## Contents

- **Introduction** ........................................................................................................................................... 1
  - Browser Support........................................................................................................................................ 1
  - Getting Help ........................................................................................................................................... 1

- **Monitoring Doors, Cameras, and System Resources** ........................................................................ 3
  - Monitoring Cameras ................................................................................................................................ 3
  - Monitoring Multi-Camera Views ............................................................................................................... 4
  - Adding Duty Log Messages to the Activity Log ....................................................................................... 5
  - Live Monitoring Options ........................................................................................................................ 5
  - Monitoring the Activity Log .................................................................................................................... 6
    - Filtering Activity Log Data .................................................................................................................. 6
  - Navigating to a Person Record from the Activity Log ........................................................................... 8
  - About Activity Log Messages ................................................................................................................ 8
    - Times .................................................................................................................................................. 8
    - Names .............................................................................................................................................. 8
    - Numbers ......................................................................................................................................... 8
    - Reset Types ..................................................................................................................................... 9
    - Reason Codes .................................................................................................................................. 9
  - Monitoring Floorplans ........................................................................................................................... 11
  - Using the Home Page ............................................................................................................................. 12
  - Using the Monitoring Desktop ............................................................................................................. 13
    - Activity Log Tab .............................................................................................................................. 13
    - Cameras Tab .................................................................................................................................. 14
    - Camera Views Tab ............................................................................................................................ 14
    - Camera Monitor Tab .......................................................................................................................... 14
    - Floorplans Tab ................................................................................................................................. 15
    - Events Tab ..................................................................................................................................... 15
  - Using the Widget Desktop ...................................................................................................................... 16
    - About the Alarm Workflow Widget ..................................................................................................... 19
    - Changing the Alarm Workflow Widget Properties ............................................................................. 20
    - Monitoring and Resolving Alarms ................................................................................................. 21
  - Granting Passback Grace to Cardholders ............................................................................................. 23
  - Managing Floor Access Using the Elevator Status Widget ................................................................... 23
  - Unlocking Portals and Viewing Their Status ........................................................................................ 25
  - Scheduling Actions for Inputs and Outputs .......................................................................................... 29
  - Selecting Partitions ............................................................................................................................... 30

- **Managing Evacuations** ....................................................................................................................... 31
  - Starting an Evacuation Plan .................................................................................................................. 31
  - Ending an Evacuation Plan ................................................................................................................... 32

- **Managing People Data** ..................................................................................................................... 33
  - Adding People to the System ................................................................................................................ 33
  - Finding and Changing Person Records .............................................................................................. 34
    - Searching for a Person Record ........................................................................................................... 34
  - Editing a Person Record ....................................................................................................................... 36
  - Managing a Person’s Credentials ....................................................................................................... 40
    - Issuing New Credentials ..................................................................................................................... 40
    - Revoking and Disabling Credentials ............................................................................................... 43
Contents

Backup System and Other Utilities ................................................................................................... 78
  Backing Up the Security Database ............................................................................................... 78
  Configuring a NAS (network attached storage): ................................................................. 78
  Configuring an FTP server: ..................................................................................................... 79
  Arming and Disarming Alarm Panels .................................................................................. 80

Where to Go for More Information ................................................................................................. 81

Index ..................................................................................................................................................... 82
## Introduction

This guide is intended for users of the following S2 systems:

- S2 NetBox® and S2 NetBox® Extreme
- S2 Enterprise® Exacta 50 and S2 Enterprise® Exacta 100
- S2 NetBox® VR and S2 NetBox® VR Quatro

The guide provides a printable version of much of the online help that is available for common monitoring and administration tasks.

**Note:** Check the S2 Security website (www.s2sys.com) for updated specifications, lists of supported devices, and software updates.

## Browser Support

For Release 4.6, recommended browsers are:

- Internet Explorer 9 and 11
- Firefox 33 (Firefox 32 is also supported.)
- Safari 6 (Safari 5 is also supported.)

## Getting Help

As you use the system, you can click the Help icon in the header bar to open the help window shown below. The topic displayed in the right pane provides assistance with the page you are currently viewing.

To use help:

- Click the Contents and Search buttons above the navigation pane on the left to switch between the table of contents and the search feature.
• Click the close button to hide the navigation pane. To show it again, click the Contents or Search button.

• In the table of contents, click a book to show or hide its list of topics. Click a topic title to display that topic in the right pane.

• When viewing a topic, click Back to return to the previous topic, click Index to display the help Index, and click Print to print the current help topic.

• To use the search feature, enter the word you want to find and then either click Go or press ENTER. To search for a phrase, enter it in quotation marks.

---

**Note:** If the Highlight search results check box is selected when you perform a search, all instances of the word or phrase you entered will be highlighted in the search results.
Monitoring Doors, Cameras, and System Resources

The Monitor menu contains options for monitoring camera views, entering duty log messages, accessing all live monitoring options, granting passback grace, unlocking portals, and selecting different partitions to monitor.

<table>
<thead>
<tr>
<th>Choose this:</th>
<th>To do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameras</td>
<td>Monitor individual cameras.</td>
</tr>
<tr>
<td>Camera Views</td>
<td>Monitor up to four camera views simultaneously in a quad view.</td>
</tr>
<tr>
<td>Duty Log Entry</td>
<td>Enter duty log comments into the Activity Log.</td>
</tr>
<tr>
<td>Live Monitoring</td>
<td>See options for viewing system activities and floorplans, and for initiating live monitoring sessions.</td>
</tr>
<tr>
<td>Portal Status</td>
<td>Unlock portals and view their status.</td>
</tr>
<tr>
<td>Passback Grace</td>
<td>Grace cardholders from anti-passback violations.</td>
</tr>
<tr>
<td>Select Partition</td>
<td>Select a different partition to monitor, in a multi-partition system.</td>
</tr>
</tbody>
</table>

Monitoring Cameras

Select **Monitor : Cameras**.

On this page you can select any camera defined in the system to monitor a live camera view.

**Note:** For information on monitoring NetVR cameras, see the *NetVR User Guide*.

**To monitor a live camera view:**

1. Select a camera from the Cameras menu.
2. From the **Camera Preset** drop-down list, select the preset position you want to view. (The list automatically shows the selected camera’s presets.)
3. Use the controls described in the following table to review recorded video, aim the camera, move it to its home position, zoom in and out, and adjust the speed of camera movement.
Control: Use to:

Display VCR controls you can use to review recorded video. This control will appear only for video management system (VMS) cameras.

Display PTZ (pan, tilt, zoom) controls.

Move the camera to its preset home position.

Move the camera one step in the direction of the arrow. **Note:** If the camera is connected to a ViconNet, a single click starts the camera movement and a second click is required to stop the camera movement. If the camera moves too quickly for accurate positioning, select a lower speed number from the camera speed drop-down, described below.

