  **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 9).
2. Select the event that you want to view instructions for. (Events with instructions will display with  in the **Icon** column.)
3. Click **Instructions** to view instructions for the selected event.  
The Monitor Screen - Instructions Window will display. View the instructions in the table that displays.
4. Close the window to return to the Monitor Events page.


## View Event Identity Details

Follow the steps below to view event identity details.

1. Click  **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 9).
2. Select the event that you want to view identity details for.
3. Click **Identity** to view identity details for the selected event.  
The Monitor Screen - Identity Window will display.
4. View the details (e.g. Last Name, First Name, Title, etc.).
5. Close the window to return to the Monitor Events page.


## View Event History

Follow the steps below to view event history.

1. Click  **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 9).
2. Select the event that you want to view history for.
3. Click **History** to view history for the selected event.  
The Monitor Screen - History Window will display.
4. View the history details.
5. Close the window to return to the Events list.


## Change Events List Settings

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

1. Click  **Monitor** to access the Monitor Events page.  
The list displays in date order, with the most recent events at the top of the list.
2. If you want to re-sort the order of the list:
  - Click in the heading of the column to sort by (e.g. Priority). The list will sort in ascending order based on that column (e.g. ascending order of priority).
  - To change the sort order to descending, click the column heading again.
3. If you want to re-sort the order of the columns, click on the column you want to move then drag and drop this to 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.
5. Click **Save Settings** if you want to save the new settings.  
A message box displays with the message ACM Notification. Successfully saved.'.

## Reconnect to Events List



Follow the steps below to reconnect to the ACM appliance.

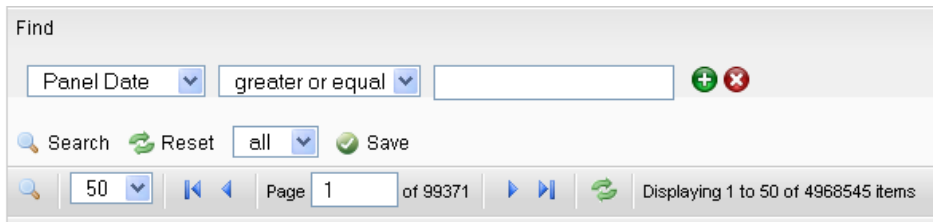
1. Click  **Monitor** to access the Monitor Events page (for more information, see *Monitoring Events* on page 9).  
If your browser loses connectivity with ACM appliance the **Reconnect** button displays.
2. Click **Reconnect** to reconnect.

# Searching for Events and Alarms

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



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

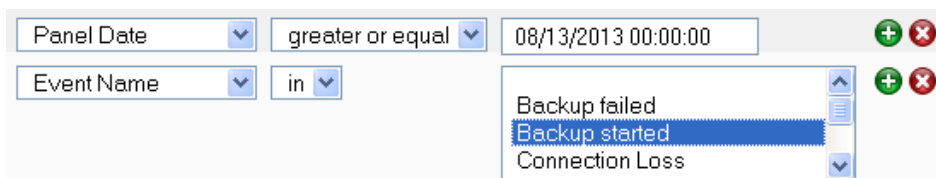
1. Select  **Monitor > Search**.
2. Scroll to the bottom of the page and click the  icon.




The image shows a search interface titled "Find". It features a search bar with a dropdown menu set to "Panel Date", a comparison operator dropdown set to "greater or equal", and an empty text input field. To the right of the input field are green "+" and red "x" icons. Below the search bar are buttons for "Search" (with a magnifying glass icon), "Reset" (with a circular arrow icon), a dropdown menu set to "all", and a "Save" button (with a green checkmark icon). At the bottom, there is a pagination bar showing "50" items per page, "Page 1 of 99371", and a status message "Displaying 1 to 50 of 4968545 items".

**Figure 1:** Search options

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




The image shows the search results interface. It features two search filters. The first filter has a dropdown menu set to "Panel Date", a comparison operator dropdown set to "greater or equal", and a text input field containing "08/13/2013 00:00:00". To the right of the input field are green "+" and red "x" icons. The second filter has a dropdown menu set to "Event Name" and a comparison operator dropdown set to "in". Below the second filter is a list of search results: "Backup failed", "Backup started" (highlighted in blue), and "Connection Loss". To the right of the list are green "+" and red "x" icons.


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

## View Camera (Search)

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

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

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

Only events or alarms with an  icon will have video. The icons are not displayed by default. For more information, see *Change Transactions List Settings* on page 17.

3. Click **Camera** to display live video that is associated with the selected event.
4. View the live video in this window.


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

## View Recorded Video (Search)

Recorded video that is associated with a searched event can be displayed from the Monitoring Search page. For example, if an unusual event is found in the search results, the recorded video can be viewed to observe the event and determine if any actions need to be taken.

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

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

Only events or alarms with an  icon will have video. The icons are not displayed by default. For more information, see *Change Transactions List Settings* on page 17.

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

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

4. View the video in this window.



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

## Create Event Notes (Search)

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

made on an event, a note can be created for that event.


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

1. Click  **Monitor > Search**.
2. Select the event that you want to create notes for.
3. Click **Notes** to create notes for the selected event.  
The Monitor Screen - Notes Window will display.
4. Enter text in the **New Note** field.
5. Click  to save the new note.  
The note will display in the list below the **New Note** section. The date, Operator and note will display in this list.
6. Close the dialog box.

## View Event Notes (Search)

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


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

1. Click  **Monitor > Search**.
2. Select the event that you want to view notes for.
3. Click **Notes** to view notes for the selected event.  
The Monitor Screen - Notes Window will display. Existing notes will display as a list below the **New Note** section. The date, Operator and note will display in this list.

## View Event Instructions (Search)

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


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

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

## View Event Identity Details (Search)


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



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


## View Event History (Search)

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


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

## Change Transactions List Settings


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

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

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

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

# Monitoring Alarms

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

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

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

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

- **Acknowledge** — Click this button to acknowledge one or more selected alarms. The selected alarms are moved to the Acknowledged Alarms list.
- **Acknowledge All** — Click this button to acknowledge all alarms that are currently active and unacknowledged.
- **Live Video** — Click this button to display live video associated with the selected alarm.
- **Recorded Video** — Click this button to display recorded video associated with the selected alarm.
- **Notes** — Click this button to enter a new note or display any previously saved notes for the selected event.
- **Instructions** — Click this button to display any instructions that should be completed when the alarm occurs. The instructions were added when the event was created.
- **Identity** — Click this button to display details about the person that triggered the selected alarm.
- **History** — Click this button to display a detailed history of this alarm.
- **Assign** — Click this button to assign one or more selected alarms to a specific operator.
- **Save Settings** — Click this button to save your current settings for this page. For example, the columns and order for this page.
- **Sound Off** — Click this button to mute any alarm sounds on the device used to monitor Alarms. When sound is muted, the button changes to **Sound On**. Click this button to turn the sound back on.
- **Select Columns** — Click this button then choose the information that you want displayed. Check the box for each column that you want to see, and clear the box for each column that you want hidden.

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


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

- **Clear** — Click this button to clear one or more acknowledged alarms from the list.
- **Clear All** — Click this button to clear all alarms from the Acknowledged Alarms list.
- **Select Columns** — Click this button then choose the information that you want displayed.  
Check the box for each column that you want to see, and clear the box for each column that you want hidden.

## Acknowledge Alarms

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

Follow the steps below to acknowledge alarms.

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

## Assign Alarms

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

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

To assign one or more alarms:

1. Click **Monitor > Alarms**. The Monitor Alarms page displays (for more information see *Monitoring Alarms* on the previous page).
2. Click on one or more alarms.  
To select a series of alarms, click the first alarm then **Shift** + click the last alarm in the series. To select non-contiguous alarms, **Ctrl** + click the alarms you want to select.
3. Click **Assign**.
4. Select an operator from the drop-down list.
5. Click **Save**.



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

## View Live Video (Alarms)

Live video that is associated with a selected alarm can be displayed from the Monitoring Alarms page. For

example, if an alarm occurs, the live video can be viewed to observe the alarm and determine if any actions need to be taken.



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

1. Click  **Monitor > Alarms**. For more information see *Monitoring Alarms* on page 18.
2. Select an alarm from the list.  
Only events or alarms with an  icon will have video.
3. Click **Live Video** to display live video that is associated with the selected alarm. This button only displays if video is available for this alarm.  
The Monitor Screen - Live Video window displays. View the live video in this window.  
If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## View Recorded Video (Alarms)

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



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

1. Click  **Monitor > Alarms**. The Monitor Alarms page displays (for more information see *Monitoring Alarms* on page 18).
2. Select an event from the list.  
Only events or alarms with an  icon will have video.
3. Click **Recorded Video** to display live video that is associated with the selected event. (This button only displays if video is available for this event.)  
The Monitor Screen - Recorded Video window displays. View the video in this window.  
If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

## Create Event Notes (Alarms)

Notes can be added and viewed for all alarms that occur in the system. For example, if an observation or action is made on an alarm, a note can be created to document the details.

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

1. Click  **Monitor > Alarms**. The Monitor Alarms page displays. For more information see *Monitoring Alarms* on page 18.
2. Select the event that you want to create notes for.
3. Click **Notes** to create notes for the selected event.  
The Monitor Screen - Notes Window will display.
4. Enter text in the **New Note** field.
5. Click  to save the new note.  
The note will display in the list below the **New Note** section. The date, Operator and note will display




in this list.

6. Close the dialog box.

## View Event Notes (Alarms)

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



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

1. Click  **Monitor > Alarms**. The Monitor Alarms page displays. For more information see *Monitoring Alarms* on page 18.
2. Select the event that you want to view notes for. Events with notes will display with  in the **Icon** column.
3. Click **Notes** to view notes for the selected event. Alternatively clicking  will do the same thing. The Monitor Screen - Notes Window will display. Existing notes will display as a list below the **New Note** section. The date, Operator and note will display in this list.
4. Close the dialog box to return to the Monitor Alarms page.

