# Table of Contents

Introduction ................................................................. 6

Monitoring ........................................................................ 7
  Monitoring Events .......................................................... 7
  Pause/Resume Events ...................................................... 8
  Clear Events .................................................................. 8
  View Live Video ............................................................ 9
  View Recorded Video ..................................................... 9
  Create Event Notes ........................................................ 9
  View Event Notes .......................................................... 10
  View Event Instructions .................................................. 10
  View Event Identity Details .............................................. 11
  View Event History ........................................................ 11
  Change Events List Settings ............................................. 11
  Reconnect to Events List ................................................ 12

Searching for Events and Alarms ........................................ 13
  View Recorded Video (Search) .......................................... 14
  Create Event Notes (Search) ............................................ 14
  View Event Notes (Search) .............................................. 15
  View Event Instructions (Search) ...................................... 15
  View Event Identity Details (Search) ................................ 15
  View Event History (Search) ............................................ 16

Monitor Alarms ................................................................. 17
  Acknowledge Alarms ..................................................... 18
  View Live Video (Alarms) ............................................... 18
  View Recorded Video (Alarms) ........................................ 19
  Create Event Notes (Alarms) .......................................... 19
  View Event Notes (Alarms) ............................................. 20
  View Event Instructions (Alarms) .................................... 20
  View Event Identity Details (Alarms) ............................... 20
  View Event History (Alarms) .......................................... 21
  Change Alarms List Settings .......................................... 21

Monitor - Verification screen ............................................ 22
  Verifying Identities at Doors ........................................... 22
  Verification Events List ................................................. 23
  Monitor - Dashboard ..................................................... 24
Scheduling a Global Action ................................................................. 64
Setting Batch Door Modes ............................................................... 66
Permissions and Rights ..................................................................... 68
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 68.

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

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

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

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

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

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

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

- **Resume** — Click this button to restart the flow of events that are displayed on the page.
  
  This button only appears when the flow of events is paused.

- **Clear** — Click this button to temporarily clear all events from the screen. New events automatically begin to populate the list. To restore the cleared events, refresh the page.

- **Live Video** — Click this button to display live video that is associated with the selected event.

- **Recorded Video** — Click this button to display recorded video that is associated with the selected event.
Notes — Click this button to enter a new note or display any previously saved notes for the selected event.

Instructions — Click this button to display any instructions that should be completed when the event occurs. The instructions were added when the event was created.

Identity — Click this button to display details about the person that triggered the selected event.

History — Click this button to display a detailed history of this event.

Save Settings — Click this button to save your current settings for this page. For example, the columns and order for this page.

Select Columns — Click this button then choose the information that you want displayed.

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

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

Reconnect — Click this button to reconnect to the appliance.

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

Pause/Resume Events

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

Follow the steps below to pause and resume events.

1. Click Monitor to access the Monitor Events page. For more detail see Monitoring Events on the previous page.

2. Click Pause to pause the flow of events that are displayed on the page.

The flow of events does not actually stop, the system simply pauses the display of live updates until you click Resume (this button only appears when the flow of events is paused).

3. Click Resume to restart the flow of events that are displayed on the page.

The list of events will resume updating.

Clear Events

Follow the steps below to clear all displayed events.

1. Click Monitor to access the Monitor Events page.

2. Click Clear to temporarily clear all events from the screen.

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

NOTE: This does not delete the events, it just removes the existing events from the view. To restore the cleared events, refresh the page.
View Live Video

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

Follow the steps below to view live video.

1. Click Monitor. The Monitor Events page displays (for more information, see Monitoring Events on page 7).
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 7).
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 7).

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 7).

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 7).
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 7).
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 **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 7).

   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.

The Events Search (Transactions) page appears.

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

The Search area is displayed:

![Search options](image)

**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.

Add as many search filters as you need to fulfill your search criteria.

8. When you have entered all your search criteria, click Search. The search results are listed in the table above the search area.

9. Select any transaction from the search result and use the action buttons at the top of the page to see the details of the event.

**View Recorded Video (Search)**

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

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

1. Click Monitor > Search. The Events Search (Transactions) page displays.

2. Select an event from the list.

   Only events or alams with an icon will have video. The icons are not displayed by default. For more information, see Change Transactions List Settings on page 1.

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

   The Monitor Screen - Recorded Video window displays.

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

2. Select the event that you want to create notes for.

3. Click **Notes** to create notes for the selected event.

   The Monitor Screen - Notes Window will display.

4. Enter text in the **New Note** field.

5. Click to save the new note.

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

6. Close the dialog box.

**View Event Notes (Search)**

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

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

1. Click **Monitor > Search**. The Events Search (Transactions) page displays.

2. Select the event that you want to view notes for.

3. Click **Notes** to view notes for the selected event.

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

**View Event Instructions (Search)**

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

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

1. Click **Monitor > Search**. The Events Search (Transactions) page displays.

2. Select the event that you want to view instructions for.

3. Click **Instructions** to view instructions for the selected event.

   The Monitor Screen - Instructions Window will display.

4. Close the window to return to the Events Search (Transactions) page.

**View Event Identity Details (Search)**

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

### View Event History (Search)

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

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

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

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

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

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

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

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

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

**NOTE:** Some of the buttons are disabled until you select an event that includes the relevant details.
- **Clear** — Click this button to clear one or more acknowledged alarms from the list.
- **Clear All** — Click this button to clear all alarms from the Acknowledged Alarms list.
- **Select Columns** — Click this button then choose the information that you want displayed.

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

**Acknowledge Alarms**

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

Follow the steps below to acknowledge alarms.

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

**View Live Video (Alarms)**

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

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

1. Click **Monitor > Alarms**. The Monitor Alarms page displays. For more information see **Monitor Alarms** on the previous page.
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 *Monitor Alarms* on page 17).
2. Select an event from the list.
   - Only events or alarms with an icon will have video.
3. Click **Recorded Video** to display live video that is associated with the selected event. (This button only displays if video is available for this event.)
   - The Monitor Screen - Recorded Video window displays. View the video in this window.
   - If the window does not display any video in the image panel, you may need to change your browser settings to allow the display of insecure or mixed content. For more information, see the Help files for your browser.

**Create Event Notes (Alarms)**

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

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

1. Click **Monitor > Alarms**. The Monitor Alarms page displays. For more information see *Monitor Alarms* on page 17.
2. Select the event that you want to create notes for.
3. Click **Notes** to create notes for the selected event.
   - The Monitor Screen - Notes Window will display.
4. Enter text in the **New Note** field.
5. Click to save the new note.
   - The note will display in the list below the **New Note** section. The date, Operator and note will display in this list.
6. Close the dialog box.
View Event Notes (Alarms)

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

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

1. Click Monitor > Alarms. The Monitor Alarms page displays. For more information see Monitor Alarms on page 17.

2. Select the event that you want to view notes for. Events with notes will display with in the Icon column.

3. Click Notes to view notes for the selected event. Alternatively clicking will do the same thing. The Monitor Screen - Notes Window will display. Existing notes will display as a list below the New Note section. The date, Operator and note will display in this list.