Zoom in.

Zoom out.

Select the speed of camera movement: 1 is slowest, 10 is fastest.

**Note:** If the camera does not have PTZ capabilities, or if the home, tilt, pan and zoom URLs have not been set up, these controls will not appear. If the video management system (VMS) does not support variable speed PTZ, the camera speed drop-down will not appear. In addition, the VMS and other factors determine whether the PTZ buttons toggle rather than operate with one click to move one step.

---

**Monitoring Multi-Camera Views**

Select **Monitor : Camera Views**.

On this page you can monitor a quad view, which displays up to four camera views simultaneously.

**Note:** For information on monitoring NetVR multi-camera views, see the NetVR User Guide.

---

**To monitor a multi-camera (quad) view:**

1. Select a camera view from the Camera Views menu.

2. When the quad view appears on the page, click the pane displaying the camera view you want to monitor. A border appears around the pane to indicate that it is selected.

3. Click this control [ ] to display the **Camera Preset** drop-down list and select the preset position you want to view. (The list automatically shows the selected camera’s presets.)
4. Use the controls described in the previous section, Monitoring Cameras, to view recorded video, aim the camera, move it to its home position, zoom in and out, and adjust the speed of camera movement.

Adding Duty Log Messages to the Activity Log

Select Monitor : Duty Log Entry.

To add a duty log message to the Activity Log, you can type the message into a text box or select a preset message, if any have been configured.

To add a duty log message to the Activity Log:

1. Type your message into the Enter duty log message text box.
2. Alternatively, if the Use Duty Log Response drop-down list appears on the page, select a preset message from the list.
3. Click Save.

Notes: To view a duty log message for an entry in the Activity Log, click the clipboard icon that appears at the end of the entry.

When you double-click an Activity Log entry, a dialog box appears in which you can append a duty log entry to that entry.

Live Monitoring Options

The Monitor: Live Monitoring menu contains options for viewing system activities and floorplans, and for initiating live monitoring sessions.

<table>
<thead>
<tr>
<th>Choose this:</th>
<th>To do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Log</td>
<td>View recent entries in the log of system activity.</td>
</tr>
<tr>
<td>Floorplans</td>
<td>View the state of alarms and other system resources on a floorplan.</td>
</tr>
<tr>
<td>Home Page</td>
<td>View a full system summary (available in selected versions of the security management system).</td>
</tr>
<tr>
<td>Monitoring Desktop</td>
<td>Use a familiar fixed display to view system information.</td>
</tr>
<tr>
<td>Widget Desktop</td>
<td>Use a custom real-time display to view system information.</td>
</tr>
</tbody>
</table>
Monitoring the Activity Log

Select **Monitor : Live Monitoring : Activity Log**.

**Note:** You can also view the Activity Log on the Monitoring Desktop, in the Activity Log widget on the Widget Desktop, and in the Activity Log Widget on the Home page.

When you first open the Activity Log page, it displays 301 of the most recent entries in the log of system activity. If you remain on the page, additional entries appear in the list, until up to 1,000 of the most recent entries are displayed.

If an administrator or monitor has added a duty log message to an entry, you can click the clipboard icon ( ) to view the message. If there is recorded video associated with an entry, you can click the camera icon ( ) to view the recording.

Filtering Activity Log Data

When monitoring system activity in the Activity Log, you can filter the current list of log entries to focus on specific information. There are two types of filters you can apply:

- **Text filters:** In an Activity Log tab (displayed on the Monitoring Desktop) or an Activity Log widget (displayed on the Monitoring Desktop, Home page, or Widget Desktop), you can apply a text filter to view only entries from the original list that contain a specific text string.

  **Note:** Text filters are not available in the full page view of the Activity Log.

- **Category filters:** In an Activity Log tab or widget, and also in the full page view of the Activity Log, you can apply a category filter to view only entries from the original list that belong to a particular category.

You can also combine a text filter with a category filter. For example, suppose that after applying the text filter “Jean Gauthier,” you apply the category filter Access Denied to the results. The new results will show only denied access requests for the cardholder Jean Gauthier.

  **Note:** If filters were not enabled when an Activity Log widget was created, that instance of the widget will not have text and category filtering capabilities.

  Your filtered results will include only entries currently defined for the view of the Activity Log you are monitoring. For example, in an Activity Log widget that is configured to display only "Access denied" entries, applying the Access Granted category filter will return no results.
Applying Text Filters

To apply a text filter, you type text into the Filter box that appears in the upper right corner of the Activity Log tab or widget. The results will include only entries from the original list containing text matching your entry. Text filtering is not case-sensitive; you can enter either uppercase or lowercase characters.

For example, to see only entries containing the name “Jean Gauthier,” apply the filter shown below.

Filter: Jean Gauthier

Filtering begins as you start to type. The filtered data will be displayed in the Activity Log until you click the Clear Filters icon, enter a different text filter, or ending the current monitoring session.

Applying Category Filters

To apply a category filter, you select an entry from the Category drop-down list in the upper right corner of the Activity Log page, tab, or widget. The results will include only entries from the original list that belong to the selected category. The following categories are available:

- **All** (default): Select when you want to remove the currently applied category filter without applying a new one, and without removing the current text filter if one is applied. (Clicking the Clear Filters icon clears all category and text filters.)
- **Access Control**: Select to view only access control related entries, such as Access Denied, Access Granted, Forced Open, Relocked, Timed Unlock Expired, and Unlock entries.
- **Alarms and Events**: Select to view only alarm and event related entries, such as Alarm Acknowledged, Alarm Actions Cleared, Alarm Adopted, Alarm Panel Armed, Event Actions Cleared, Event Triggered, and Tamper Alarm entries.
- **Threat Levels**: Select to view only threat level related entries, such as Threat Level Set, Threat Level Set (ALM), and Threat Level Set (API) entries.
- **System Administration**: Select to view only system administration related entries, such as FTP Backup Complete, FTP Backup Failed, Log Archive Failed, Logged In, Logged Out, and System Backup Successful entries.
- **Devices**: Select to view only device related activity, such as Battery Failed, Blade Not Responding, Intrusion Panel Alarm, NAS Backup Complete, and Secondary System Restored events.
- **Network Nodes**: Select to view only Network Node related entries, such as Coproc Not Responding, NN Connected, NN Startup, and NN Timeout, entries.
- **Access Granted**: Select to view only entries for granted access requests.
- **Access Denied**: Select to view only entries for denied access requests.
Once you have applied a category filter, the filtered data will be displayed in the Activity Log until you click the Clear Filters icon, select a different filter, or end the current monitoring session.

**Navigating to a Person Record from the Activity Log**

If you have the right to view a cardholder's person record, clicking that person's name within an Activity Log entry opens a window in which his or her person record is displayed. Any rights you have to view and edit information in a particular person record will apply when you access the record from the Activity Log.