## View Event Instructions (Alarms)


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

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

1. Click  **Monitor > Alarms** to access the Monitor Alarms page displays. For more information see *Monitoring Alarms* on page 18.
2. Select the event that you want to view instructions for. (Events with instructions will display with  in the **Icon** column.)
3. Click **Instructions** to view instructions for the selected event. The Monitor Screen - Instructions Window will display. View the instructions in the table that displays.
4. Close the window to return to the Monitor Alarms page.


## View Event Identity Details (Alarms)

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

1. Click  **Monitor > Alarms**. The Monitor Alarms page displays. For more information see *Monitoring Alarms* on page 18.
2. Select the event that you want to view identity details for.
3. Click **Identity** to view identity details for the selected event. The Monitor Screen - Identity Window will display.
4. View the details (e.g. Last Name, First Name, Title, etc.).
5. Close the window to return to the Monitor Alarms page.


## View Event History (Alarms)


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

1. Click  **Monitor > Alarms** to access the Monitor Alarms page. For more information see *Monitoring Alarms* on page 18.
2. Select the event that you want to view history for.
3. Click **History** to view history for the selected event.  
The Monitor Screen - History Window will display.
4. View the history details.
5. Close the window to return to the Monitor Alarms page.

## Change Alarms List Settings

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

1. Click  **Monitor > Alarms** to access the Monitor Alarms page. For more information see *Monitoring Alarms* on page 18.  
The list displays in date order, with the most recent events at the top of the list.
2. If you want to re-sort the order of the list:
  - Click in the heading of the column to sort by (e.g. Priority). The list will sort in ascending order based on that column (e.g. ascending order of priority).
  - To change the sort order to descending, click the column heading again.
3. If you want to re-sort the order of the columns, click on the column you want to move then drag and drop this to it's new location.
4. If you want to add or remove columns, click **Select Columns** and do the following:
  - Click beside the Column name of any columns to be added so that a check mark displays.
  - Click beside the Column name of any column to be deleted so that a check mark no longer displays.
5. If you want to change the sound settings:
  - If the sound is on, click **Sound Off** to turn the sound off.
  - If the sound is off, click **Sound On** to turn the sound on.
6. Click **Save Settings** if you want to save the new settings.  
A message box displays with the message 'ACM Notification. Successfully saved.'

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

## Turning Sound On/Off

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

To turn the sound off:

- On the Alarms page, click the **Sound Off** button.  
The sound is muted and the **Sound On** button appears.

To turn the sound on:

- On the Alarms page, click the **Sound On** button.  
The sound is audible and the **Sound Off** button appears.

# Using the Verification page


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

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

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

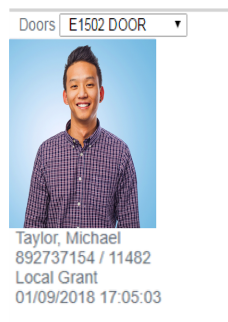
- At the top of the page are four door panes that allow you to select and monitor four doors at a time. After you select a door to a pane, you can monitor live event transactions as they occur at that door.
- Underneath the door panes is a list of live door transactions displayed like the Events page.  
Not all door events will display in this list. Only events in the priority number range 300 to 700 display. A full listing of all events is available on the Monitor Events page.

## Verifying Identities at Doors

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

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

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



If the person:

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

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

## Verification Events List

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



1. Click  **Monitor > Verification**. The Verification page displays.


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

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

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

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

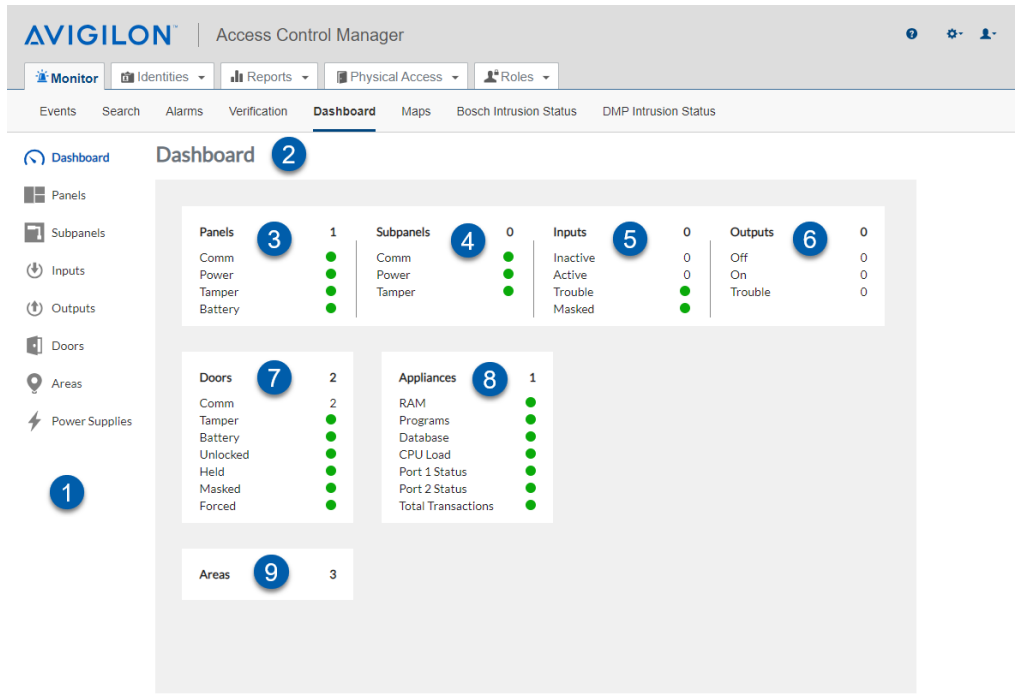
**Note:** Saving the settings only saves the column configuration. The doors selected for verification will need to be selected each time you return to the page.









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

# Using the Dashboard

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

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







Area	Description
1	<div>Dashboard Sidebar</div> <div>Navigation menu for the  Dashboard,  Panels table,  Subpanels table,  Inputs table,  Outputs table,  Doors table,  Areas table, and  Power Supplies table ( if a LifeSafety power supply is connected).</div> <div>From the Panels table, you can access a list of subpanels in the Subpanels table. From the Subpanels table, you can access a list of inputs and outputs in the Inputs and Outputs tables.</div> <div>From the Inputs and Outputs tables, you can directly access the list of inputs and outputs.</div> <div>From the Doors table, you can control individual doors, investigate doors with active faults, and see more information about the state of individual doors.</div> <div>From the Areas table, you can view the details, including current identities, for each area.</div>

	Area	Description
2	Dashboard	<p>Displays a summary of hardware faults or unexpected input and output state changes as they occur. As the status of hardware components changes, the status indicators on the Dashboard change color. For more information, see <i>Status Colors</i> below.</p> <p>The total number of connected hardware components (installed and uninstalled) is displayed above a real-time fault or status list. For panels, subpanels, inputs and doors, the number of installed components in each fault state is displayed. If no faults occur, their status is green. For outputs, the numbers indicate the number of installed outputs in each state. When no components are displayed in a state, the status is either green or 0.</p>
3	Panels	Displays a summary of the fault state of the installed panels. Click the number next to the fault to drill down to the details of the fault in the Panels table, which is filtered to display only the panels with that fault.
4	Subpanels	Displays a summary of the fault state of the installed subpanels. Click the number next to the fault to drill down to the details of the fault in the Subpanels table, which is filtered to display only subpanels with that fault.
5	Inputs	Displays the total number of inputs in each state. Click the number next to the state to drill down to the Inputs table, which is filtered to display only inputs with that state.
6	Outputs	Displays the total number outputs in each state. Click the number next to the state to drill down to the Outputs table, which is filtered to display only inputs with that state.
7	Doors	Displays the summary of the fault state of the installed doors. Click the number next to the fault to drill down to the Doors table, which is filtered to display only alarms with that fault.
8	Appliances	When no issues occur in the ACM appliance items, their status is green. Hover the mouse over each status indicator to see more details. For example, "RAM free 45%" displays for the RAM status.
9	Areas	Indicates the number of defined areas.




## Status Colors

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

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

## Appliance Transactions Indicators

The status colors represent the following appliance states:

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

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

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

## Device Status












Panels, Subpanels, Inputs, Outputs and Doors only.

To see the legend for device status:

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

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


battery statuses apply to Control locks.


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

## Security Status



To see the legend for device status:

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

Icon	Status	Description
	TLS Required	The panel is configured to use Transport Layer Security (TLS) protocol to secure communication with the ACM appliance.

Icon	Status	Description
	TLS & Certificate Required	The panel is configured to use TLS protocol and a certificate to secure communication with the ACM appliance.

## Controlling Doors

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

Doors can also be controlled from  **Monitor > Maps**. For more information, see *Using a Map* on page 33.

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

1. Select the checkbox for each the door you want to control.  
Or click **All** at the top of the left column to select all doors or **None** to deselect all doors.
2. For one or more doors, select a **Door Action** if required:

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

- **Grant** — Momentarily grants access to the door to permit a single-time entry.
- **Restore** — Restores the Door Mode to its default configuration or Custom Mode.  
*Schlage locks with activated lock functions only.* Restoring a door that has an activated Lock Function (Classroom, Office, Privacy, or Apartment) removes the Lock Function and resets the door mode to its default configuration.  
*For ASSA ABLOY IP doors only.* Restoring a door results in the door going offline temporarily in the ACM system.
- **Unlock** — Unlocks the door. The door remains unlocked until the **Locked No Access** command is issued or until an operator override or scheduled action is initiated.
- **Locked No Access** — Locks the door. The door remains locked until the **Restore** command is initiated or until an operator override or scheduled action is initiated.
- **Disable** — Disables the door. The door stops operating and allows no access to anyone.
- **Lock (ASSA ABLOY Only)** — *For ASSA ABLOY IP doors only.* Locks the door. The door remains locked until a scheduled action is initiated.