4. Close the dialog box to return to the Monitor Alarms page.

View Event Instructions (Alarms)

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

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

1. Click Monitor > Alarms to access the Monitor Alarms page displays. For more information see Monitor Alarms on page 17.

2. Select the event that you want to view instructions for. (Events with instructions will display with in the Icon column.)

3. Click Instructions to view instructions for the selected event. The Monitor Screen - Instructions Window will display. View the instructions in the table that displays.

4. Close the window to return to the Monitor Alarms page.

View Event Identity Details (Alarms)

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

1. Click Monitor > Alarms. The Monitor Alarms page displays. For more information see Monitor Alarms on page 17.

2. Select the event that you want to view identity details for.

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

**View Event History (Alarms)**

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

1. Click Monitor > Alarms to access the Monitor Alarms page. For more information see Monitor Alarms on page 17.
2. Select the event that you want to view history for.
3. Click History to view history for the selected event.
   - The Monitor Screen - History Window will display.
4. View the history details.
5. Close the window to return to the Monitor Alarms page.

**Change Alarms List Settings**

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

1. Click Monitor > Alarms to access the Monitor Alarms page. For more information see Monitor Alarms on page 17.
   - The list displays in date order, with the most recent events at the top of the list.
2. If you want to re-sort the order of the list:
   - Click in the heading of the column to sort by (e.g. Priority). The list will sort in ascending order based on that column (e.g. ascending order of priority).
   - To change the sort order to descending, click the column heading again.
3. If you want to re-sort the order of the columns, click on the column you want to move then drag and drop this to it's new location.
4. If you want to add or remove columns, click Select Columns and do the following:
   - Click beside the Column name of any columns to be added so that a check mark displays.
   - Click beside the Column name of any column to be deleted so that a check mark no longer displays.
5. If you want to change the sound settings:
   - If the sound is on, click Sound Off to turn the sound off.
   - If the sound is off, click Sound On to turn the sound on.
6. Click Save Settings if you want to save the new settings.
   - A message box displays with the message 'ACM Notification. Successfully saved.'

**NOTE:** To reset default settings, select > Clear Custom Layouts. This resets all customized lists to their default setting.
Monitor - Verification screen

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

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

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

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

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

Verifying Identities at Doors

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

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

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

If the person:

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

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

**Verification Events List**

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

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

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

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

2. If you want to clear a single event from the list, select the event and click **Clear**. To clear all events, click **Clear all**.

3. If you want to re-sort the order of the list:
   - Click in the heading of the column to sort by (e.g. Priority). The list will sort in ascending order based on that column (e.g. ascending order of priority).
   - To change the sort order to descending, click the column heading again.

4. If you want to re-sort the order of the columns, click on the column you want to move then drag and drop this to it's new location.

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

6. Click **Save Settings** if you want to save the new settings.

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

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

**NOTE:** To reset default settings, select **Clear Custom Layouts**. This resets all customized lists to their default setting.
Monitor - Dashboard

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

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

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

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

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

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

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

The color applied to icons in the Dashboard tables indicate the status of the hardware component.
<table>
<thead>
<tr>
<th>Color</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>⬤</td>
<td>Normal</td>
<td>Online and working properly.</td>
</tr>
<tr>
<td>⬤</td>
<td>Trouble</td>
<td>Indeterminate status. Seen for inputs, outputs, and the ACM appliance.</td>
</tr>
<tr>
<td>⬤</td>
<td>Alarm</td>
<td>Alarm condition. An ACM operator should investigate the problem and resolve the issue.</td>
</tr>
<tr>
<td>⬤</td>
<td>Masked</td>
<td>Input is currently masked. Its actual state is not displayed. Mask inputs that are intended to change as part of normal operations, so that they are not constantly being reported.</td>
</tr>
</tbody>
</table>

**Panels table**

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

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

**Installing, uninstalling, or deleting a panel or subpanel:**

Click ![install_uninstall](image) at the end of a row in the Panels table or Subpanels table to complete any of the following actions:

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

**Masking and unmasking inputs:**

Click ![mask_unmask](image) at the end of a row in the Inputs table to complete any of the following actions:

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

**Masking and unmasking outputs:**

Click ![mask_unmask](image) at the end of a row in the Outputs table to complete any of the following actions:

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

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

- Click on the name of the panel to expand the Subpanels table.
• Click on the name of a subpanel to expand the Inputs and Outputs tables.

Searching the Panels table:

1. Use any (or all) of the following to define your search:
   • Enter your search term in the Search... field. Use any series of letters and numbers to search for the panels you want to see.
   • If known, select the Device Status.
   • If known, select the Appliance the panel is connected to.
   • If known, select the Group the panel is included in.
2. Click OK. The Panels list is filtered to show the results of your search.

Sorting the Panels table:

1. Click in a column heading:
   • Click ▲ to sort in ascending order.
   • Click ▼ to sort in descending order.

To see the legend for panel statuses:

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

Doors table

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

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

Controlling doors:

Select doors in the list and then use the drop-down options from the control buttons at the top of the page to control them:

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

### Door Mode
- **Card Only** — This door can be accessed using a card. No PIN is required.
- **Card and Pin** — This door can only be accessed using both a card and a PIN.
- **Card or Pin** — This door can be accessed either by entering a PIN at a keypad or by using a card at the card reader.
- **Pin Only** — This door can only be accessed by entering a PIN at a keypad. No card is required.
- **Facility Code Only** — This door can be accessed using a facility code.

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

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

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

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

### Searching, sorting, and filtering

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

### Searching the Doors table:

1. Use any (or all) of the following to define your search:
   - Enter your search term in the **Search**... field. Use any series of letters and numbers to search for the doors you want to see.
   - If known, select the **Device Status**.
   - If known, select the **Appliance** the door is connected to.
   - If known, select the **Group** the door is included in.

2. Click **OK**.

### Creating a filter that includes multiple filters:
1. Click **Advanced Filters**.

2. Select filters:
   - **Alarms**—Select the alarms to include from the list of alarms.
   - **Masked**—Select the masks to include from the list of masks.
   - **Normal**—Select to include all properly functioning doors.
   - **Door Mode**—Select the door modes to include from the list of door modes.

   To unselect all selected filters, click **Unselect All**.

3. If you want to save the selected filters, select **Remember Filters**.

4. Click **OK**.

**Sorting the Doors table:**

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

**To see the legend for all door statuses:**

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

There are three groupings which are color-coded — Normal ✅, Alarms ✖, Masked ☑.