**About Activity Log Messages**

The messages are color coded.

- **Red** indicates a process failure or access control issue.
- **Green** indicates a successful process.
- The color currently selected for Trace person log color on the Network Controller page indicates valid or invalid access attempts in the current partition by individuals whose activity is being traced.
- **Black** is used for all other messages.

Descriptions of the message text and variables included in Activity Log messages follow.

**Times**

Each Activity Log message begins with the controller time—the time when the event was communicated to the Network Controller. Depending on how your system is configured, the controller time might be followed (in square brackets) by the time when the event actually occurred on the node.

**Names**

Specific names entered into the system during setup and configuration will be used in log entries in place of variables such as: <username>, <locationname>, <portalname>, <nodename>, <eventname>, <elevatorname>, <alarmpanel>, and <threatlevel>. This provides a strong reason for assigning names that are descriptive. The log will be much easier to understand.

**Numbers**

Specific numbers will be used in log entries in place of <ipaddress>, <slotnumber>, and <rev>.
Reset Types

Specific `<reset_type>` messages for the “Network Node Ident” log entry include:

- **Power on reset** - The node reset on power up.
- **Watchdog timer reset** - This occurs when the system takes too long to process an operation involving a node. It should restart and continue processing. If the problem persists, contact your system administrator.
- **Normal reset** - Physical reset by pushing the node reset button on the node blade.
- **Network loss** - No reset has occurred. The node lost network connectivity but has now reconnected.

Reason Codes

Specific `<reasoncode>` messages for “Access denied” and “Access granted” log entries are listed below.

**Note:** In addition to “Access denied” and “Access granted” log entries, “Access not completed” entries will appear for access requests that are initiated but not completed. For example, if a user presents his or her credentials at a door but never opens the door, an “Access not completed” entry will appear in the Activity Log.

- **[BIT MISMATCH]** - The data format of this credential does not match any data format configured in the system. Clicking this message code opens the Card Decoder window.
- **[DISABLED]** (or [CLEAR], [DAMAGED], [FORGOTTEN], [LOST], [NOT RETURNED], [NOT VALIDATED], [RETURNED], [STOLEN], or [SUSPENDED]) - This credential has been disabled.
- **[EXPIRED]** - This credential has expired.
- **[HOLIDAY]** - A defined holiday does not allow access for this person at this time.
- **[LOCATION]** - This person's access level or the current threat level does not allow the use of this reader.
- **[MISSING (DISABLED)]** – This credential was reported as missing and is disabled.
- **[NO PIN]** – No PIN was entered within the PIN entry timeout period set on the Network Controller page.
- **[NO ESCORT]** – This person’s Escort Required access level permits access only if the next access request reader comes within 15 seconds, from a cardholder holding an Escort access level.
• [NOT IN NODE] - The node has no record of this credential and was unable to load it in time. The name of the person who owns the credential is displayed.

• [NOT USED] – This credential was disabled after the maximum number of days of non-use specified for your system.

• [PIN] - The PIN entered is incorrect.

• [PASSBACK VIOLATION] - This credential was presented to enter a region where the cardholder is already known to be. (This is a subset of tailgate violations.)

• [TAILGATE VIOLATION] - This credential was presented in a region where the cardholder is known NOT to be.

• [TEMPORARY (EXPIRED)] – This credential was issued as a temporary credential and has expired.

• [TIME] - Time specs do not allow access for this person at this time.

• [THREAT LEVEL] - This person's access level does not allow access under the current threat level.

• [UNKNOWN] - The data format of this credential is valid, but there is no record of the credential anywhere in the system. Clicking this message opens the Card Decoder window.

• [WRONG DAY] - Time specs or holiday definitions do not allow access for this person on this day.

Note: “Access denied” log entries for remote-lockset portals may incorrectly report the [TIME] reason code rather than the [WRONG DAY] REASON CODE. This is because remote locksets do not distinguish between a rejection based on the wrong time of day and a rejection based on the wrong day of the week.

There are two [<reasoncode>] messages for “Access granted” log entries:

• [DURESS] - A cardholder presented his or her card and then entered a duress PIN (his or her assigned PIN, with the last digit incremented by 1) into the keypad. This resulted in an apparently normal access that was actually a duress access.

• [PASSBACK] - A cardholder presented credentials that were used previously in this reader group. However, on the person record, the person's Regional anti-passback privileges are set to Exempt or Soft Always, so the person was allowed access and the access was logged.
Monitoring Floorplans

Select **Monitor : Live Monitoring : Floorplans.**

On this page you can:

- View any floorplan that is configured in the system.
- See the locations of system resources such as portals, online remote locksets, cameras, inputs, outputs, and temperature sensors.
- Use a floorplan link to switch to a different floorplan.
- Display temperature graphs for each temperature point.
- Momentarily unlock portals.
- Scheduled extended locks and unlocks of portals.
- Perform scheduled disarming of inputs.
- Perform scheduled activations and deactivations of outputs.
- Display thumbnail images from cameras.
- View the current status of an alarm.

**Note:** Viewing and configuring floorplans requires Version 9.0 or later of Macromedia Flash Player.

**To monitor floorplans:**

1. Select from the **Floorplan** drop-down the floor you want to monitor.
2. Click the icon for any system resource on the floorplan to display its type and name in the **Type** and **Name** text boxes.
   - Selected icons are slightly dimmed on the floorplan.
3. Right-click anywhere on the floorplan to display the Flash Player menu. You can use the options on this menu.
4. Hold down the left mouse button over the icon for a resource to display a menu of the actions you can perform:
   - The menu for a portal lets you perform a momentary unlock or schedule an extended lock or unlock.
   - The menu for a camera lets you select a thumbnail image.
   - The menu for an alarm lets you view its current status.
   - The menu for a floorplan link lets you view its current status and/or display that floorplan.
   - The menu for an input lets you perform a scheduled disarming of the input.
The menu for an output lets you perform a scheduled activation or deactivation of the output.

The menu for a temperature sensor lets you select a temperature graph.

Note: Whenever there is a valid entry at a portal, the cardholder’s name appears below the icon for that portal. Whenever an event is triggered, the icon for that alarm turns red.

5. You can click on an input icon or an output icon and select Schedule Action.
6. You can click on a camera icon and select a thumbnail image.
7. You can click on a temperature icon and select a temperature graph.
8. Alarm icons turn red if that event is triggered.

Using the Home Page


The Home page, which is available in selected versions of the security application, provides a layout for viewing full system information using an Activity Log, Auto-Monitor, Video Stream, and User Tasks widget for direct access to these functions. You can click the button provided to make this your start page.

Note: Opening the Home page automatically hides the Table of Contents. To display it again, click Show TOC in the header bar.