3. Select any of the following **Door Mode** options to change the door mode.  
For more information, see *Door Modes* on the next page.

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

## Door Modes

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

For Mercury Security and HID VertX panels. The same list of options is provided for the Offline Door Mode option.


For ASSA ABLOY IP-enabled doors, SALTO standalone doors and Schlage offline Wi-Fi doors. Any locks that do not support real-time communication with a server, will not display door mode options on the Doors list page and maps. Door mode can be set on the Door: Edit page and by using a batch job (specification).

Door Mode	Description
<b>Disabled</b>	The door is disabled for all access.
<b>Unlocked</b>	The door is always unlocked.
<b>Locked No Access</b>	The door is always locked. No access is allowed through this system.
<b>Locked No Access (Unlocked on Next Exit)</b>	The door is locked until a person presses the push bar to exit.
<b>Facility Code Only</b>	<p>The door can be accessed using a facility code.</p> <p>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.</p> <p><i>Mercury door only.</i> The Offline Door Mode is no longer supported if the door controller is connected to an LP4502 panel that has replaced an HID VertX panel.</p>
<b>Card Only</b>	<p>The door can be accessed using a card. No PIN is required. To support the selected <b>Assurance Profile</b> for a pivCLASS configured door, it is recommended to set the Door Mode to <b>Card Only</b>.</p> <p><i>Mercury door only.</i> The type of reader used to read this card is determined in the Reader Type field.</p>

Door Mode	Description
<b>Pin Only</b>	<p>The door can only be accessed by entering a PIN at a keypad.</p> <p>No card is required.</p> <div> <b>Note:</b> This door mode is not available if the 'Allow duplicate PINs' option has been selected on the System Settings - General page. </div>
<b>Card and Pin</b>	<p>The door can only be accessed using both a card and a PIN.</p> <p><i>ASSA ABLOY IP door only.</i> If the token does not have a PIN, the door can be accessed by swiping the card only.</p>
<b>Card or Pin</b>	<p>The door can be accessed either by entering a PIN at a keypad or by using a card at the card reader.</p> <div> <b>Note:</b> This door mode is not available if the 'Allow duplicate PINs' option has been selected on the System Settings - General page. </div>
<b>Office</b>	<p><i>SALTO door only.</i> The lock allows the cardholder to leave the lock open.</p> <p>To use this mode, the cardholder presents the key to the door while pressing down the inner handle and repeats the procedure to undo the mode.</p>
<b>Toggle</b>	<p><i>SALTO door only.</i> The door allows the cardholder to toggle between leaving the lock open and closing it by presenting the assigned key (there is no need to press down the inner handle).</p> <p>To use this mode, the cardholder presents the key to leave the lock open and repeats the procedure to close it.</p>
<b>Keypad Only</b>	<p><i>SALTO door only.</i> The door can only be accessed by entering the shared keypad code at a keypad. If selected, Keypad Code is displayed. You can enter up to 8 digits.</p>
<b>First Person Through</b>	<p><i>ASSA ABLOY battery-powered or external-powered door only.</i> The first person who is granted access to the door will unlock the lock.</p>
<b>Exit Leaves Open</b>	<p><i>SALTO door (not connected to control unit) only.</i> The door is unlocked when the inner door handle is pressed. Allows the cardholder to exit and return to the building without using an assigned key during an emergency (referred to as Escape and Return mode).</p> <p>To lock the door, add a global action to set a time limit on the open door.</p>
<b>Toggle and Exit Leaves Open</b>	<p><i>SALTO door (not connected to control unit) only.</i> The door allows the cardholder to use either the Toggle or Exit Leaves Open door mode during an emergency (referred to as Escape and Return mode).</p>






# Using Map Templates

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

## Adding Maps




Follow the steps below to add maps.

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

## Using a Map

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


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

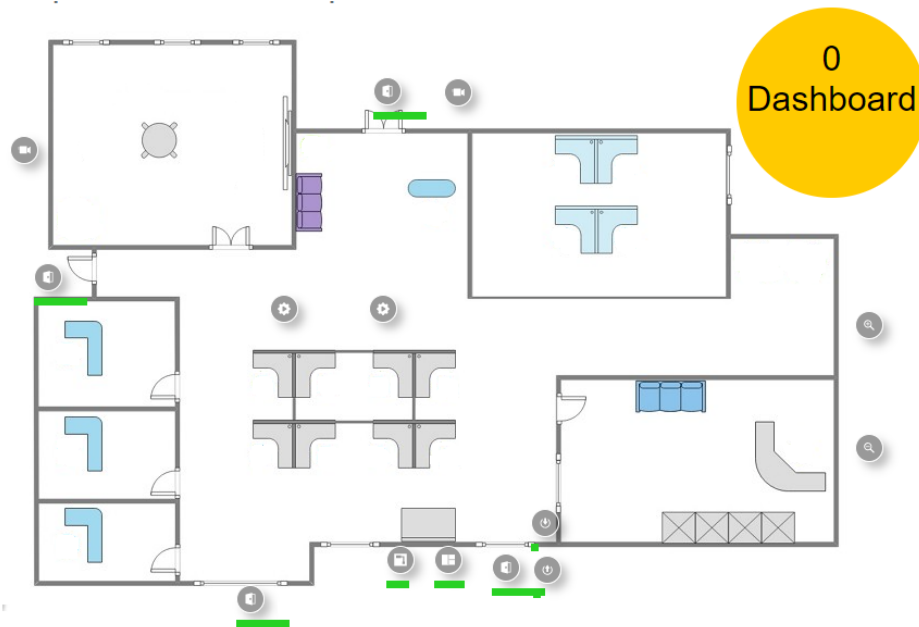
**Note:** Unlike the  **Physical Access** > **Doors** or  **Monitor** > **Dashboard** page which displays all modes and commands regardless of door type, the  **Monitor** > **Maps** page displays only the modes and commands that are supported by your door or device.

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










## Viewing a Map

To access and monitor your site from a map:

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








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

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

## Hardware Status

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




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






## Map Actions

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

To...	Do this...
Review hardware status	<p>The colored bar below each item displays an overview of the current communication and power status.</p> <ul style="list-style-type: none"> <li>Click the icon on the map to display the control menu.</li> </ul> <p>For more information about the colored hardware status bar, see the specific hardware status page. For more information about the status colors, see <i>Status Colors</i> on page 27.</p>
Review an alarm	<p>If you see a red alarm indicator, the item on the map is in an alarm state.</p> <ul style="list-style-type: none"> <li>Click the alarm indicator to see the status details.</li> </ul> <p>For more information about alarm actions, see <i>Monitoring Alarms</i> on page 18.</p>
Modify or delete an override	<p>If you see solid blue disk indicator, an active override is in effect on the door. If you see a hollow blue disk indicator, an inactive override is defined.</p> <ul style="list-style-type: none"> <li>Click the indicator to open the Doors: Overrides page to see details.</li> </ul>
Respond to a priority situation	<p>If you see a red bounding box around the status indicator, the door is in Priority Mode.</p>

**Important:** A door is in Priority Mode when a priority situation has been declared at your site. All doors affected by the situation are placed into Priority Mode and only the Priority ACM Operator, responsible for dealing with priority situations can interact with the door.

To...	Do this...
Control a door	<p>Click  on the map to display the control menu for the selected door.</p> <div style="border: 1px solid #f0e68c; padding: 10px; margin: 10px 0;"> <p><b>Note:</b> Fields in this list are dependent on the door or device. Some commands or fields are not supported for all doors or devices.</p> </div> <p>Use the menu options to set the Door Mode. For more information, see <i>Door Modes</i> on page 31.</p> <p>Use the following menu options to mask or unmask alarms:</p> <ul style="list-style-type: none"> <li>• <b>Mask Held</b> — Mask the Door Held Open Alarm.</li> <li>• <b>Unmask Held</b> — Unmask the Door Held Open Alarm.</li> <li>• <b>Mask Forced</b> — Mask the Door Forced Open Alarm.</li> <li>• <b>Unmask Forced</b> — Unmask the Door Forced Open Alarm.</li> </ul> <p>To view live video, recorded video, notes, instructions, identities, and history click <b>Trace</b> to display the event transactions for the door.</p> <p>To hide the control menu, click the icon again.</p>
Control a panel or subpanel	<p>Click  or  on the map to display the panel control menu, and then for the panel or subpanel use these options:</p> <ul style="list-style-type: none"> <li>• Panels <ul style="list-style-type: none"> <li>◦ <b>Download Params</b> — Download the latest system configurations to the panel.</li> <li>◦ <b>Tokens</b> — Download the tokens to the panel.</li> <li>◦ <b>Reset/Download</b> — Reset and download the current system configuration to the panel.</li> <li>◦ <b>APB Reset</b> — Resets all panel and area counts to zero.</li> <li>◦ <b>Clock</b> — Re-sync the panel time.</li> <li>◦ <b>Trace</b> — Display the event transactions for the panel.</li> </ul> <div style="border: 1px solid #f0e68c; padding: 10px; margin: 10px 0;"> <p><b>Note:</b> This is the only option supported for ASSA ABLOY IP panels.</p> </div> </li> <li>• Subpanels <ul style="list-style-type: none"> <li>◦ <b>Trace</b> — Display the event transactions for the subpanel.</li> </ul> </li> </ul> <p>Viewing live video, recorded video, notes, instructions, identities, and history can be performed on the event transactions.</p> <p>To hide the control menu, click the icon again.</p>

To...	Do this...
Control an input	<p>Click the  on the map to display the input control menu for the input.</p> <p>Use these options to mask or unmask the input:</p> <ul style="list-style-type: none"> <li>• <b>Mask</b> — Mask the input.</li> <li>• <b>Unmask</b> — Unmask the input.</li> </ul> <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 for the output.</p> <p>Use these options to initiate output actions:</p> <ul style="list-style-type: none"> <li>• <b>On</b> — Activate the output.</li> <li>• <b>Off</b> — Deactivate the output.</li> <li>• <b>Pulse</b> — Pulse the output.</li> </ul> <p>To hide the control menu, click the icon again.</p>
Display video	<p>Click the  on the map to display the <b>Camera Video</b> window.</p>
Open a linked map	<p>Click  to display a linked map, or  to display a linked map.</p>
Monitor the dashboard	<p>If there is a Mustering dashboard configured on the map, it may appear as a line of text or as a shape with text inside.</p> <p>The dashboard displays the number of identities in the area and may include the name of the area. In <i>Using a Map</i> on page 33, the dashboard is the gray square.</p> <p>Click the dashboard to see a list of all the identities that are in the area. Click outside the pop-up dialog to hide the identities list. Click the First Name or Last Name to view the identity.</p>


# Monitoring Bosch Intrusion Panels

The following procedures relate to monitoring Bosch intrusion panels.