**LifeSafety Panels table**

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The name of the LifeSafety panel. Click this name to display the panel details.</td>
</tr>
<tr>
<td><strong>Installed</strong></td>
<td>The status of the panel’s installation: ✅ (installed) or ✖ (uninstalled). This field is not selectable and cannot be toggled.</td>
</tr>
<tr>
<td><strong>Commands</strong></td>
<td>The commands available to control a LifeSafety panel:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status</strong> — Click this button to display the current status of the displayed LifeSafety panel.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Log</strong> — Click this button to view the log of events/alarms recorded by the LifeSafety panel.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Edit</strong> — Click this button to open the browser page for this remotely connected panel and make changes to the configuration as required. The page displayed is</td>
</tr>
</tbody>
</table>
Controlling System Hardware

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

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

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

- Click the Held dropdown, then:
  - Click Mask Held to mask the Door Held Open alarm for this door. The status color changes to blue and is no longer included in any alarm subtotal.
  - Click Unmask Held to unmask the Door Held Open alarm for this door.
- Click the Forced dropdown, then:
  - Click Mask Forced to mask the Door Forced Open alarm for this door. The status color changes to blue and is no longer included in any alarm subtotal.
  - Click Mask Unforced to unmask the Door Forced Open alarm for this door.
4. To change the door mode, Click **Door Mode**, then choose from the following options:
   - Card Only
   - Card and Pin
   - Card or Pin
   - Pin Only
   - Facility Code Only

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

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

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

7. To install or uninstall a door or subpanel, click on the existing icon (e.g. if Installed is the current status, click on the installed icon ✅ to change the status to ✗ Uninstalled).

The action is performed on the specified device.

### Status Colors

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

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢 Normal</td>
<td>The Access Control Manager component is online and working properly.</td>
</tr>
<tr>
<td>⚫ Trouble</td>
<td>The Access Control Manager component has an indeterminate status.</td>
</tr>
<tr>
<td>🔴 Alarm</td>
<td>The Access Control Manager component is experiencing an alarm condition. The delegated operator should investigate the problem and resolve the issue.</td>
</tr>
<tr>
<td>Color</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Masked</td>
<td>The specified Access Control Manager input is currently masked. Its actual state is not displayed. Mask inputs that are intended to change as part of normal operations, so that they are not constantly being reported.</td>
</tr>
</tbody>
</table>
Monitor Screen - Map Templates page

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New Map Template</td>
<td>Click this button to add a new map template. For more information, see Maps - Creating and Editing a Map.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the map template.</td>
</tr>
<tr>
<td></td>
<td>A list of all the configured maps is displayed. Also included in the list are configured Mustering dashboards.</td>
</tr>
<tr>
<td></td>
<td>Click the name of the map template to display the configured map or dashboard.</td>
</tr>
</tbody>
</table>

Using a Map

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

From the map, you can:

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

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

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

To access and monitor your site from a map:

2. In the Map Templates list, click the name of a map.
   
   The map is displayed. Some of the displayed elements may not appear in your map or the example below.
Figure 2: Example map

<table>
<thead>
<tr>
<th>Feature</th>
<th>Map Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doors</td>
<td>![Door Icon]</td>
</tr>
<tr>
<td>Panels</td>
<td>![Panel Icon]</td>
</tr>
<tr>
<td>Subpanels</td>
<td>![Subpanel Icon]</td>
</tr>
<tr>
<td>Inputs</td>
<td>![Input Icon]</td>
</tr>
<tr>
<td>Outputs</td>
<td>![Output Icon]</td>
</tr>
<tr>
<td>Cameras</td>
<td>![Camera Icon]</td>
</tr>
<tr>
<td>Zoom In</td>
<td>![Zoom In Icon]</td>
</tr>
<tr>
<td>Zoom Out</td>
<td>![Zoom Out Icon]</td>
</tr>
<tr>
<td>Global Actions</td>
<td>![Global Action Icon]</td>
</tr>
<tr>
<td>Dashboard Elements</td>
<td><strong>Square, circle or text object</strong></td>
</tr>
</tbody>
</table>
The actions you can complete on a map are determined by the permissions delegated to you by the roles you are assigned.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review hardware status</td>
<td>The colored bar below each item displays an overview of the current communication and power status. Click the icon on the map to display the control menu. For more information about the colored hardware status bar, see the specific hardware status page. For more information about the status colors, see Status Colors on page 30.</td>
</tr>
<tr>
<td>Review an alarm</td>
<td>If you see a red alarm indicator, the item on the map is in an alarm state. Click the alarm indicator to see the status details. For more information about alarm actions, see Monitor Alarms on page 17.</td>
</tr>
<tr>
<td>Modify or delete an override</td>
<td>If you see solid blue disk indicator, an active override is in effect on the door. If you see a hollow blue disk indicator, an inactive override is defined. Click the indicator to open the Doors: Overrides page to see details.</td>
</tr>
<tr>
<td>Respond to a priority situation</td>
<td>If you see a red bounding box around the status indicator, the door is in Priority Mode. <strong>Important:</strong> 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.</td>
</tr>
</tbody>
</table>
| Control a door | Click on the map to display the door control menu for that door. Use these options to set the Door Mode:  
  - **Card Only** — set the Door Mode to Card Only. The person must swipe their card to be granted access.  
  - **Card and PIN** — set the Door Mode to Card and PIN. The person must swipe their card and enter their PIN to be granted access.  
  - **Card or PIN** — set the Door Mode to Card or PIN. The person must swipe their card or enter their PIN to be granted access.  
  - **Facility Code Only** — set the Door Mode to Facility Code Only. The person must enter the facility code to be granted access.  
To confirm these changes, navigate to Physical Access > Doors to open the Doors listing page, then check the value in the Door mode column for this door. Use these options to initiate door actions:  
  - **Unlock** — unlock the door. This door will remain unlocked until the Restore command is issued.  
  - **Lock** — lock the door. This door will remain locked until the Restore command is issued. |
To... | Do this...
---|---
| **Grant** — grant access to the person who is at the door. The door will be momentarily unlocked to permit entry.  
**Restore** — reset the door mode to its configured value.  
Use these options to mask or unmask alarms:  
| **Mask Held** — mask the Door Held Open Alarm.  
| **Unmask Held** — unmask the Door Held Open Alarm.  
| **Mask Forced** — mask the Door Forced Open Alarm.  
| **Unmask Forced** — unmask the Door Forced Open Alarm.  
| To view live video, recorded video, notes, instructions, identities, and history click **Trace** to display the event transactions for the door.  
| To hide the control menu, click the icon again.

**Control a panel or subpanel**

Click the 🖼️ on the map to display the panel control menu, then for the panel or subpanel use these options:

- **Panels**
  - **Download Params** — download the latest system configurations to the panel.
  - **Tokens** — download the tokens to the panel.
  - **Reset/Download** — reset and download the current system configuration to the panel.
  - **APB Reset** — resets all panel and area counts to zero.
  - **Clock** — re-sync the panel time.
  - **Trace** — display the event transactions for the panel.

- **Subpanels**
  - **Trace** — display the event transactions for the subpanel.

Viewing live video, recorded video, notes, instructions, identities, and history can be performed on the event transactions.