On the Home page, you can:

- Use the Activity Log widget to view recent entries in the log of system activity.

- Use the Auto-Monitor widget to view issues that might require attention. This widget displays notifications of all currently active events of the following types: Unacknowledged Events, Node Communication Loss, Door Forced Open, and Door Held Open. It also displays all Access Denied events that have occurred within the last hour. Pointing to a notification displays an informational tooltip showing more detail about each event.

- Use the Video Stream widget to monitor a camera view. The first camera in your system's Camera Menu order will appear by default in this widget. If there are no camera definitions in the system, the Video Stream widget will not display a camera view.

- Use the User Tasks widget for direct access to common features (based on your login permissions). Clicking the icon for a task takes you directly to the page for performing the task. For example, if you have Administrator access, clicking the People
Locator takes you to a page where you can run searches to find people in the system.

Using the Monitoring Desktop


The Monitoring Desktop provides a fixed layout for viewing dynamic system information. It has separate tabbed pages for monitoring various system functions, such as events, camera views, and floorplans.

To use a fixed display to monitor all system activities:

1. In the upper left pane, click either the Events or Activity Log tab, depending on the type of system information you want to view in that pane.

   **Note**: The Events tab displays all currently active system events. Events can be sorted on the Date/Time, Priority, Name, or Commands column.

2. In the lower left pane, click the Activity Log, Cameras, Camera Views, Camera Monitor, Floorplans, or Events tab, depending on the type of information you want to view in that pane.

3. Use the windows on the right side of the desktop to view the current threat level, unlock portals, view cameras, and view a recent history of cardholders who have presented their credentials to readers in the system.

   **Note**: Two links appear in the upper right corner of the Monitoring Desktop. You can use the tearoff link to open the Monitoring Desktop in a separate window, so you can continue to use it as you work with other pages in the application. If you have a Generation 1 Dedicated Micros DVR integration, you can use the setup video link to determine whether the version of Java available in your browser will work with the DVR, and to update Java if necessary.

Activity Log Tab

The Activity Log tab displays recent entries in the log of system activity. For more information, see Monitoring the Activity Log on page 6.
Cameras Tab

You can select any camera defined in the system to monitor a live camera view. For more information, see Monitoring Cameras on page 3.

Camera Views Tab

You can monitor a multi-camera (quad) view, which displays up to four camera views simultaneously. For more information, see Monitoring Multi-Camera Views on page 4.

Camera Monitor Tab

The Camera Monitor tab is for use on systems that are not integrated with NetVR. By adding a camera to this tab, you can designate it as the camera monitor.

The camera monitor can accept camera views and recorded video from other cameras, and it can be used for event-driven video or event replay. For example, you can configure a single camera monitor to switch to events as they occur.

To designate a camera as the camera monitor:

1. In the Cameras widget on the right side of the page, point to this icon above the camera you want to select:

   ![Camera Icon]

   The icon changes to this button:

   ![Camera Monitor Icon]

2. Click the button to bring the Camera Monitor tab forward and display the video stream or image from that camera.

You can use the controls described in the following table to review recorded video, aim the camera, move it to its home position, zoom in and out, and adjust the speed of camera movement.
### Control:

<table>
<thead>
<tr>
<th>Control</th>
<th>Use to:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Display VCR controls" /></td>
<td>Display VCR controls you can use to review recorded video. This control will appear only for video management system (VMS) cameras.</td>
</tr>
<tr>
<td><img src="image" alt="Display PTZ controls" /></td>
<td>Display PTZ (pan, tilt, zoom) controls.</td>
</tr>
<tr>
<td><img src="image" alt="Move camera" /></td>
<td>Move the camera to its preset home position.</td>
</tr>
<tr>
<td><img src="image" alt="Move camera one step" /></td>
<td>Move the camera one step in the direction of the arrow. <strong>Note:</strong> If the camera is connected to a ViconNet, a single click starts the camera movement and a second click is required to stop the camera movement. If the camera moves too quickly for accurate positioning, select a lower speed number from the camera speed drop-down, described below.</td>
</tr>
<tr>
<td><img src="image" alt="Zoom in" /></td>
<td>Zoom in.</td>
</tr>
<tr>
<td><img src="image" alt="Zoom out" /></td>
<td>Zoom out.</td>
</tr>
<tr>
<td><img src="image" alt="Select speed" /></td>
<td>Select the speed of camera movement: 1 is slowest, 10 is fastest.</td>
</tr>
</tbody>
</table>

**Note:** If the camera does not have PTZ capabilities, or if the home, tilt, pan and zoom URLs have not been set up, these controls will not appear. If the video management system (VMS) does not support variable speed PTZ, the camera speed drop-down will not appear. In addition, the VMS and other factors determine whether the PTZ buttons toggle rather than operate with one click to move one step.

### Floorplans Tab

You can use the Floorplans tab to monitor any floorplan configured in the system. For more information, see [Monitoring Floorplans](#) on page 11.

**Note:** Viewing and configuring floorplans requires a browser plug-in from Macromedia called Flash Player 9.0 or higher. Your operating system and browser will automatically determine which version of the plug-in to install.

### Events Tab

The active events listed on this tab are sorted in priority order by default. To reverse the sort order, click the **Priority** column header. You can also click the **Date/Time** or **Name** column header to sort on those columns.

An event will appear in the list as long as its cause is still active and/or it requires acknowledgment.
To acknowledge and respond to events:

1. Select **Monitor : Monitoring Desktop**.

2. To investigate and acknowledge an event, you can:
   - If this icon 🎞️ appears in the Name column for an event, click it to view recorded video associated with the event.
   - Click Camera 📹 in the Commands column to view live video for an event.
   - Click Details 📋 in the Commands column to view the **Operator long message** entered in the event definition.
   - Click Acknowledge ✅ in the Commands column to acknowledge the event. Otherwise, it will remain active until all actions triggered by the event are concluded, or the **Maximum Duration** specified in the event definition elapses and the event auto-acknowledges.
   - Click Clear 🗑️ to clear all active actions triggered by the event. This button will appear for an event only if both **Allow Clear Actions** and **While Active?** are both selected in the event definition.

Using the Widget Desktop

Select **Monitor : Live Monitoring : Widget Desktop**.

The Widget Desktop provides a custom real-time display for monitoring the system. When you open the Widget Desktop, you see one or more windows, called **widgets**, arranged in the default layout for your system. Each widget has a special function, such as displaying system activity, unlocking portals, or delivering real-time web content from another system.

**Note**: Internet Explorer 7 or higher is required for optimal viewing of the Widget Desktop. Page display problems occur when the Widget Desktop is viewed in other browsers or other versions of Internet Explorer.