## Monitor Bosch Intrusion Panel Status

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

To monitor intrusion panel status:

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

The following statuses display for panels:

- Communications
- Battery
- Power
- Tamper
- Phone Line

The following statuses apply to all of the above:



Online





Alarm




Trouble

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


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

## Monitoring Areas in Bosch Intrusion Systems

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

### Viewing Areas

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

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

A status is displayed for each area.

-  Armed
-  Ready to Arm
-  Not Ready to Arm
-  Partial Arm
-  Trouble
-  Alarm

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

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

## Arming Areas

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

## Arming Perimeter Areas

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

## Disarming Areas

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

## Silencing Keypad Alarms

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

## Clearing Alarms

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

## Resetting Sensors


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

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

## Monitor Bosch Intrusion Panel Points

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

To monitor intrusion panel point status:

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

The following statuses apply to all of the above:



Normal



Faulted





Bypassed



Trouble

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

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









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


## Monitor Bosch Intrusion Panel Outputs

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


To monitor intrusion panel outputs status:


1. Select  **Monitor** > **Bosch Intrusion Status**.
2. Click the **Outputs** tab.
3. View the list that displays. A status is displayed for each output - the available statuses are:
  -  Inactive
  -  Active
  -  Trouble
4. If you want to narrow the list that displays, either:
  - Use the filter function. Enter an output name to filter the list results by output. Type in the name (or part of the name) of the output, or panel and the list will update as you type.
  - Select a single status (e.g. Active) to view.
5. If you want to sort the list, click  to sort in ascending order, or  to sort in descending order in each column.
6. If you want to activate or deactivate an output:
  - Select the outputs in the list, and
  - Click either the **Activate** or **Deactivate** button.

## Monitoring and Controlling DMP Intrusion Systems

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

### Viewing Panels, Areas, Zones and Outputs

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

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

<input checked="" type="checkbox"/> <b>Normal</b>	Online and working. Examples: Area is armed. Zone is in the expected state.
<input checked="" type="checkbox"/> <b>Warning</b>	Warning condition. Examples: Area is disarmed. Zone is bypassed.
<input checked="" type="checkbox"/> <b>Critical</b>	Critical condition. Examples: Area is armed with alarm. Zone is in not in the expected state or in alarm state.
<input checked="" type="checkbox"/> <b>Unknown</b>	Unknown condition.

- Panels tab only. View the connection status.

<b>Encryption Fails</b>	Encrypted connection or remote key failed.
<b>Incompatible</b>	DMP firmware version is not supported.
<b>Offline</b>	Panel is not connected.
<b>Online</b>	Panel is online.

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

- Click the column heading to sort the lists.

## Silencing Keypad Alarms on Panels

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

## Resetting Sensors on Panels

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

## Arming or Disarming Areas

1. Click the **Areas** tab.
2. To arm an area:
  - a. Select one or more areas in **Disarmed** status.  
To select all items, click the first column heading.
  - b. In **Bad Zone Action**, select the action for a zone in an area that might not be in the expected condition at the time of arming.

- **Bypass:** All bad zones are bypassed.
  - **Force:** All bad zones are force armed.
  - **Refuse:** No zones are armed until the zone is restored.
- c. Click **Arm**.  
The area is Armed.
3. To disarm an area:
    - a. Select one or more areas in **Armed** status.  
To select all items, click the first column heading.
    - b. Click **Disarm**.  
The area is Disarmed.

## Bypassing Zones and Resetting Bypassed Zones

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

## Activating and Deactivating Outputs

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

# Identities

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

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

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

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

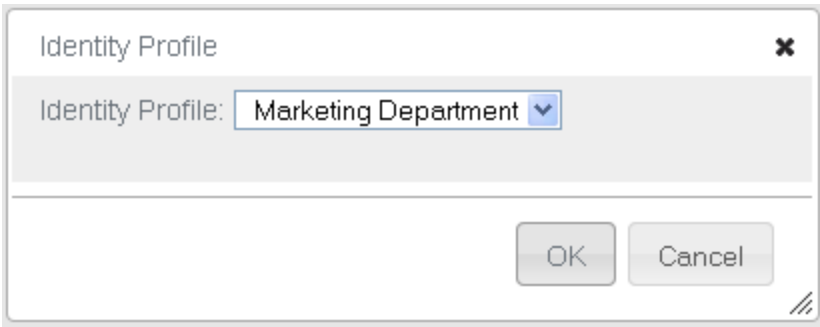
## Adding an Identity

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

To add a new identity:

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


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

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


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

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

4. Click  **Save**.

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

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

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

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

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

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

When you are finished, click .

7. Optional: Add notes about the identity and review previous notes, if any.  
8. Add more details about the identity on the following tabs:

- **Roles:** Assigns a role to this identity.
- **Tokens :** Creates a token for the identity.
- **Groups:** Assigns the identity to a group.
- **Capture:** Takes a photo of the user.
- **Photos:** Uploads an existing photo of the user.
- **Badge:** Assigns a badge to the user.
- **Timed Access:** Assigns timed access to the user.
- **Access:** View the identity's access privileges including roles, access groups and doors.
- **Transactions:** View transactional data associated with the identity.
- **Audit:** View a log of all the changes that have been made to this identity.




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

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

## Assigning Roles to Identities

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

To assign roles to an identity:

1. Click  **Identities**.
  2. From the Identities Search page, perform a search for an identity.  
For more information, see *Searching for an Identity* on page 52.
  3. Click on the name of the identity you want to edit.
  4. Select the **Roles** tab.
  5. From the Available list, select all the roles that you want to assign to the user, then click .  
The role is added to the Members list to show that it is now assigned.
- To remove a role from the user, select the role from the Members list, then click .

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


6. Click  **Save**.

## Assigning Tokens to Identities




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

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

To create tokens and assign them to an identity:

1. Select  **Identities** > **Identities**.
2. Search for an identity.  
For more information, see *Searching for an Identity* on page 52.
3. Click the name of the identity you want to edit.
4. Select the **Tokens** tab.
5. If only one token has been defined, the Token: Edit page appears.  
If more than one token has been defined, the Tokens list appears. Click **Add Token**.
6. Enter the details as required.



**Note:** If you are assigning HID Origo tokens, see *Enrolling Identities and Issuing HID Origo Tokens* on page 54.


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

# Assigning Groups to Identities

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

To assign groups to an identity:

1. Click  **Identities**.
2. From the Identities Search page, perform a search for an identity.  
For more information, see *Searching for an Identity* on page 52.
3. Click on the name of the identity you want to edit.
4. Select the **Groups** tab.
5. From the Available list, select all the groups that you want to add the user to, then click  .  
The group is added to the Members list to show that the user is now a member.

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

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

6. Click  **Save**.

## Capturing and Uploading Photos of an Identity

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

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

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

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

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

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

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


Before you can:

- Use a camera to capture photos, you must specify the badge camera you want to use in your user profile. For more information, see *External Systems - Defining the Badge Camera for the System* on page 64.
- Generate and print a badge, at least one badge template must be defined in your system.

After a photo has been added to the **Photos** tab of an identity, you can edit the photo to suit the requirements of your badge templates. Then you can create a badge with that photo. For more information, see *Creating Badges for Identities* on page 51.

### Capturing a photo

1. There are two ways to access the Capture page:

- From the Identities Search page, click  from the **Image Capture** column.
- From the Identities Search page, click on the name of an identity, select the **Photos** tab, then click **Capture a Photo**.

2. If you are using:

- a. A local camera that you have not used before, this page will not appear unless you allow your web browser to access your camera. The first time you access the Capture page, you are prompted to allow your browser to access your local camera. Click **Allow**.
- b. An IP-based camera and the camera requires authentication, this page will not appear until you have entered your login credentials.