To hide the control menu, click the icon again.

**Control an input**

Click the 🕒 on the map to display the input control menu for the input.

Use these options to mask or unmask the input:

- **Mask** — mask the input.
- **Unmask** — unmask the input.

To hide the control menu, click the icon again.
<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Control an output | Click the 🌞 on the map to display the output control menu for the output. Use these options to initiate output actions:  
  * On — activate the output.  
  * Off — deactivate the output.  
  * Pulse — pulse the output.  
  To hide the control menu, click the icon again. |
| Display video     | Click the 🎬 on the map to display the Camera Video window.                 |
| Open a linked map | Click 🎬 to display a linked map, or 🎬 to display a linked map.            |
| Execute a global action | Click 🎬 to execute the global action associated with the icon. Hover over the icon to display the global action configured for each icon. |
| Monitor the dashboard | If there is a Mustering dashboard configured on the map, it may appear as a line of text or as a shape with text inside. The dashboard displays the number of identities in the area and may include the name of the area. In Example map on page 33, the dashboard is the gray square.  
  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. |

Add Map

Follow the steps below to add maps.

1. Click Monitor > Maps. The Map Templates (Monitor) list displays.
2. Click Add New Map Template.
   The Map Template: Add New page displays.
3. Enter a name for the Map in the Name field.
4. To:
   - upload a file, select File and click Browse then select the file to upload in the Choose File to Upload dialog box and click Open.
   - create a blank canvas, select Blank Canvas.
5. To resize the image, enter resizing proportions in the Re-size To fields.
6. Click ✓ to save the map.

The Map Template: Edit page displays.
Monitor Intrusion Panels

The following procedures relate to monitoring Bosch intrusion panels.

Monitor Intrusion Panel Status

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

To monitor intrusion panel status:

1. Select Monitor > Intrusion Status.
   The Monitor Intrusion Status - Panels screen displays.

2. View the list that displays.

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

   The following statuses apply to all of the above:

   - Online
   - Alarm
   - Trouble

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

3. If you want to narrow the list that displays use the filter function. Enter a panel name to filter the list results by panel. Type in the name (or part of the name) of the panel and the list will update as you type.

4. If you want to sort the list, click to sort in ascending order, or to sort in descending order in each column.

Monitor Intrusion Panel Areas

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

To monitor intrusion panel area status and make updates as required:
1. Select **Monitor > Intrusion Status**.

2. Click the **Areas** tab.

   The Monitor Intrusion Status - Areas screen displays.

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

   The following statuses apply to all of the above:

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

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

4. If you want to narrow the list that displays, either:
   
   - Use the filter function. Enter an area name to filter the list results by area. Type in the name (or part of the name) of the area or panel and the list will update as you type.
   
   - Select a single status (e.g. Partial Arm) to view.

5. If you want to sort the list, click ▲ to sort in ascending order, or ▼ to sort in descending order in each column.

6. To arm an area:
   
   - Select the areas to be armed.
   
   - Click **Master** then select the arming option. Options are:
     
     - **Instant Arm** - Arm all points for the selected areas instantly
     - **Delay Arm** - Arm all points for the selected areas with an entry/exit delay
     - **Force Instant Arm** - Arm all points for the selected areas instantly, regardless of their current state
     - **Force Delay Arm** - Arm all points for the selected areas with an entry/exit delay, regardless of their current state

7. To arm a perimeter area:
- Select the areas to be armed.
- Click **Perimeter** then select the arming option.
  - Instant Arm
  - Delay Arm
  - Force Instant Arm
  - Force Delay Arm

8. To disarm select the areas to be disarmed and click **Disarm**.
9. To silence intrusion alarms select the areas to be silenced and click **Silence**.
10. To reset the sensors select the areas to be reset and click **Reset Sensors**.
    
    The reset time is 5 seconds. During the reset time, alarms from the points associated with the selected areas will be ignored.

**Monitor Intrusion Panel Points**

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

To monitor intrusion panel point status:

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

The following statuses apply to all of the above:

- **Green**: Normal
- **Red**: Faulted
- **Orange**: Bypassed
- **Yellow**: Trouble

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

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

6. If you want to bypass or unbypass a point:
   - Select the point (or points) in the list, and
   - Click either the **Bypass** or **Unbypass** button.

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

**Monitor Intrusion Panel Outputs**

The intrusion panel outputs display the current status of all connected outputs. For example, if 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 > Intrusion Status**.

2. Click the **Outputs** tab.

   The Monitor Intrusion Status - Outputs screen displays.

3. View the list that displays. A status is displayed for each output - the available statuses are:

   - Inactive
   - Active
   - Trouble

4. If you want to narrow the list that displays, either:
   - Use the filter function. Enter an output name to filter the list results by output. Type in the name (or part of the name) of the output, or panel and the list will update as you type.
   - Select a single status (e.g. Active) to view.

5. If you want to sort the list, click ✷ to sort in ascending order, or ◼ to sort in descending order in each column.

6. If you want to activate or deactivate an output:
   - Select the outputs in the list, and
   - Click either the **Activate** or **Deactivate** button.
Identities

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

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

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

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

Adding an Identity

Any person who needs access to the site managed by the ACM system or to the ACM software must have an identity record in the ACM system. A person with an identity record can be issued a badge to allow them access to the site, and a user of the ACM software can be issued a login and password.

WARNING — Do not add identities authenticated with pivCLASS using this procedure. You must use the pivCLASS registration system to add these identities in the ACM system. Using pivCLASS-compliant registration software to add identities to the ACM system is out of scope of this document.

To add a new identity:

1. Click Identities.
   The Identities Search page appears.

2. Click Add New Identity.
   If you have defined one or more Identity Profiles for this system, the Identity Profile dialog box will pop up:
From the **Identity Profile** drop down list, select the profile you want to assign to this identity, then click **OK**.

If you do not want to assign an identity profile to this identity, click **Cancel**.

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

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

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

4. Click ✅.

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

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

   When the page refreshes, you are automatically taken to the Token: Add page.

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

   When you are finished, click ✅.

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

### Identities - Assigning Roles

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

To assign roles to an identity:
1. Click **Identities**.
   The Identities Search page is displayed.

2. From the Identities Search page, perform a search for an identity.
   For more information, see *Searching for an Identity* on page 51.

3. Click on the name of the identity you want to edit.
   The Identity Edit screen appears.

4. Select the **Roles** tab.

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

   To remove a role from the user, select the role from the Members list, then click.
   **NOTE:** You can select multiple items by using the **Ctrl** or **Shift** key.

6. Click

---

**Identities - Assigning Tokens**

Tokens are used to authenticate individuals and allow (or deny) them physical access to the access-controlled parts of your site. Tokens can be associated with access cards, biometric data (such as fingerprints), or with connected devices such as smartphones. They are part of the person's Identity record.