**Summary of Available Widgets**

When you load a Widget Desktop layout, the widgets you see will depend on the way the layout was set up. If a particular widget is included in the layout by default, you can add it for the current monitoring session by selecting it from the Desktop menu in the lower left corner of the page. If a widget has a close button in its upper right corner, you can click the button to remove the widget from the layout for the current monitoring session.

The widgets that may be available for a given layout are (see the online help for details):

- **Activity Log**
- **Alarm Workflow**
- **Auto-Monitor**
Monitoring Doors, Cameras, and System Resources

- Camera View
- Clock
- Duty Log Entry
- Elevator Status
- Events
- Explorer
- Floorplans
- Intrusion Panel
- Passback Grace
- Photo ID History
- Portal Status
- Portal Unlock
- Statistics Block
- Status
- Threat Level

If the default Widget Desktop layout does not meet your needs, you can select a different layout if others are available. You can also customize a layout for the current monitoring session, by adding available widgets and selecting a different background. See the online help for details about available widgets.

**Note:** Changes you make to a layout are not saved across monitoring sessions. Once you close the Widget Desktop, the layout reverts to its original appearance. If you need a custom layout, and you do not have setup privileges in the active partition, see your security administrator for assistance. If you do have setup privileges in the active partition, you can switch to Compose mode, edit and save the current layout or any available layout, then switch back to monitoring mode. See *Using the Widget Desktop* in the online help for more information.

You may also be able to change the individual widgets in a layout, depending on how it was set up. For example, you may be able to:

- Move, size, minimize, and close a widget.
- Change a widget's unique properties.
- Change the scope of the data displayed in a widget.
Note: If a grid is displayed on the desktop background, widgets will automatically align to the nearest intersection of lines in the grid whenever you move or resize them.

To display the default Widget Desktop layout:
• Select Monitor : Live Monitoring : Widget Desktop. The default Widget Desktop layout appears automatically.

To select a different layout:
1. Select Load Layout from the Desktop menu in the lower left corner of the page.
2. In the Load Layout dialog box, select the layout you want, and then click OK.
3. To return to the default layout at any time, select Default from the Load Layout dialog box.

To add a widget to the selected layout:
• Click Desktop in the lower left corner of the page to display the Desktop menu.

• Select the widget you want to add.

To select a different partition to monitor:
1. Click the name of the current partition on the lower right edge of the page.
2. In the Switch Partition dialog box, select the partition you want to monitor.
3. Click OK.
   The partition you selected becomes the current partition until you select a different one.

To change the Widget Desktop background:
• Right-click anywhere on the background, select a number from the Background drop-down, and then click OK.

To make the Widget Desktop your start page:
• Select Make This My Start Page from the Desktop menu in the lower left corner of the page. The next time you log in to the system, your default Widget Desktop layout will be displayed automatically.

Note: Your default Widget Desktop layout is the one that is currently selected on the Login tab of your person record.
To get Help from the Widget Desktop:

- Click the information icon 🔄 in the lower right corner of the page.

To switch to Compose mode:

1. If you have setup privileges in the active partition, click Compose Mode from the Desktop menu in the lower left corner of the page.

   To the right of the Desktop menu, you will now see the word “Compose” and property sheets for changing the Desktop menu, layout properties, and default widget properties for the selected layout:

   ![Compose Mode](image)

2. Make any changes you want to the current layout, or any available layout, and then save the layout.

3. When you have finished, select **End Compose Mode** from the Desktop menu to return to monitoring mode, or select **Exit** from the menu to return to the Main Menu.

To exit the Widget Desktop:

- Select Exit from the Desktop menu in the lower left corner of the page to return to the main menu.

About the Alarm Workflow Widget

If the creator of a Widget Desktop layout has made the Alarm Workflow widget available, you can use it to monitor and resolve alarms.

Depending on how the Alarm Workflow widget was configured for the current layout, it will show alarms from the current partition only, from selected partitions, or from all partitions.

There is an **Operator is present** check box in the upper left corner of the Alarm Workflow widget. You can select or clear this check box to indicate your current availability for handling alarms in the partitions you are viewing. Depending on how the alarm workflow feature was implemented for your system, alarms might behave differently when this check box is selected than when it is clear.

The Alarm Workflow widget includes two views for managing alarms. The **Offered Alarms** view includes alarms that are unowned or are owned by another operator. The **My Alarms** view includes alarms that are owned by you. The following information appears for each alarm:

- **Priority/Color**: The priority and color specified for alarms in the event definition. The column header will display either a P or a C, depending on whether the column is currently set to sort by priority or by color.

- **Date/Time**: The date and time the alarm was triggered.

- **Partition**: The partition in which the alarm occurred.
• **Name**: The name of the event.

• **Policy**: The alarm workflow policy selected in the associated event definition. This policy determines the conditions under which the alarm will be moved from its initial Active state to the Escalated state and from the Escalated state to the Urgent state.

• **Owner** (Offered Alarms view only): The current owner of the alarm. For example, if the alarm has no owner, `<Unassigned>` appears in this column.

• **State**: The current state of the alarm. If there is a timer associated with the current alarm state, a progress bar indicates the number of seconds remaining before the timer expires. The progress bar is green for the first half of that time period and yellow for the remaining half.

The Offered Alarms and My Alarms views are separated by a splitter bar, shown in the following figure, which you can use to change the amount of vertical space each view occupies within the widget.

Click the middle of the bar to collapse or expand the Offered Alarms view.

Drag either side of the bar up and down to change the relative view heights.

---

**Note**: By default, the alarms in each view are sorted by priority. To reverse the sort order, click the priority (P) column header. Arrows indicating the current sort order appear in the header. To sort the view on a different column, click that column header.

### Changing the Alarm Workflow Widget Properties

If the creator of the Widget Desktop layout has made the Alarm Workflow widget configurable, you can change its common properties and its scope properties. You can also specify the following unique properties for the widget:

• **Priority sorting method**: Select the sorting method used to sort alarms on the Priority/Color column.
  - Sort by priority: With this setting, alarms are sorted according to their priority numbers.
  - Sort by color: With this setting, alarms are sorted according to their colors.

• **Update progress bar every**: Select the frequency (1, 2, 5, or 10 seconds) with which progress bars displayed in the State column.
Monitoring and Resolving Alarms

When the Alarm Workflow widget is available in a Widget Desktop layout, you can use it to monitor and resolve alarms. You can:

- Indicate your presence and availability for handling alarms
- Add a duty log entry for selected alarms
- Adopt selected alarms
- Clear actions for selected alarms
- Acknowledge selected alarms

To indicate your presence:

- To indicate that you are available to handle alarms, select the Operator is present check box in the upper left corner of the widget.

You can select or clear this check box to indicate your current availability for handling alarms in the partitions you are viewing. Depending on how the alarm workflow is configured for your system, alarms might behave differently when this check box is selected than when it is clear.