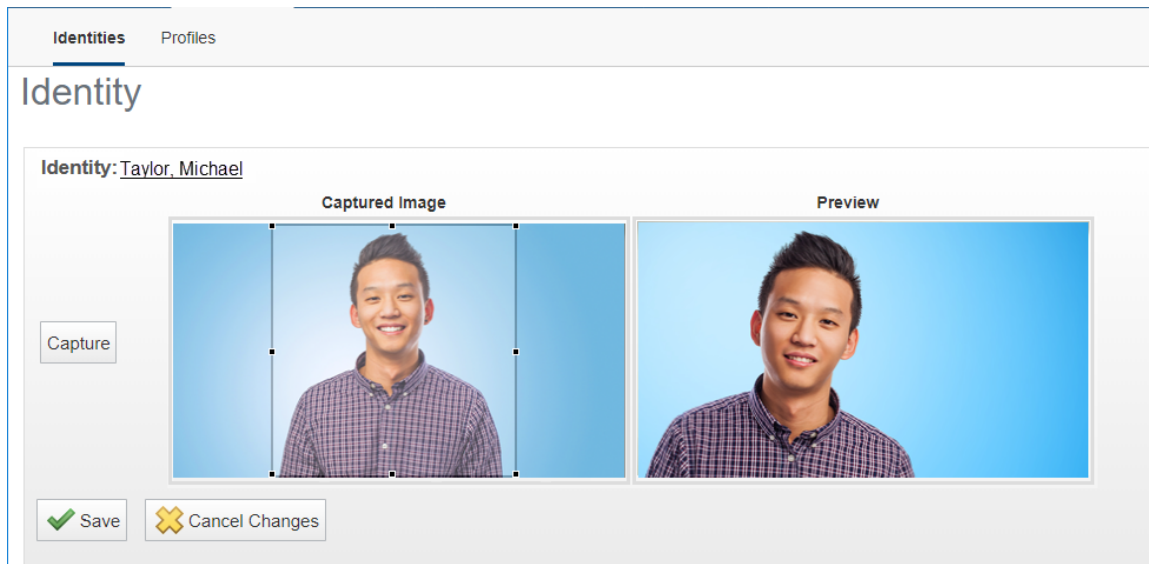
Enter a user name and password, then click **OK**.

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





3. Click **Capture**.

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


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






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

### Uploading a photo

1. From the Identities Search page, click on the name of an identity, select the **Photos** tab, then click **Upload a Photo**.  
The screen expands to include more fields.
2. Click **Choose File** and navigate the directory to find the photo you want to upload.  
Click **Open** to select the photo. You can upload files in JPG, PNG, or GIF format.
3. On the **Photos** tab, click the **Primary** checkbox if you want this photo to appear on this person's Identity page and access badge. If no primary photo is selected, the first photo on the list is used.
4. Click  **Save**.

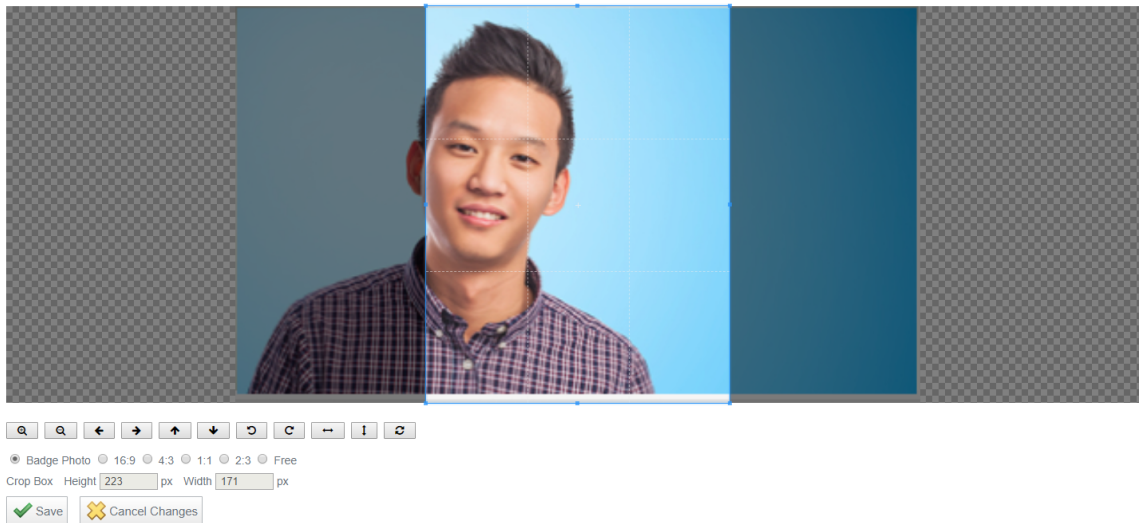
### Editing a photo

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

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

Use the mouse in combination with the control buttons under the photo to crop, resize, rotate and flip the photo. You cannot edit the actual photo, or change its resolution by zooming in and out. The dimensions shown in the Crop Box options are read-only and cannot be entered directly, but are dynamically updated as you manipulate the cropping overlay with the mouse.

## Photo Edit



### 1. Adjust the overlay.

- To reposition the overlay over the photo:
  - a. Click inside the cropping overlay.
  - b. Drag the mouse to move the overlay.
- To resize the overlay
  - a. Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay can be resized.
  - b. Resize the overlay. The selected aspect ratio (usually the Badge Photo aspect ratio) is retained.
- To change to a different aspect ratio:  
Click to select the required aspect ratio.
- To resize the overlay freely:
  - a. Click **Free**.
  - b. Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay will be resized.
  - c. Drag the mouse to resize the overlay. The overlay will be resized only in the direction of the cursor.
- To rotate the overlay:
  - a. Click outside the current overlay.
  - b. Drag the mouse to draw a new overlay.
- To replace the overlay:
  - a. Click outside the current overlay.
  - b. Drag the mouse to draw a new overlay.

### 2. Adjust the photo.

- To enlarge or reduce the photo:  
Use the + and - magnifier control buttons to adjust the photo size in stepped increments.
- To reposition the photo:  
Use the up, down, left and right control buttons to adjust the photo position in stepped increments.

- To rotate the photo:
  - a. Use the counterclockwise circular arrow to rotate the photo to the left by 90°.
  - b. Use the clockwise circular arrow to rotate the photo to the right by 90°.
- To flip the photo:
  - a. Use the horizontal double-ended control button to flip the photo left to right.
  - b. Use the vertical double-ended control button to flip the photo top to bottom.
- To reset the photo:  
Use the reset control button to cancel your changes and revert the photo to its previously saved version.

### 3. Save the photo:

Click  **Save.**

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

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


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

### Specifying the Primary photo

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

### Deleting a photo

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



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

## Creating Badges for Identities

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

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

To create a badge for a user:

1. Click  **Identities**.
2. From the **Identities** list, click on the name of the identity you want to edit.
3. Select the **Badge** tab.
4. From the **Badge Photo** drop down list, select a photo for this badge.  
Only the photos that have been previously uploaded or captured for this identity appear in this list.
5. From the **Badge Token** drop down list, select the token you want to associate with this badge.  
Only the tokens that have been previously defined for this user appear in this list.
6. From the **Badge Template** drop down list, select the badge template that you want to use for this badge.  
Only the badge templates that have been previously defined appear in this list.
7. Click  **Save**.
8. To print the badge, click **Create Badge**.  
The badge appears in a preview window.
9. Click **Print**.

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

## Searching for an Identity

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

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

Blank entries will return all identities.

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

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

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

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


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

The page displays your search results.

## Editing an Identity

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


To edit an existing identity:

1. Click  **Identities**.
2. Search on the Identity Search screen, then click on the identity you want to edit.
3. Optional: Add notes about the identity and review previous notes, if any.
4. Navigate through the tabbed pages and make the required changes.
  - **Identity:** The identity details.

The default Enrollment Operator role cannot edit this page. Contact your System Administrator for more details.
  - **Roles:** Assigns a role to this identity.
  - **Tokens :** Creates a token for the identity.
  - **Groups:** Assigns the identity to a group.
  - **Capture:** Takes a photo of the user.
  - **Photos:** Uploads an existing photo of the user.
  - **Badge:** Assigns a badge to the user.
  - **Timed Access:** Assigns timed access to the user.
  - **Access:** View the identity's access privileges including roles, access groups and doors.
  - **Transactions:** View transactional data associated with the identity.
  - **Audit:** View a log of all the changes that have been made to this identity.

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

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

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


# Enrolling Identities and Issuing HID Origo Tokens

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

To enroll an identity and issue an HID Origo token:


1. Select  **Identities > Identities** and click **Search** to select an identity already created.
2. Click the **Tokens** tab and enter:

<b>Token Type</b>	HID Origo
<b>Mobile ID Type</b>	The mobile ID to be issued to the registered device.


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

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

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


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

<b>Token Type</b>	HID Origo
<b>Mobile ID Type</b>	The HID mobile card that is not already issued to the device.

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


## Registering a New Mobile Device for an Enrolled Identity

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

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

## Searching for HID Origo Tokens

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

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

## Setting Up Multi-Factor Authentication

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

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

### Add Your MFA Devices

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


Contact your ACM administrator for permission to manage MFA devices.

#### Add MFA Device

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

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


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

3. Enter your current password in **Password**.
4. Click **Next**. A QR code is generated.
5. Follow the instructions to set up the app and scan the QR code using your mobile device.  
If your mobile device cannot scan or you are using a desktop app, click **Can't scan?** to display the contents of the QR code. Go to your app and type the code.
6. In **Name your device**, enter a name and click **Next**.
7. Enter the six-digit code generated by the app and click  **Verify**. The device is added.



Next, see *Logging In* on the next page.

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

## Delete MFA Device

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


## Disable MFA

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

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

## Logging In

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

1. Open your preferred browser.
2. In the address bar, enter the IP address of your ACM appliance.
3. Enter your username in the **Login** field.  
If enabled, enter also your remote login account in **Remote Login**. Enter the login name in this format: *username@domain.org*.
4. Enter your password in the **Password** field.
5. Click the **Sign in** button.  
If enabled, select the MFA device in **Device**. Enter the six-digit code generated by your authenticator app and click  **Verify**.

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

If prompted to change your password, enter the **Old Password** and new password in **Password**. Click **Save**.