If someone requires access to a controlled area, they are issued a token that is associated with the type of reader and method they use to authenticate themselves. The token is then associated with an access card, fingerprint record, or app that the person can present to authenticate themselves at a reader. To further restrict access, identities can be assigned to specific roles that allow access to role-specific areas within your site.

To create tokens and assign them to an identity:

1. Click **Identities**.
   The Identities Search page is displayed.

2. From the Identities Search page, perform a search for an identity.
   For more information, see *Searching for an Identity* on page 51.

3. Click on the name of the identity you want to edit.
   The Identity Edit screen appears.

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.

7. Click✔.

8. Click **Download** to download the token to the connected panels and associated doors.

9. To assign this token to a badge, select the **Badge** tab.

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

11. Click✔ (Save).

**Identities - Assigning Groups**

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

To assign groups to an identity:

1. Click **Identities**.
   
The Identities Search page is displayed.

2. From the Identities Search page, perform a search for an identity.
   
   For more information, see *Searching for an Identity* on page 51.

3. Click on the name of the identity you want to edit.
   
The Identities: Edit screen is displayed.

4. Select the **Groups** tab.

5. From the Available list, select all the groups that you want to add the user to, then click✔.
   
The group is added to the Members list to show that the user is now a member.

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

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

6. Click✔.

**Capturing and Uploading Photos of an Identity**

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

**Captured photo:** A photograph taken by a badge camera connected to your computer and to the ACM system, and saved in the ACM system. Captured photos are in JPG format.
Uploaded photo: A graphics file in JPG, PNG, GIF format that you upload from any location your computer can access and save in the ACM system. Typically, you would upload a JPG file for access badges.

NOTE: The Internet Explorer web browser supports only the uploading of JPG files. Do not attempt to upload any other file format if you are using the ACM client in the Internet Explorer web browser.

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

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

- **Local Camera** — Any camera connected directly to your computer or built into your computer or monitor.

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

- **IP-based camera** — Any IP-based camera previously connected to your network and added to your ACM system.

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

Before you can:

- Use a camera to capture photos, you must specify the badge camera you want to use in your user profile. For more information, see *External Systems - Defining the Badge Camera for the System* on page 58.

- 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 *Identities - Creating Badges* on page 50.

Capturing a photo

1. There are two ways to access the Capture page:
   - From the Identities Search page, click ![Image Capture](image_capture.png) 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](image) **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](image) **Save and Edit** to save the photo and open the photo editing tool, or ![Save](image) **Save** to add the photo directly to the **Photos** tab.

5. On the **Photos** tab, select the **Primary** check box if you want this photo to appear on this person's Identity page and access badge.

6. Click ![Check](image).

**Uploading a photo**

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

   The screen expands to include more fields.

2. Click **Choose File** and navigate the directory to find the photo you want to upload.

   Click **Open** to select the photo. You can upload files in JPG, PNG, GIF format.

3. On the **Photos** tab, click the **Primary** check box if you want this photo to appear on this person's
Identity page and access badge. If no primary photo is selected, the first photo on the list is used.

4. Click ✓.

Editing a photo

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

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

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

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

• To resize the overlay freely:
  1. Click **Free**.
  2. Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay will be resized.
  3. Drag the mouse to resize the overlay. The overlay will be resized only in the direction of the cursor.

• To rotate the overlay:
  1. Click outside the current overlay.
  2. Drag the mouse to draw a new overlay.

• To replace the overlay:
  1. Click outside the current overlay.
  2. Drag the mouse to draw a new overlay.

2. Adjust the photo.

• To enlarge or reduce the photo:
  Use the + and - magnifier control buttons to adjust the photo size in stepped increments.

• To reposition the photo:
  Use the up, down, left and right control buttons to adjust the photo position in stepped increments.

• To rotate the photo:
  1. Use the counterclockwise circular arrow to rotate the photo to the left by 90°.
  2. Use the clockwise circular arrow to rotate the photo to the right by 90°.

• To flip the photo:
  1. Use the horizontal double-ended control button to flip the photo left to right.
  2. Use the vertical double-ended control button to flip the photo top to bottom.

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

3. Save the photo:

  Click ✅.

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

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

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

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

**Deleting a photo**

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

1. Click 🚭.
2. Click 🆐.

**Identities - Creating Badges**

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

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

To create a badge for a user:

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

**NOTE:** When printing the badge, ensure that the Header and Footer settings are turned off or set to blank.
Searching for an Identity

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

1. The Search area is at the top of the Identity Search page. Fill out the following fields:
   - Last Name field.
   - (Optional) The First Name and/or Internal Number fields.
   - (Optional) The Group field.
2. Add any additional search criteria as follows:
   - Select the criteria from the Search Field drop down list.
   - Enter or select the value to search for in the Search Value field.
   - Click Add Criteria to add an additional search, then repeat the steps in the bullets above for each additional criteria. Add as many search filters as you need to fulfill your search criteria.
   - At any time, you can click Clear Search to clear all fields.
   - To remove a single criteria row, click Remove.
3. In the drop down list to the right of the Search button, select whether the values entered in the fields should be combined into a single search criteria (And) or used as separate search criteria (Or).
   - If And is selected, only the identities that fit all entered criteria will appear. If Or is selected, the identities that fit one or more of the entered criteria will appear.
4. When you have entered all your search criteria, click Search.
   - The page refreshes and displays your search results.
   - NOTE: Always enter data in the Search Value field. Searching using blank entries will return all identities as the result.

Editing an Identity

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

To edit an existing identity:

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

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

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

**Reports - Generating Reports**

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

You can generate a copy of reports from the Reports 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 *Reports - Editing* on the next page.

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

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

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

**Reports - Report Preview**

When you click the name of a report from the Report 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.
### Generate Report

The generate report options are displayed in the top left corner of the report preview.

- ![PDF](Image) — Click this button to generate a PDF copy of the current report.
- ![CSV](Image) — Click this button to generate a CSV or spreadsheet copy of the current report.

### Preview Bar

The preview options are displayed at the bottom of the report page.

- ![Filter](Image) — Click this icon to filter the report.

  The report filter options are displayed. The options change depending on the report.

  - Click **Search** to perform a search using the selected filter options.
  - Click **Reset** to clear the report filter options.
  - In the drop down list beside the Reset button, choose if the search will locate **all or any** transactions that match the selected report filters.
  - Click **Save** to save and apply the selected filters to the default report.

- ![Pagination](Image) — Select the number of items you want to display on a single page.

- ![First Page](Image) — Click this button to return to the first page of the report.

- ![Previous Page](Image) — Click this button to return to the previous page of the report.

- **Page 1** of 1 — Enter the page you want to go to.

- ![Next Page](Image) — Click this button to bring up the next page of the report.

- ![Last Page](Image) — Click this button to go to the last page of the report.

- ![Refresh](Image) — Click this button to refresh the report.

### Reports - Editing

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

If you plan to use the filtered report frequently, you may want to create a custom report rather than modifying the default system report every time. For more information see *Reports - Creating Custom Reports* on page 56.

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 59.