To add a duty log entry for selected alarms:

1. In the Offered Alarms or My Alarms view, select each alarm to which you want to add a duty log message.
2. Click the Add Duty Log button.
   
   Tip: Right-clicking an alarm listed in the My Alarms view both selects it and displays a menu from which you can select Add Duty Log.

3. In the Duty Log Entry dialog box, enter your duty log message and click Save.

   A duty log entry is added to the Activity Log for the selected alarms. Monitors will be able to click a clipboard icon in the entry to view your message.

To adopt selected alarms:

1. In the Offered Alarms view, select each alarm for which you want to take ownership.
2. On the Ownership Options drop-down list, select one of the following options:
   - Adopt Alarm: Moves the selected alarms to the My Alarms view.
   - Adopt and Acknowledge: Moves the selected alarms to the My Alarms view and acknowledges them. Note that acknowledging an alarm does not resolve it, unless the cause of the alarm is no longer active.
Monitoring Doors, Cameras, and System Resources

- **Adopt and Clear Actions**: Moves the selected alarms to the My Alarms view and clears all active actions for the alarms.

  **Tip**: Right-clicking an alarm listed in the Offered Alarms view both selects the alarm and displays a menu from which you can select any of the ownership options listed above.

3. If you are prompted, click **Yes** to confirm that you want to perform all selected actions, or click **No** to cancel all actions.

**Note**: The **Allow Clear Actions** settings for an event will determine whether a Clear Actions request will have an effect on its associated actions.

### To clear actions for selected alarms:

1. In the **My Alarms** view, select each alarm for which you want to clear active actions.

2. Click **Clear Actions**.

   **Tip**: Right-clicking an alarm listed in the **My Alarms** view both selects it and displays a menu from which you can select **Clear Actions**.

3. If you are prompted, click **Yes** to confirm that you want to perform all selected actions, or click **No** to cancel all actions.  

   If you click **Yes**, all active actions are cleared for every selected alarm, regardless of the view in which it appears.

**Note**: The **Allow Clear Actions** settings for an event will determine whether a Clear Actions request will have an effect on its associated actions.

### To acknowledge selected alarms:

1. In the **My Alarms** view, select each alarm you want to acknowledge.

2. Click **Acknowledge**.

   **Tip**: Right-clicking an alarm listed in the **My Alarms** view both selects it and displays a menu from which you can select **Acknowledge**.

3. If you are prompted, click **Yes** to confirm that you want to perform all selected actions, or click **No** to cancel all actions.  

   If you click **Yes**, every selected alarm is acknowledged, regardless of the view in which it appears. Note that acknowledging an alarm does not resolve it, unless the underlying cause of the alarm is no longer active.
Granting Passback Grace to Cardholders

Select Monitor : Passback Grace.

On this page, system users with at least an Administration user role can grant passback grace to cardholders. When a cardholder is “graced,” the person's next card read is allowed, no violations are triggered, and the person is moved to the region specified by the Auto-passback Grace to Region setting on the Network Controller page. Thereafter, all anti-passback rules are in effect, as before.

**Note:** A system user with only a Monitor user role can also grace cardholders, if both of following settings are selected on the Network Controller page: The monitoring role can grant passback grace and Show Region and Passback Grace info in the Roster and People reports.

To grant passback grace to cardholders:

1. In the search form, select the region in which you want to search, and enter sufficient additional data to find the people you want to grace.
2. Click Search.  
   A report containing the search results is displayed below the form. The report shows each person's name and current location.
3. To grace an individual cardholder, click the Grace button for that person. To grace all cardholders listed in the report, click the Grace all shown button.

**Note:** A Grace pending button appears for any cardholder who does not require passback grace—such as a person who was just added to the system and is still in the Uncontrolled Space region.

Managing Floor Access Using the Elevator Status Widget

When the Elevator Status widget is displayed on the Widget Desktop, you can use it to review the current status and free-access schedule for floor-select buttons in elevators you have permission to view.

If your user role gives you the Free Access privileges for an elevator group, you can also use the widget to manage access to any elevator in that group. You can:

- Momentarily enable free access for a floor-select button. This will allow people temporary access to the floor without valid credential reads.
- Schedule an extended period of free access or controlled access for a floor-select button. This will allow people either free access to the floor, or access via valid credential reads, for the period of time you specify.
To momentarily enable free access for a floor plan button:
1. In the list of elevators, locate the elevator and floor.
   The output corresponding to the floor-select button for that elevator/floor combination appears in the Door column.
2. Click **Momentarily Enable Free Access**.
   The floor-select button enters the free access state immediately and remains in that state for the button activation time configured in the elevator definition.

To schedule an extended period of time of free access or controlled access for a floor-select button:
1. In the list of elevators, locate the elevator and floor.
   The output corresponding to the floor-select button for that elevator/floor combination appears in the Door column.
2. Click **Edit Schedule** in the Action column to display a list of scheduled actions for the selected output.
3. To add a scheduled action, click add.
4. In the scheduled Actions dialog box, select **Free Access** or **Controlled Access** from the Action drop-down list.
5. In the Scheduled Actions dialog box, select **Free Access** or **Controlled Access** from the Action drop-down list.
6. For the **Uses Time** setting:
   - Select **System Time** if you want the start and end times to be based on the Network Controller time zone.
   - Select **Local Site Time** if you want the start and end times to be based on the Network Node time zone.
7. To schedule the **Start Time**, select one of the following:
   - **Now**: the Action will start at the current date and time
   - **At**: (selected by default) The action will start at the date and time you enter.
   - **In**: The action will start once the number of specified hours and minutes have elapsed.
8. To schedule the **End Time**, select one of the following:
   - **At**: The action will end at the data and time you enter. Use the format shown for the start time.
   - **After**: The action will end once the number of specified hours and minutes past the action’s start time have elapsed.
9. In the **Comment** box, enter any comments you want to appear in the list of scheduled action for the elevator output.
10. Click **OK** to close the Scheduled Actions dialog box.
Example: Select Free Access and set the start time to Now. Set the end time to After 1:30 (one hour and thirty minutes). Click OK. The floor button will enter the Free Access state immediately and will remain in that state for one hour and thirty minutes.

11. To remove a scheduled action, repeat Step 2, select the action, click delete and click OK.

12. To edit a scheduled action, repeat Step 2, select the action, click edit, make any changes you want in the dialog box, and click OK.

Unlocking Portals and Viewing Their Status

In addition to presenting valid credentials at a portal, there are multiple ways to unlock the portal and view its status:

- Under Monitor : Portal Status, or in the Portal Status Widget, you can:
  - View the current location, status, and unlock schedule of any portal.
  - View the current threat level of any portal whose location has a different threat level than the default location for that partition.
  - Momentarily unlock a portal.
  - Switch a portal to a persistent locked or unlocked state.
  - Disable or enable a portal.
  - Schedule an extended lock or unlock of a portal.