6. The application's Home page is displayed.

**Tip:** To change your password after initial installation, see *Changing the Password in My Account* on page 64.





# Reports

The Reports screen allows you to create, edit, preview, and generate reports. Reports are used to gather information from the system in either a PDF or Spreadsheet. Reports can be saved on your local computer and referred to offline. For example, the Identity/Doors with Access Report can be used to view which doors each identity has access to. You have the option of using the default system reports or customizing the reports to fit your needs.

Monitoring Supervisors are responsible for creating, editing, and generating reports when required.



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

## Generating Reports

Anytime you see  **PDF** or  **Spreadsheet**, you can generate and save a copy of the current report.

You can generate a copy of reports from the Reports list, the Report Edit page or from the Report Preview page.


Generated reports will only show the filtered information that is displayed. To edit the report before you generate it, see *Editing Reports* on the next page.

- Click  to save the current report as a PDF file.
- Click  to save the current report as a CSV format spreadsheet.

Most generated reports saved as PDF files contain a maximum of 2,000 records, except the Audit Log Report, which contains a maximum of 1,000 records. Reports saved as CSV format spreadsheet files contain a maximum of 2,000 records.

Depending on your web browser, the file may be auto-downloaded or you will be prompted to save the file to your local computer.




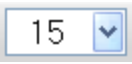





## Report Preview

When you click the name of a report from the Reports list and select , a preview of the selected report is displayed.

In the preview, you can check the report to see if the report gives you the information you need, search the report, or generate the report. For example, if you wanted to know the role of an identity, you can preview the Identity Summary report and search for the specific identity.

You can use the following options to control what is displayed:

**Tip:** Click  to filter the report. The preview bar expands to display search criteria.

Feature	Description
<b>Generate Report</b>	
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.
<b>Preview Bar</b>	
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 report. <ul style="list-style-type: none"> <li>Click <b>Search</b> to perform a search using the selected filter options.</li> <li>Click <b>Reset</b> to clear the report filter options.</li> <li>In the drop down list beside the Reset button, choose if the search will locate <b>all</b> or <b>any</b> transactions that match the selected report filters.</li> <li>Click <b>Save</b> to save and apply the selected filters to the default report.</li> </ul>
	Select the number of items you want to display on a single page.
	Click this button to return to the first page of the report.
	Click this button to return to the previous page of the report.
Page <input type="text" value="1"/> of 1	Enter the page you want to go to.
	Click this button to bring up the next page of the report.
	Click this button to go to the last page of the report.
	Click this button to refresh the report.

## Editing Reports




All reports can be edited or filtered to only display the information that you need. You can edit default system reports and custom reports in the same way.


If you plan to use the filtered report frequently, you can create a custom report rather than modify the default system report every time. For more information see *Creating Custom Reports* on page 60.


Most generated reports saved as PDF files contain a maximum of 2,000 records, except the Audit Log

Report, which contains a maximum of 1,000 records. Reports saved as CSV format spreadsheet files contain a maximum of 2,000 records.

Reports requiring more than 2,000 rows must be scheduled as a batch job for system performance. For more information, see *Generating a Batch Report* on page 65.

1. Display the Reports list.
  - To display the system reports page, click  **Reports**.
  - To display the custom reports page, select  **Reports > Custom Reports**.
2. Click  for your report.

**Note:** The Audit Log Report and Transaction Report do not have  available. To edit, click on the report name and follow the steps in the related procedure - *Editing Audit Log and Transaction Reports* below.


3. Edit the report criteria.
4. Click  to save your changes.

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

## Editing Audit Log and Transaction Reports





The Audit Log and Transaction Reports are edited differently from other reports. There is no edit function directly available from the Reports list.

Follow the steps below to edit these reports.

1. Display the Reports list.
  - To display the system reports page, click **Reports**.
  - To display the custom reports page, select **Reports > Custom Reports**.
2. Click on the name of the report.
3. Click  in the bottom left-hand corner on the following page (either the Grid: Transaction Report or Grid: Audit Log page).  
The Find section opens.
4. Do the following to define criteria for the report:
  - Select an option in the search type field (e.g. External System ID).
  - Select an option in the search operator field (e.g. greater or equal to).
  - Select an option in the search value field (e.g 12/07/2015 00:00:00).

The **Full Name** search type field available for the Transaction Report returns results for a limited number of combinations of search operator and search value entries. For example, using an identity with the name John Smith, the following searches will succeed:




Search Operator	Search Value
contains	Smith, John
	John
	Smith
equal	Smith, John
begins with	Smith
ends with	John

- Click  to add more search fields, if required.  
Complete step 4 above for each additional field added.
- Click  **Save** to save your changes.  
The ACM Notification message displays with the message 'Search Parameters successfully changed'.
- To save these filter settings as a custom report, enter a name in the Create Custom Report: field , then click  **Create Custom Report:**.
- To reset the search criteria, click  **Reset**.

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

## Creating Custom Reports

A custom report is a system report that has been duplicated and edited to meet your requirements. You can create a custom report that are used frequently.

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

See *Scheduling a Custom Report By Batch Job (Specification)* below.

## Scheduling a Custom Report By Batch Job (Specification)

To schedule the creation of a custom report by batch job:

1. Select  **Reports > Custom Reports.**

2. Click the **Schedule** link next to the report name.

3. Create the schedule:

a. In the Job Specification window with the report information, enter:

<b>Name</b>	The name of the schedule.
<b>Output Format</b>	<b>pdf</b> (default) or <b>csv</b> .

b. Click **Next**.

The current values of the report cannot be edited here. If you need to edit, go to the Custom Reports tab and click  Edit.

c. Enter the schedule:

<b>Repeat</b>	<b>Once, Hourly, Daily, Weekly</b> or <b>Monthly</b> . (The page refreshes depending on your selection.) For Weekly: Any of the <b>Sun, Mon, Tue, Wed, Thu, Fri, Sat</b> checkboxes. For Monthly: The date.
<b>On</b>	The time in 24-hour clock format in <b>HH</b> (hour, such as 20) and <b>MM</b> (minute, such as 00). For Once: Click the field to select the date from the calendar. Then adjust the hour, minute and second selectors to set the time.

d. Click **Next**.

e. Optional. Enter a checkmark in **Send Email** and the email address.

If an email is not specified, go to the **Batch Jobs** tab to retrieve the report on the appliance (after the job specification completes).

a. Click **Submit**. The schedule is created.

4. Create the batch job to run the custom report on schedule:

a. Select  **> My Account.**

b. Click the **Job Specification** tab.

c. Select the schedule and click  **Activate/Deactivate.**





The **Activated on** date is displayed in the right-most column.

5. To view the reports generated by the batch job, click the **Batch Jobs** tab. The reports stay in the list until manually deleted.

To remove a report, select the row and click .

## Creating Custom Audit Log and Transaction Reports

A custom audit log report lists all the selected recorded system logs. You can create a custom audit log report to report only a selection of required audit logs. A custom transaction report lists all the selected recorded system transactions. You can create a custom transaction report to report only a selection of required system transactions.

1. Click  **Reports**.
2. Click **Transaction Report** in the Report Name column.
3. Click  at the bottom of the page. The preview bar expands to display search criteria.
4. Enter the details you want to include in the report in the Find section. (Click  to add more fields.)
5. Click **Search**.  
The system transactions are filtered into a report.
6. In the **Create Custom Report** field, enter a name for the report.
7. Click  **Create Custom Report** to save the new report.




## Identity Correlation Report

The ACM Identity Correlation Report lists all identities that have attempted to access the same door, but not all doors, in the building on a particular date and time range.

### Example uses

- Support tracing of the identities suspected of exposure to contaminated door surfaces (referred to as 'correlated identities') by an infected origin (referred to as the 'origin identity').
- Support tracing of the identities suspected of burglary attempts at the door.


### Generating the report

1. Select  **Reports > Reports**.
2. Click **Identity Correlation Report**.
3. Follow the required steps in the ACM notification popup to produce a refined list of correlated identities for investigation and avoid search performance issues.
4. Click  and  to add items to **Find** including the date, identity name or token number, and time range:



<b>Origin Panel Date</b>	The date when the origin identity accessed the door panel.
<b>Origin Last Name</b>	The last name of the origin identity.
<b>Origin First Name</b>	The first name of the origin identity.
<b>Origin Card Number</b>	The token number of the origin identity.
<b>Time Range: max minutes before</b>	The time frame of door access by correlated identities before origin identity access.
<b>Time Range: max minutes after</b>	The time frame of door access by correlated identities after origin identity access.

5.  Save the search.


### Generating a report for other identity correlations

1. Change the identity name or token number.
2. Click  **Search** again.

## Exporting the report to a spreadsheet

1.  Save the search. The last saved filter is used.
2. Click  above the search results.



# Setting Personal Preferences

To set up your personal preferences, select  > **My Account** from the top-right. Navigate through the tabbed pages and edit the details as required. The tabbed pages include:

- **Profile:** use this page to edit your account details and preferences.
- **Batch Jobs:** use this page to view the batch jobs that have been run from your account.
- **Job Specification:** use this page to add, edit, activate/ deactivate, or delete batch jobs.



## Changing the Password in My Account

While you are logged in to the ACM system, you can choose to change your password any time.

1. In the top-right, select  > **My Account**.
2. On the Profile tab, enter your current password in **Old Password**.
3. In **Password**, enter your new password.  
As you enter your new password, the status bar underneath will tell you the strength of your password. Red is weak, while green is very strong. Use a combination of numbers, letters, and symbols to increase the password strength. The password must be at least 4 characters long.
4. Click  **Save**.  
A system message tells you that you will be logged out.
5. When the login screen appears, log in with your new password.

## External Systems - Defining the Badge Camera for the System

Once all cameras or other imaging devices have been added as part of an external system, you can set which camera to use when creating badges for identities.