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 the report that you want to edit.

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

3. On the following page, select your preferences for the report.

4. Click to save your changes.

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

### Reports - Editing Audit Log and Transaction Reports

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

3. Click in the bottom left-hand corner on the following page (either the Grid: Transaction Report or Grid: Audit Log page).

   The Find section opens.

4. Do the following to define criteria for the report:
   - Select an option in the search type field (e.g. Panel Date).
   - Select an option in the search operator field (e.g. greater or equal to).
   - Select an option in the search value field (e.g. 12/07/2015 00:00:00).

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

5. Click to add more search fields, if required.
   Complete step 4 above for each additional field added.

6. Click Save to save your changes.
   The ACM Notification message displays with the message ‘Search Parameters successfully changed’.

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

8. To reset the search criteria, click Reset

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

**Reports - Creating Custom Reports**

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

1. Click Reports.

2. Click for the report you want to base the custom report on.

3. On the following Report Edit page, select the Copy Report check box.

4. Give the new report a name.

5. Edit the report options to meet your requirements.

6. Click to save the new custom report.

   The Custom Reports list displays with the new report automatically added to the list.
Reports - Creating Custom Audit Log and Transaction Reports

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

1. Click Reports.
2. Click Transaction Report in the Report Name column.
3. Click at the bottom of the page. The preview bar expands to display search criteria.
4. Enter the details you want to include in the report in the Find section. (Click to add more fields.)
5. Click Search.

The system transactions are filtered into a report.

6. In the Create Custom Report field, enter a name for the report.
7. Click Create Custom Report to save the new report.

The new report is automatically added to the Custom Reports list.
Setting Personal Preferences

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

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

### Changing the Password in My Account

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

1. In the top-right, select My Account.
2. On the following Profile page, enter your current password in the **Old Password** field.
3. In the **Password** field, enter your new password.
   
   As you enter your new password, the status bar underneath will tell you the strength of your password. Red is weak, while green is very strong. Use a combination of numbers, letters, and symbols to increase the password strength. The password must be at least four characters long.

4. Click ✔️ to save your new password.

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

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

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

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

1. Select My Account.
2. Under the Profile tab, select a camera from the **Badge Camera** drop down list:
   
   - **Local Camera** — Any camera connected directly to your computer or built into your computer or monitor.
     
     **NOTE**: Images cannot be captured with a local camera from an ACM client running in the Internet Explorer or Safari web browsers, or running on a mobile device.
   
   - **IP-based camera** — Any IP-based camera previously connected to your network and added to
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 check box for each day the report will be generated, and enter the specific time in 24 hour format.
   
   - **Monthly** — The report will be generated each month on the same day and time. Select the days when the report is generated and enter the specific time in 24 hour format. **Shift + click** to select a series of days, or **Ctrl + click** to select separate days.

9. Click **Next**.

   A summary is displayed.

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

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

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

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

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

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

Scenarios to apply an identity profile to a group of identities include:
• To apply a set of standard settings. When you have many identities defined with non-standard settings, create a group containing these users and a new profile containing the standard settings. Then apply the new profile to the group of identities.

• To apply modified settings in a commonly used identity profile. After you make changes to an identity profile, the identities created from the identity profile are not automatically updated. You need to create a batch job to apply these changes. Create a group of all the users that were created using this profile, and then apply the modified profile to that group. If the profile is frequently modified, you can create a repeating schedule.

• To apply a profile temporarily to a group. When you have identities that require a different profile for a short time that cannot be cannot be satisfied using a policy, you can use an Identity Update batch job to "turn on" a temporary profile for a specified duration, and then "turn off" that profile by replacing it with a permanent profile. If the temporary profile is used repeatedly in a predictable manner, you can create a repeating schedule.

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

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

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

To create an Identity Update job specification:

1. Select **My Account** and click the Job Specification tab.
   The Job Specification page is displayed.

2. Click the **Add** button.
   The Job Specification dialog box is displayed.

3. In the **Appliance** drop down list, select the appliance on which this job will run.
   Only those appliances previously defined for this system appear in this option list.
   If only one appliance is used for this system (the default), this field is automatically populated.

4. In the **Name** field, enter a name for this batch job.
5. From the **Type** drop down list, select **Identity Update**.
   After you select the job type, more options are displayed.
• From the **Group** drop down list, select the group of identities that you want to change.

• From the **Identity Profile** drop down list, select the identity profile that you want to apply to the group. If you are applying a temporary profile, this is the "on" profile.

• From the **Off Identity Profile** drop down list, select the identity profile to be applied if you want an identity profile applied temporarily (that is, you want the identity profile to expire).

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

6. Click **Next** to continue.

   The Job Specification - Schedule dialog box is displayed.

7. From the **Repeat** drop down list, select how often this batch job is run. Then specify the time you want the profile to be applied. If you selected an Off Identity Profile, you also specify when the Off profile is applied.

   • **Once** — The batch job is run once. Click the **On** and **Off** fields to display the calendar and select a specific date and time.

   • **Hourly** — The batch job is run at the same minute of every hour. Enter the minute when the batch job is run at each hour. For example, if you want the job to run at 1:30, 2:30, etc. then you would enter 30.

   • **Daily** — The batch job is run every day at the same time. Enter the specific time when the job is run in 24 hour time format.

   • **Weekly** — The batch job is run each week on the same day and time. Select the check box for each day the job will run, and enter the specific time in 24 hour format.

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

8. Click **Next**.

   A summary is displayed.

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

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

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

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

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

Scenarios to apply a door template to a group of doors include:
To apply a set of standard settings. When you have many doors defined with non-standard settings, create a group containing doors and a new template containing the standard settings. Then apply the new template to the group of doors.

To apply modified settings in a commonly used door template. After you make changes to a door template, the identities created from the door template are not automatically updated. You need to create a batch job to apply these changes. Create a group of all the doors that were created using this template, and then apply the modified template to that group. If the template is frequently modified, you can create a repeating schedule.

To apply a template temporarily to a group. When you have doors that require a different template for a short time that cannot be cannot be satisfied using a policy, you can use an Identity Update batch job to "turn on" a temporary template for a specified duration, and then "turn off" that template by replacing it with a permanent template. If the temporary template is used repeatedly in a predictable manner, you can create a repeating schedule.

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

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

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

To create a Door Update job specification:

1. Select **My Account** and click the Job Specification tab.
   The Job Specification page is displayed.

2. Click the **Add** button.
   The Job Specification - General dialog box is displayed. All options marked with * are required.

3. In the **Appliance** drop down list, select the appliance on which this job will run.
   Only those appliances previously defined for this system appear in this option list.
   If only one appliance is used for this system (the default), this field is automatically populated.

4. In the **Name** field, enter a name for this batch job.

5. From the **Type** drop down list, select **Door Update**.
   After you select the job type, additional options are displayed.
- From the **Group** drop down list, select the group of doors that you want to change.
- From the **Door Template** drop down list, select the door template that you want to apply to the group.
- From the **Off Door Template** drop down list, you have the option to select to an alternative door template when the first door template expires.
- From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.