- Under Administration : Schedule Action, or under Monitor : Live Monitoring : Floorplans, you can:
  - Schedule an extended lock or unlock of a portal.
  - You can also schedule the disarming of an input or activation or deactivation of an output. See Scheduling Actions for Inputs and Outputs on page 29.

Note: For more information about using Floorplans, see Monitoring Floorplans on page 11.

You can also unlock a portal by assigning it to a portal group to which an Unlock time spec is assigned. The portal will be unlocked at the start of the period defined by the unlock time spec and re-locked at the end of that time period.

To momentarily unlock a portal:

2. In the Portal column, locate the portal or lockset you want to unlock.
3. Click Momentarily Unlock Portal in the Action column. The portal or lockset unlocks for the unlock time configured in the portal definition.
To switch a portal to a persistent locked or unlocked state:

1. Select **Monitor : Portal Status**.

2. In the Action column, click **Lock Portal** for the portal you want to lock.
   
   The portal locks immediately. It will remain in a locked state until it is
   unlocked again – either manually via the **Unlock Portal** button or a double
   card read, or automatically when any new scheduled action for this portal
   becomes active or any portal group time spec change involving this portal
   occurs. Once the portal has been returned to automatic control by a time spec
   change, any suspended event action defined for the portal is resumed.

3. In the Action column, click **Unlock Portal** for the portal you want to
   unlock.

   The portal unlocks immediately. It will remain in an unlocked state until it is
   locked again – either manually via the **Lock Portal** button or a double card
   read, or automatically when any new scheduled action for this portal
   becomes active or any portal group time spec change involving this portal
   occurs. Once the portal has been returned to automatic control by a time spec
   change, any suspended event action defined for the portal is resumed.

---

**Note:** The **Lock Portal** and **Unlock Portal** buttons are also available in the
Portal Status and Portal Unlock widgets.

To disable or enable a portal:

1. Select **Monitor : Portal Status**.

2. In the Portal column, locate the portal or lockset you want to unlock.

3. To disable the portal, click **Disable Portal** in the Action column. The
   portal is locked and temporarily removed from the system’s control.

4. To enable the portal, click **Enable Portal** in the Action column. The
   portal is returned to the system’s control.

To schedule an extended lock or unlock of a portal:

1. Select **Monitor : Portal Status**.

2. In the Portal column, locate the portal you want to unlock.

3. Click **Edit Schedule** in the Action column to display a list of scheduled
   actions for the selected portal.

4. To add a scheduled action, click the add button 🗓.

5. In the Scheduled Actions dialog box, select **Lock** or **Unlock** from the Action
   drop-down list.

6. For the **Uses Time** setting:
   
   o Select **System Time** if you want the start and end times to be based on
     the Network Controller time zone.
7. To schedule the **Start Time**, select one of the following:
   - **Now**: The action will start at the current date and time (filled in by default).
   - **At**: (selected by default) The action will start at the date and time you enter.
   - **In**: The action will start once the number of specified hours and minutes have elapsed.

8. To schedule the **End Time**, select one of the following:
   - **At**: The action will end at the date and time you enter. Use the format shown for the start time.
   - **After**: The action will end once the number of specified hours and minutes past the action's start time have elapsed.

9. In the **Comment** box, enter any comments you want to appear in the list of scheduled actions for the portal.

10. When you have finished, click **OK** to close the dialog box.

   **Example**: Select **Unlock** and set the **Start Time** to **Now**. Set the **End Time** to **After** 1:30 (one hour and thirty minutes). Click **OK**. The portal will unlock immediately and stay unlocked for one hour and thirty minutes.

11. To remove a scheduled action, repeat step 2, select the action, click the delete button, and click **OK**.

12. To edit a scheduled action, repeat step 2, select the action, click the edit button, make any changes you want in the dialog box, and click **OK**.

---

**Note**: If a threat level group is selected under Portal Policies in the portal’s definition, threat level changes at the portal’s location might override a scheduled unlock currently in effect for the portal.

---

**To schedule an extended lock or unlock from the Schedule Action page:**

1. Select **Administration : Schedule Action**.

2. Click the **Schedule** link for the portal for which you want to schedule an action. A **Scheduled Action** dialog box appears.

3. In the **Action** column, select **Lock** or **Unlock**.

   **Note**: Do not unlock a portal by scheduling an action for its lock output. This could create an alarm condition, because the portal may be opened without a valid card read.

4. In the **Start Date/Time** column, select one of the following:
o Now: (the default setting) The action will start at the current date and time.

o At: The action will start at the date and time you specify.

o In: The action will start once the number of specified hours and minutes have elapsed.

5. In the **End Date/Time** column, select one of the following:

   o At: The action will end at the date and time you enter. Use the format shown for the Start Date/Time.

   o After: The action will end once the number of specified hours and minutes past the action's start time have elapsed.

6. Under **Use**, select either **Local Site Time** or **System Time**.

   When you select **Local Site Time**, the time specs for the selected action will be based on the time zone set for the local Network Node. When you select **System Time**, the time specs will be based on the time zone set for the Network Controller.

7. Click **Save**.

---

**Note:** If a threat level group is selected under Portal Policies in the portal’s definition, threat level changes at the portal’s location might override a scheduled unlock currently in effect for the portal.

---

### To schedule an extended lock or unlock from a floorplan:

1. Select **Monitor : Live Monitoring : Floorplans**.

2. Select a floorplan from the **Floorplan** drop-down menu.

3. Hold down the left mouse button on the icon for a portal and select **Schedule Action** from the popup menu. A **Scheduled Action** dialog box appears.

   **Note:** Selecting **Momentarily Unlock** from the popup menu for a portal unlocks the portal for its configured unlock time.

4. In the **Action** column, select **Lock** or **Unlock** for a portal.

5. In the **Start Date/Time** column, select one of the following:

   o Now: (the default setting) The action will start at the current date and time.

   o At: The action will start at the date and time you specify.

   o In: The action will start once the number of specified hours and minutes have elapsed.

6. In the **End Date/Time** column, select one of the following:

   o At: The action will end at the date and time you enter. Use the format shown for the Start Date/Time.

   o After: The action will end once the number of specified hours and minutes past the action's start time have elapsed.
7. Click **Save**.

   For example, for an output, select **Disarmed** and leave the **Start Time** at **Now**. Set the **End Time** to **After** 1:30 (one hour and thirty minutes). Click **Save**. The output will be disarmed for one hour and thirty minutes, starting immediately.

### Scheduling Actions for Inputs and Outputs

Select **Administration : Schedule Action** or **Monitor : Live Monitoring : Floorplans**.

On this page you can schedule the disarming of an input or an activation or deactivation of an output.