1. Select  > **My Account**.
2. Under the Profile tab, select a camera from the **Badge Camera** drop down list:
  - **Local Camera** — Any camera connected directly to your computer or built into your computer or monitor.
  - **IP-based camera** — Any IP-based camera previously connected to your network and added to your ACM system.
3. When you're finished, click .

Next time you create a badge, the selected camera is used to take the identity photo.

## Scheduling Batch Jobs

Batch jobs are processes, such as generating reports, that are performed automatically, according to a



schedule.

From the Job Specification page, you can create the following batch jobs:



## Generating a Batch Report

Batch reports are custom reports generated on a schedule and which can contain more data than reports generated from the Reports list, the Report Edit page or from the Report Preview page.

There are no length limits on any batch reports generated in the CSV spreadsheet format. In PDF format, the Audit Log report is limited to 13,000 records, the Identity Summary Report is limited to 100,000 records, and the Transaction Report is limited to 50,000 records.

**WARNING** — Risk of system becoming unusable. Scheduling large reports on separate but overlapping schedules, may cause memory problems that can result in the ACM system being unusable. To avoid this risk, schedule the start times for large reports, such as audit logs in any format, to allow for each report to finish before the next starts.

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

1. Select  **>My Account** and click the Job Specification tab.  
The Job Specification page is displayed.
2. Click the  **Add** button.  
The Job Specification - General dialog box is displayed.
3. In the **Appliance** drop down list, select the appliance on which this job will run.  
Only those appliances previously defined for this system appear in this option list.  
If only one appliance is used for this system (the default), this field is automatically populated.
4. In the **Name** field, enter a name for this batch job.
5. From the **Type** drop down list, select **Report**.  
After you select the job type, additional options are displayed.
  - From the **Report** drop down list, select the report you want to batch.  
Only custom reports appear in this list.
  - From the **Output Format** drop down list, select the format in which you want this job generated.
6. Click **Next**.  
The following screen shows the select report definition. Click **Back** to select a different report.
7. Click **Next** to continue.
8. On the following page, select how often the batch report is generated. From the **Repeat** drop down list, select one of the following options:
  - **Once** — The report will be generated once. Click the **On** field to display the calendar and select a specific date and time.
  - **Hourly** — The report will be generated at the same minute of every hour. Enter the minute when the report is generated at each hour. For example, if you want the report generated at 1:30, 2:30, etc. then you would enter 30.
  - **Daily** — The report will be generated every day at the same time. Enter the specific time when the report is generated in 24 hour time format.
  - **Weekly** — The report will be generated each week on the same day and time. Select the checkbox for each day the report will be generated, and enter the specific time in 24 hour format.

- **Monthly** — The report will be generated each month on the same day and time. Select the days when the report is generated and enter the specific time in 24 hour format. **Shift** + click to select a series of days, or **Ctrl** + click to select separate days.

9. Click **Next**.

A summary is displayed.

Select the **Send Email** checkbox if you want to receive an email copy of the report after it has been generated. In the following field, enter your email address.

10. Click **Submit** to create this job.

11. To activate or deactivate this job, select the job and click  **Activate/Deactivate**

## Applying an Identity Profile to a Group Using a Job Specification

Create and schedule an Identity Update batch job to apply a new, updated or temporary identity profile to all of the identities in a predefined group.

**Note:** Not all identity fields are supported in identity profiles.

After you make changes to an identity profile, the identities previously created from the identity profile are not automatically updated. Using a job specification and scheduling the job is one of the ways that these changes can be applied.

Scenarios to apply an identity profile to a group of identities include:




- To apply a set of standard settings. When you have many identities defined with non-standard settings, create a group containing these users and a new profile containing the standard settings. Then apply the new profile to the group of identities.
- To apply modified settings in a commonly used identity profile. After you make changes to an identity profile, the identities created from the identity profile are not automatically updated. You need to create a batch job to apply these changes. Create a group of all the users that were created using this profile, and then apply the modified profile to that group. If the profile is frequently modified, you can create a repeating schedule.
- To apply a profile temporarily to a group. When you have identities that require a different profile for a short time that cannot be satisfied using a policy, you can use an Identity Update batch job to "turn on" a temporary profile for a specified duration, and then "turn off" that profile by replacing it with a permanent profile. If the temporary profile is used repeatedly in a predictable manner, you can create a repeating schedule.

**Note:** A group containing all of the identities previously created from the identity profile must be created before the changes can be applied to the group. If the required groups have not been created, contact your System Administrator.

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

A temporary door template is one that is applied for a specific period of time (either once or repeating) You can apply a temporary door template to a group by using the Off Identity Profile option. Once the new identity profile expires, the original identity profile is applied.

To create an Identity Update job specification:

1. Select  > **My Account** and click the Job Specification tab.  
The Job Specification page is displayed.
2. Click the  **Add** button.  
The Job Specification dialog box is displayed.
3. In the **Appliance** drop down list, select the appliance on which this job will run.  
Only those appliances previously defined for this system appear in this option list.  
If only one appliance is used for this system (the default), this field is automatically populated.
4. In the **Name** field, enter a name for this batch job.
5. From the **Type** drop down list, select **Identity Update**.  
After you select the job type, more options are displayed.
  - From the **Group** drop down list, select the group of identities that you want to change.
  - From the **Identity Profile** drop down list, select the identity profile that you want to apply to the group. If you are applying a temporary profile, this is the "on" profile.
  - From the **Off Identity Profile** drop down list, select the identity profile to be applied if you want an identity profile applied temporarily (that is, you want the identity profile to expire).
  - From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.
6. Click **Next** to continue.  
The Job Specification - Schedule dialog box is displayed.
7. From the **Repeat** drop down list, select how often this batch job is run. Then specify the time you want the profile to be applied. If you selected an Off Identity Profile, you also specify when the Off profile is applied.
  - **Once** — The batch job is run once. Click the **On** and **Off** fields to display the calendar and select a specific date and time.
  - **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter 30.
  - **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.
  - **Weekly** — The batch job is run each week on the same day and time. Select the checkbox for each day the job will run, and enter the specific time in 24 hour format.
  - **Monthly** — The batch job is run each month on the same day and time. Select the days when the job will run and enter the specific time in 24 hour format. **Shift** + click to select a series of days, or **Ctrl** + click to select separate days.
8. Click **Next**.  
A summary is displayed.
9. Click **Submit** to create this job.
10. To activate or deactivate this job, select the job and click  **Activate/Deactivate**.

## Applying a Door Template to a Group Using a Job Specification

For ASSA ABLOY, Avigilon and Mercury Security doors.

Create and schedule a Door Update batch job to apply a new, updated or temporary door template to all of the doors in a predefined group.

After you make changes to a door template, the doors previously created from the door template are not

automatically updated. Using a job specification and scheduling the job is one of the ways that these changes can be applied.

Scenarios to apply a door template to a group of doors include:



- To apply a set of standard settings. When you have many doors defined with non-standard settings, create a group containing doors and a new template containing the standard settings. Then apply the new template to the group of doors.
- To apply modified settings in a commonly used door template. After you make changes to a door template, the identities created from the door template are not automatically updated. You need to create a batch job to apply these changes. Create a group of all the doors that were created using this template, and then apply the modified template to that group. If the template is frequently modified, you can create a repeating schedule.
- To apply a template temporarily to a group. When you have doors that require a different template for a short time that cannot be satisfied using a policy, you can use an Identity Update batch job to "turn on" a temporary template for a specified duration, and then "turn off" that template by replacing it with a permanent template. If the temporary template is used repeatedly in a predictable manner, you can create a repeating schedule.

**Note:** A group containing all of the doors previously created from the door template must be created before the changes can be applied to the group. If the required groups have not been created, contact your System Administrator.

When you choose to create a Door Update job, you have the option to apply a new, updated or temporary door template to the group.

A temporary door template is one that is applied for a specific period of time (either once or repeating). You can apply a temporary door template to a group by using the Off Door Template option. Once the new door template expires, the original door template is applied.

To create a Door Update job specification:

1. Select  > **My Account** and click the Job Specification tab.  
The Job Specification page is displayed.
2. Click the  **Add** button.  
The Job Specification - General dialog box is displayed. All options marked with \* are required.
3. In the **Appliance** drop down list, select the appliance on which this job will run.  
Only those appliances previously defined for this system appear in this option list.  
If only one appliance is used for this system (the default), this field is automatically populated.
4. In the **Name** field, enter a name for this batch job.
5. From the **Type** drop down list, select **Door Update**.  
After you select the job type, additional options are displayed.
  - From the **Group** drop down list, select the group of doors that you want to change.
  - From the **Door Template** drop down list, select the door template that you want to apply to the group.
  - From the **Off Door Template** drop down list, you have the option to select to an alternative

door template when the first door template expires.

- From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.

6. Click **Next** to continue.

The Job Specification - Schedule dialog box is displayed.

7. Select how often this batch job is run. From the **Repeat** drop down list, select one of the following options:


If you selected an Off Door Template, you will have the option to enter when the Off template is applied. Otherwise, only the On field is displayed.

- **Once** — The batch job is run once. Click the **On** field to display the calendar and select a specific date and time.
- **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter 30.
- **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.
- **Weekly** — The batch job is run each week on the same day and time. Select the checkbox for each day the job will run, and enter the specific time in 24 hour format.
- **Monthly** — The batch job is run each month on the same day and time. Select the days when the job will run and enter the specific time in 24 hour format. **Shift** + click to select a series of days, or **Ctrl** + click to select separate days.

8. Click **Next**.

A summary is displayed.



9. Click **Submit** to create this job.

10. To activate or deactivate this job, select the job from the list in the Batch Job Specifications window and click  **Activate/Deactivate**.