6. Click **Next** to continue.

The Job Specification - Schedule dialog box is displayed.

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

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

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

8. Click **Next**.

A summary is displayed.

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

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

### Scheduling a Global Action

Perform this procedure to schedule global actions.

**NOTE:** The global actions must be created before they can be scheduled. If the required global actions have not been created, contact your System Administrator.
1. Select My Account and click the Job Specification tab.
   The Job Specification page appears.

2. Click the Add button.
   The Job Specification dialog box is displayed.

3. In the Appliance drop down list, select the appliance on which this job will run.
   Only those appliances previously defined for this system appear in this option list.
   If only one appliance is used for this system (the default), this field is automatically populated.

4. In the Name field, enter a name for this batch job.

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

6. Click Next to continue.

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

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

8. Click Next.
   A summary is displayed.
9. Click **Submit** to create this job.

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

### Setting Batch Door Modes

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

1. Select ➡️ **My Account** and click the Job Specification tab.
   
The Job Specification page appears.

2. Click the ✈️ **Add** button.
   
The Job Specification dialog box is displayed.

3. In the **Appliance** drop down list, select the appliance on which this job will run.
   
   Only those appliances previously defined for this system appear in this option list.
   
   If only one appliance is used for this system (the default), this field is automatically populated.

4. In the **Name** field, enter a name for this batch job.

5. From the **Type** drop down list, select **Door Mode**.
   
   After you select the job type, additional options are displayed.
   
   - From the **Available** list, select the required doors then click ⬅️ to add it to the **Members** list.
   - From the **On Door mode** drop down list, select the door mode that you want to apply to the selected doors.
   - From the **Off Door mode** drop down list, select the door mode that you want to apply to the doors when the On action is complete.
   - From the **Output Format** drop down list, select the format for the report that is generated when the job is complete.
   - Select the **Activate** check box to make the door modes active.

6. Click **Next** to continue.

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

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

8. Click **Next**.

A summary is displayed.

9. Click **Submit** to create this job.
Permissions and Rights

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

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Events page</td>
<td>System Summary Listing</td>
</tr>
<tr>
<td></td>
<td>System Summary Screen Refresh</td>
</tr>
<tr>
<td></td>
<td>System Summary Get Layout</td>
</tr>
<tr>
<td></td>
<td>System Summary Update Layout</td>
</tr>
<tr>
<td></td>
<td>Monitor Listing</td>
</tr>
<tr>
<td></td>
<td>Monitor Notes Show</td>
</tr>
<tr>
<td></td>
<td>Monitor Instructions Show</td>
</tr>
<tr>
<td></td>
<td>Monitor Identity Show</td>
</tr>
<tr>
<td>Search for events</td>
<td>Spork Listing</td>
</tr>
<tr>
<td></td>
<td>Spork Search</td>
</tr>
<tr>
<td></td>
<td>Monitor/Search Filters Save</td>
</tr>
<tr>
<td></td>
<td>System Summary Get Layout</td>
</tr>
<tr>
<td></td>
<td>System Summary Update Layout</td>
</tr>
<tr>
<td>View Alarms</td>
<td>Alarm Monitor Listing</td>
</tr>
<tr>
<td></td>
<td>Monitor Notes Show</td>
</tr>
<tr>
<td></td>
<td>Monitor Instructions Show</td>
</tr>
<tr>
<td></td>
<td>Alarms Code Photo</td>
</tr>
<tr>
<td></td>
<td>Monitor View Actions</td>
</tr>
<tr>
<td></td>
<td>Maps-Alarms Show</td>
</tr>
<tr>
<td>Respond to alarm activity</td>
<td>Alarm Monitor Acknowledge</td>
</tr>
<tr>
<td></td>
<td>Alarm Monitor Clear</td>
</tr>
<tr>
<td></td>
<td>Alarms Create Notes</td>
</tr>
<tr>
<td></td>
<td>Alarm Monitor Acknowledge All</td>
</tr>
<tr>
<td></td>
<td>Alarm Monitor Clear All</td>
</tr>
<tr>
<td>View verifications</td>
<td>Swipe &amp; Show</td>
</tr>
<tr>
<td>Permissions</td>
<td>Rights</td>
</tr>
<tr>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>Swipe &amp; Show Get Doors</td>
<td>Monitor Listing</td>
</tr>
<tr>
<td>Swipe &amp; Show Get Door Name</td>
<td>Monitor Panels Status</td>
</tr>
<tr>
<td>Get Photo</td>
<td>Monitor Periodic Update</td>
</tr>
<tr>
<td>Monitor Identity Show</td>
<td>Monitor Appliance Status</td>
</tr>
<tr>
<td>System Summary Get Layout</td>
<td></td>
</tr>
<tr>
<td>System Summary Update Layout</td>
<td></td>
</tr>
</tbody>
</table>

**View the status of assigned hardware**

- Monitor Listing
- Monitor Panels Status
- Monitor Periodic Update
- Monitor Appliance Status

**Control assigned hardware**

- Doors Grant
- Doors Disable
- Doors Unlock
- Doors Lock
- Doors Restore
- Doors Mask Held
- Doors Mask Forced
- Doors Unmask Held
- Doors Unmask Forced

**View and monitor status on assigned maps**

- Maps Monitor Listing
- Maps Show
- Maps Show Generate Image
- Maps Show Image
- Maps View Listing
- Maps Trace
- Mustering Dashboard Drill-Down

**View the intrusion status**

- Monitor Intrusion Panel Status

**Control the assigned intrusion panels**

- Intrusion Panel Master Instant Arm
- Intrusion Panel Master Delay Arm
<table>
<thead>
<tr>
<th>Permissions</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion Panel Master Force Instant Arm</td>
<td>Permission Panel Master Force Instant Arm</td>
</tr>
<tr>
<td>Intrusion Panel Master Force Delay Arm</td>
<td>Permission Panel Master Force Delay Arm</td>
</tr>
<tr>
<td>Intrusion Panel Perimeter Instant Arm</td>
<td>Permission Panel Perimeter Instant Arm</td>
</tr>
<tr>
<td>Intrusion Panel Perimeter Delay Arm</td>
<td>Permission Panel Perimeter Delay Arm</td>
</tr>
<tr>
<td>Intrusion Panel Perimeter Force Instant Arm</td>
<td>Permission Panel Perimeter Force Instant Arm</td>
</tr>
<tr>
<td>Intrusion Panel Perimeter Force Delay Arm</td>
<td>Permission Panel Perimeter Force Delay Arm</td>
</tr>
<tr>
<td>Intrusion Panel Away Arm</td>
<td>Permission Panel Away Arm</td>
</tr>
<tr>
<td>Intrusion Panel Force Away Arm</td>
<td>Permission Panel Force Away Arm</td>
</tr>
<tr>
<td>Intrusion Panel Disarm</td>
<td>Permission Panel Disarm</td>
</tr>
<tr>
<td>Intrusion Panel Silence</td>
<td>Permission Panel Silence</td>
</tr>
<tr>
<td>Intrusion Point Bypass</td>
<td>Permission Intrusion Point Bypass</td>
</tr>
<tr>
<td>Intrusion Point Unbypass</td>
<td>Permission Intrusion Point Unbypass</td>
</tr>
<tr>
<td>Intrusion Output Activate</td>
<td>Permission Intrusion Output Activate</td>
</tr>
<tr>
<td>Intrusion Output Deactivate</td>
<td>Permission Intrusion Output Deactivate</td>
</tr>
<tr>
<td>View live and recorded video</td>
<td>Cameras Show</td>
</tr>
<tr>
<td></td>
<td>Monitor Cameras Show</td>
</tr>
<tr>
<td></td>
<td>Camera Show Video</td>
</tr>
<tr>
<td>Add new identities. Cannot update fields after initial identity setup</td>
<td>Identities My Account</td>
</tr>
<tr>
<td></td>
<td>Identities Listing</td>
</tr>
<tr>
<td></td>
<td>Identities Show</td>
</tr>
<tr>
<td></td>
<td>Identities Advance Search</td>
</tr>
<tr>
<td></td>
<td>Identities Date Search</td>
</tr>
<tr>
<td></td>
<td>Identity Profiles Listing</td>
</tr>
<tr>
<td></td>
<td>Identity Profiles Show List</td>
</tr>
<tr>
<td></td>
<td>Identity Profiles Show List</td>
</tr>
<tr>
<td></td>
<td>Identity Profiles Populate Values</td>
</tr>
<tr>
<td>Add, modify, and update available roles</td>
<td>Identities Roles List</td>
</tr>
<tr>
<td>Permissions</td>
<td>Rights</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Add, modify, and update tokens</td>
<td>Tokens Listing</td>
</tr>
<tr>
<td></td>
<td>Tokens Show</td>
</tr>
<tr>
<td></td>
<td>Tokens New</td>
</tr>
<tr>
<td></td>
<td>Tokens Create</td>
</tr>
<tr>
<td></td>
<td>Tokens Edit</td>
</tr>
<tr>
<td></td>
<td>Tokens Update</td>
</tr>
<tr>
<td></td>
<td>Tokens Set Free Pass</td>
</tr>
<tr>
<td></td>
<td>Identity Profiles Tokens Listing</td>
</tr>
<tr>
<td>Add and modify groups</td>
<td>Identities Groups List</td>
</tr>
<tr>
<td></td>
<td>Identities Groups Update</td>
</tr>
<tr>
<td>View assigned access permissions</td>
<td>Identities Show Access</td>
</tr>
<tr>
<td></td>
<td>Identity Profiles Show Access</td>
</tr>
<tr>
<td>Capture live photos and save</td>
<td>Identities Image Capture</td>
</tr>
<tr>
<td></td>
<td>Identities Image Save</td>
</tr>
<tr>
<td></td>
<td>Identities Code Image</td>
</tr>
<tr>
<td></td>
<td>Identities Photo Capture</td>
</tr>
<tr>
<td>Add and upload photos</td>
<td>Identities Photo Edit</td>
</tr>
<tr>
<td></td>
<td>Identities Photo Update</td>
</tr>
<tr>
<td></td>
<td>Identities Photo Render</td>
</tr>
<tr>
<td></td>
<td>Identities Upload Photo</td>
</tr>
<tr>
<td>View transactional data</td>
<td>Identities Transactions</td>
</tr>
<tr>
<td>Print and issue badges</td>
<td>Identities Badge Show</td>
</tr>
<tr>
<td></td>
<td>Identities Badge screen</td>
</tr>
<tr>
<td></td>
<td>Identities Print Badge</td>
</tr>
<tr>
<td></td>
<td>Identities Badge Render</td>
</tr>
<tr>
<td></td>
<td>Identities Update Badge Preview</td>
</tr>
<tr>
<td></td>
<td>Identities Update Badge</td>
</tr>
<tr>
<td>View reports</td>
<td>Reports Index</td>
</tr>
<tr>
<td>Permissions</td>
<td>Rights</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Report Show</td>
</tr>
<tr>
<td></td>
<td>Grant Access/Report</td>
</tr>
<tr>
<td></td>
<td>Reports Show Grid</td>
</tr>
<tr>
<td></td>
<td>Reports Custom Reports</td>
</tr>
<tr>
<td>Edit, preview, generate, and delete reports</td>
<td>Reports Edit</td>
</tr>
<tr>
<td></td>
<td>Reports New</td>
</tr>
<tr>
<td></td>
<td>Reports Create</td>
</tr>
<tr>
<td></td>
<td>Reports Get Report Preview</td>
</tr>
<tr>
<td></td>
<td>Reports Quick Report</td>
</tr>
<tr>
<td></td>
<td>Reports Dynamic Criteria</td>
</tr>
<tr>
<td></td>
<td>Reports Destroy</td>
</tr>
<tr>
<td>View account details, batch jobs, and job specifications</td>
<td>Identities MyAccount</td>
</tr>
<tr>
<td></td>
<td>Batch Job Specification Index</td>
</tr>
<tr>
<td></td>
<td>Batch Job Specification New</td>
</tr>
<tr>
<td></td>
<td>Batch Job Index</td>
</tr>
<tr>
<td></td>
<td>View Batch Update Schedules</td>
</tr>
<tr>
<td>Create, edit, and delete batch jobs and job specifications</td>
<td>Batch Job Specification Edit</td>
</tr>
<tr>
<td></td>
<td>Batch Job Specification Activate</td>
</tr>
<tr>
<td></td>
<td>Batch Job Specification PostProcess</td>
</tr>
<tr>
<td></td>
<td>Batch Job Specification JobSpecificationList</td>
</tr>
<tr>
<td></td>
<td>Batch Job Specification Create</td>
</tr>
<tr>
<td></td>
<td>Batch Job Specification Update</td>
</tr>
<tr>
<td></td>
<td>Batch Job Create</td>
</tr>
<tr>
<td></td>
<td>Batch Job New</td>
</tr>
<tr>
<td></td>
<td>Batch Job Update</td>
</tr>
<tr>
<td></td>
<td>Batch Job List</td>
</tr>
<tr>
<td></td>
<td>Batch Job Output</td>
</tr>
<tr>
<td></td>
<td>Custom Report Schedule</td>
</tr>
<tr>
<td></td>
<td>Reset custom UI settings</td>
</tr>
<tr>
<td>Permissions</td>
<td>Rights</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>System Settings</td>
<td>System Settings Localize</td>
</tr>
<tr>
<td></td>
<td>Batch Job Specification Destroy</td>
</tr>
<tr>
<td></td>
<td>Batch Job Destroy</td>
</tr>
</tbody>
</table>