## Scheduling a Global Action

Perform this procedure to schedule global actions.

**Note:** The global actions must be created before they can be scheduled. If the required global actions have not been created, contact your System Administrator.

1. Select  **>My Account** and click the Job Specification tab.  
The Job Specification page appears.
2. Click the  **Add** button.  
The Job Specification dialog box is displayed.
3. In the **Appliance** drop down list, select the appliance on which this job will run.  
Only those appliances previously defined for this system appear in this option list.  
If only one appliance is used for this system (the default), this field is automatically populated.
4. In the **Name** field, enter a name for this batch job.

5. From the **Type** drop down list, select **Global Action**.

After you select the job type, additional options are displayed.

- From the **Global Action** drop down list, select global action to perform. Only configured global actions will appear on the list.
- From the **Off Global Action** drop down list, you have the option to select to a global action that is performed after the first global action expires.
- From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.

6. Click **Next** to continue.

7. On the following page, select how often this batch job is run. From the **Repeat** drop down list, select one of the following options:

- **Once** — The batch job is run once. Click the **On** field to display the calendar and select a specific date and time.
- **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter 30.
- **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.
- **Weekly** — The batch job is run each week on the same day and time. Select the checkbox for each day the job will run, and enter the specific time in 24 hour format.
- **Monthly** — The batch job is run each month on the same day and time. Select the days when the job will run and enter the specific time in 24 hour format. **Shift** + click to select a series of days, or **Ctrl** + click to select separate days.

**Note:** If you selected an Off Global Action, you will have the option to enter when the Off action occurs. Otherwise, only the On field is displayed.

8. Click **Next**.



A summary is displayed.

9. Click **Submit** to create this job.

10. To activate or deactivate this job, select the job and click  **Activate/Deactivate**.


## Setting Batch Door Modes

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

1. Select  **>My Account** and click the Job Specification tab.
2. Click the  **Add** button.  
The Job Specification dialog box is displayed.
3. In the **Appliance** drop down list, select the appliance on which this job will run.  
Only those appliances previously defined for this system appear in this option list.  
If only one appliance is used for this system (the default), this field is automatically populated.
4. In the **Name** field, enter a name for this batch job.

5. From the **Type** drop down list, select **Door Mode**.

After you select the job type, additional options are displayed.

- From the **Available** list, select the required doors then click  to add it to the **Members** list.
- From the **On Door mode** drop down list, select the door mode that you want to apply to the selected doors.
- From the **Off Door mode** drop down list, select the door mode that you want to apply to the doors when the On action is complete.
- From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.
- Select the **Activate** checkbox to make the door modes active.

6. Click **Next** to continue.

7. On the following page, select how often this batch job is run. From the **Repeat** drop down list, select one of the following options:

- **Once** — The batch job is run once. Click the **On** field to display the calendar and select a specific date and time.
- **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter 30.
- **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.
- **Weekly** — The batch job is run each week on the same day and time. Select the checkbox for each day the job will run, and enter the specific time in 24 hour format.
- **Monthly** — The batch job is run each month on the same day and time. Select the days when the job will run and enter the specific time in 24 hour format. **Shift** + click to select a series of days, or **Ctrl** + click to select separate days.

**Note:** If you selected an Off Door Mode, you will have the option to enter when the Off action occurs. Otherwise, only the On field is displayed.



8. Click **Next**.


A summary is displayed.

9. Click **Submit** to create this job.

## Setting Your Preferred Language

To set your preferred language in the ACM system:

1. Select  > **My Account**.
2. Select the language in **Locale**.
3. Click  **Save**.
4. Log out and log back in.

**Note:** The online help  is provided only in English (US), French, German, Italian and Spanish. If you set your system to a language other than these five languages, English (US) online help will be the default.



# Permissions and Rights

The following table describes the permissions and rights the default Monitoring Supervisor Role allows. All roles are made up of delegations. Each delegation is made up of rights.

Permissions	Rights
View Events page	System Summary Listing
	System Summary Screen Refresh
	System Summary Get Layout
	System Summary Update Layout
	Monitor Listing
	Monitor Notes Show
	Monitor Instructions Show
Search for events	Monitor Identity Show
	Spork Listing
	Spork Search
	Monitor/Search Filters Save
	System Summary Get Layout
View Alarms	System Summary Update Layout
	Alarm Monitor Listing
	Monitor Notes Show
	Monitor Instructions Show
	Alarms Code Photo
	Monitor View Actions
Respond to alarm activity	Maps-Alarms Show
	Alarm Monitor Acknowledge
	Alarm Monitor Clear
	Alarms Create Notes
	Alarm Monitor Acknowledge All
	Alarm Monitor Clear All

Permissions	Rights
View verifications	Swipe & Show Swipe & Show Get Doors Swipe & Show Get Door Name Get Photo Monitor Identity Show System Summary Get Layout System Summary Update Layout
View the status of assigned hardware	Monitor Listing Monitor Panels Status Monitor Periodic Update Monitor Appliance Status
Control assigned hardware	Doors Grant Doors Disable Doors Unlock Doors Lock Doors Restore Doors Mask Held Doors Mask Forced Doors Unmask Held Doors Unmask Forced
View and monitor status on assigned maps	Maps Monitor Listing Maps Show Maps Show Generate Image Maps Show Image Maps View Listing Maps Trace Mustering Dashboard Drill-Down
View the intrusion status	Monitor Intrusion Panel Status

Permissions	Rights
Control the assigned Bosch intrusion panels	Bosch Intrusion Area Clear Alarms Bosch Intrusion Area Disarm Bosch Intrusion Area Perimeter Delay Arm Bosch Intrusion Area Perimeter Force Delay Arm Bosch Intrusion Area Perimeter Force Instant Arm Bosch Intrusion Area Perimeter Instant Arm Bosch Intrusion Area Primary Delay Arm Bosch Intrusion Area Primary Force Delay Arm Bosch Intrusion Area Primary Force Instant Arm Bosch Intrusion Area Primary Instant Arm Bosch Intrusion Area Reset Sensors Bosch Intrusion Area Silence Bosch Intrusion Output Activate Bosch Intrusion Output Deactivate Bosch Intrusion Panel Command Execute Bosch Intrusion Panel Create Bosch Intrusion Panel Delete Bosch Intrusion Panel Detail Listing Bosch Intrusion Panel Detail Update Bosch Intrusion Panel Edit Bosch Intrusion Panel Listing Bosch Intrusion Panel Monitor Status Bosch Intrusion Panel Monitor Update Bosch Intrusion Panel New Bosch Intrusion Panel Update Bosch Intrusion Point Bypass Bosch Intrusion Point Unbypass

Permissions	Rights
Control the assigned DMP intrusion panels	DMP Intrusion Area Bypass Instant Arm
	DMP Intrusion Area Disarm
	DMP Intrusion Area Force Instant Arm
	DMP Intrusion Area Refuse Instant Arm
	DMP Intrusion Output Activate Momentary
	DMP Intrusion Output Activate Pulse
	DMP Intrusion Output Activate Steady
	DMP Intrusion Output Activate Temporal Code
	DMP Intrusion Output Deactivate
	DMP Intrusion Panel Command Execute
	DMP Intrusion Panel Config Update
	DMP Intrusion Panel Create
	DMP Intrusion Panel Delete
	DMP Intrusion Panel Detail Listing
	DMP Intrusion Panel Entities Update
	DMP Intrusion Panel Listing
	DMP Intrusion Panel Monitor Status
	DMP Intrusion Panel New
	DMP Intrusion Panel Reset Sensors
	DMP Intrusion Panel Show
	DMP Intrusion Panel Silence Alarm
	DMP Intrusion Zone Bypass
	DMP Intrusion Zone Unbypass
View live and recorded video	Cameras Show
	Monitor Cameras Show Video

Permissions	Rights
Add new identities. Cannot update fields after initial identity setup.	Identities My Account Identities Listing Identities Show Identities Advance Search Identities Date Search Identity Profiles Listing Identity Profiles Show List Identities New Identities Create Identities Edit Identity Profiles Populate Values
Force the identity to change the password at the next login to the ACM system.	Force Password Change
Add, modify, and update available roles	Identities Roles List Identities Roles Update
<p><b>Note:</b> The Stop Dates on the Role page and Role Report are different due to the UTC (Coordinated Universal Time) time server difference. For example, 12/31/2037 23:59:59 is displayed in the former and 01/01/2038 23:59:59 is displayed in the latter. In ACM 6.18 and later releases, there is no stop date for the role that has Never Expire enabled.</p>	
Add, modify, and update tokens	Tokens Listing Tokens Show Tokens New Tokens Create Tokens Edit Tokens Update Tokens Set Free Pass Identity Profiles Tokens Listing
Add and modify groups	Identities Groups List Identities Groups Update

Permissions	Rights
View assigned access permissions	Identities Show Access Identity Profiles Show Access
Capture live photos and save	Identities Image Capture Identities Image Save Identities Code Image Identities Photo Capture
Add and upload photos	Identities Photo Edit Identities Photo Update Identities Photo Render Identities Upload Photo
View transactional data	Identities Transactions
Print and issue badges	Identities Badge Show Identities Badge screen Identities Print Badge Identities Badge Render Identities Update Badge Preview Identities Update Badge
View reports	Reports Index Report Show Grant Access/Report Reports Show Grid Reports Custom Reports
Edit, preview, generate, and delete reports	Reports Edit Reports New Reports Create Reports Get Report Preview Reports Quick Report Reports Dynamic Criteria Reports Destroy

**Permissions****Rights**

View account details, batch jobs, and job specifications

Identities MyAccount  
Batch Job Specification Index  
Batch Job Specification New  
Batch Job Index  
View Batch Update Schedules

Create, edit, and delete batch jobs and job specifications

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