**To schedule an extended action from the Schedule Action page:**

1. Select **Administration : Schedule Action**.

2. Click the **Schedule** link for the input or output for which you want to schedule an action. A **Scheduled Action** dialog box appears.

3. In the **Action** column, select one of the following:
   - Lock or Unlock for a portal
   - Disarmed for an input
   - Activate or Deactivate for an output
   - Free Access or Controlled Access for an output

4. In the **Start Date/Time** column, select one of the following:
   - **Now**: (the default setting) The action will start at the current date and time.
   - **At**: The action will start at the date and time you specify.
   - **In**: The action will start once the number of specified hours and minutes have elapsed.

5. In the **End Date/Time** column, select one of the following:
   - **At**: The action will end at the date and time you enter. Use the format shown for the Start Date/Time.
   - **After**: The action will end once the number of specified hours and minutes past the action's start time have elapsed.

6. Under **Use**, select either **Local Site Time** or **System Time**.

   When you select **Local Site Time**, the time specs for the selected action will be based on the time zone set for the local Network Node. When you select **System Time**, the time specs will be based on the time zone set for the Network Controller.

7. Click **Save**.

   For example, for an output, select **Activate** and leave the **Start Time** at **Now**. Set the **End Time** to **After** 1:30 (one hour and thirty minutes). Click
To schedule an extended action from a floorplan:

1. Select **Monitor : Live Monitoring : Floorplans**.
2. Select a floorplan from the **Floorplan** drop-down menu.
3. Hold down the left mouse button on the icon for an input or output, and select **Schedule Action** from the popup menu. A **Scheduled Action** dialog box appears.
4. In the **Action** column, select **Disarmed** for an input, or **Activate** or **Deactivate** for an output.
5. In the **Start Date/Time** column, select one of the following:
   - **Now**: (the default setting) The action will start at the current date and time.
   - **At**: The action will start at the date and time you specify.
   - **In**: The action will start once the number of specified hours and minutes have elapsed.
6. In the **End Date/Time** column, select one of the following:
   - **At**: The action will end at the date and time you enter. Use the format shown for the Start Date/Time.
   - **After**: The action will end once the number of specified hours and minutes past the action's start time have elapsed.
7. Click **Save**.

For example, for an output, select **Disarmed** and leave the **Start Time** at **Now**. Set the **End Time** to **After** 1:30 (one hours and thirty minutes). Click **Save**. The output will be disarmed for one hour and thirty minutes, starting immediately.

### Selecting Partitions

Select **Monitor : Select Partition**.

If your system is partitioned for monitoring multiple populations and/or resources separately, you can select a different partition to which you have access to:

- Monitor the other partition's activity.
- Perform administrative functions within the other partition.
- Set up and configure resources within the other partition.

To select a different partition:

1. Select the partition in which you want to work.
2. Click **Save**.
Managing Evacuations

An evacuation plan defines one or more regions to be evacuated in the event of an emergency or disaster, and one region that will serve as a mustering station during an evacuation.

If one or more evacuation plans have been added to the system, you can use options on the Administration : Evacuations menu to start and end an evacuation plan.

<table>
<thead>
<tr>
<th>Choose this:</th>
<th>To do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Evacuation Plan</td>
<td>Start an evacuation plan.</td>
</tr>
<tr>
<td>End Evacuation Plan</td>
<td>End an active evacuation plan.</td>
</tr>
</tbody>
</table>

Starting an Evacuation Plan

Select Administration : Evacuations.

Note: You can also use the Mobile Security Officer™ (MSO) App running on an iPad to start an evacuation plan. For more information, see Tech Note 27, S2 Mobile Security Officer™ Mobile Evacuation Management.

To start an evacuation plan:

1. Select the name of the plan you want to start.
2. Click Start Evacuation Plan.
   
   An entry appears in the Activity Log indicating the plan name and your username. An entry also appears for any user who starts Mustering for this plan in the MSO App. The entry will include a network address for the user's iPad. On each iPad running the MSO App, the plan is now shown as active.
   
   You are returned to the Evacuations menu page.
3. To review the progress of the evacuation:
   
   o Run the Roll Call or Occupancy report and periodically refresh the report results.
   
   o In the MSO, click Mustering to get a dynamic view of the evacuation’s progress.
Ending an Evacuation Plan

Select Administration : Evacuations.

Once all unaccounted-for individuals have been checked out at the designated mustering station for an evacuation plan, you can end the plan.

Note: You can also use the Mobile Security Officer™ (MSO) App running on an iPad to end an evacuation plan. For more information, see Tech Note 27, S2 Mobile Security Officer™ Mobile Evacuation Management.

To end an evacuation plan:

1. Select the name of the plan you want to end.
2. Click End Evacuation Plan.

   If more than one evacuation plan is active, select the one you want from the list.

   The plan’s state changes from active to inactive. An entry appears in the Activity Log indicating the plan name and your username.

   Ending the plan does not automatically remove people from the region designated as the plan's mustering station. They will be removed from that region the next time they present their credentials to enter protected regions.
Managing People Data

You can use options on the Administration : People menu to enter and change information about people in the system.

<table>
<thead>
<tr>
<th>Choose this:</th>
<th>To do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add people to the system by creating person records.</td>
</tr>
<tr>
<td>Change/delete</td>
<td>Search for, edit, and delete person records.</td>
</tr>
</tbody>
</table>

Adding People to the System

Select Administration : People : Add.

Before you can issue a credential, assign an access level, or print a photo ID, the person must added to the system. To add a person, you create a person record.

You can create a person from scratch—or, if person record templates are available in the active partition, you can use a template. This will usually save time, because values defined in the template, such as a default set of access levels, will already be filled in.

Notes: Once you create a person record from a template, subsequent edits made to the template will not affect the person record.

As long as a person record template is associated with at least one person record, users can select it when creating custom People report definitions and defining person search criteria.

To add a person:

1. In the Add person using template drop-down list, do one of the following:
   - If there are templates available in the list, select the one you want to use.
   - Select None (the default) to create the person record without a template.

   Note: Before saving the person record, you can select a different template, or switch between using a template and not using a template. Values you have entered into fields unaffected by the change will be preserved. If any of the values you have entered will be overwritten, you will be warned and given an opportunity to continue or to cancel the change.

2. Fill in the fields at the top of the person record form:
   - The Last Name and Activation Date/Time fields are required entries. Clicking the calendar icon displays a calendar you can use to select the activation date.
Managing People Data

- Enter an **Expiration Date/Time** to have the person's access expire at a particular date and time. If you are using a template, these fields might be pre-filled.
  
  The expiration date and time you set can affect the person’s credentials. See [About Automatic Credential Expiration](#) on page 44 for more information.

- Enter any relevant **Notes** for the person. If you are using a template, this field might be pre-filled.

- If your organization issues ID numbers, enter the person’s ID number in the **ID#** text box.
  
  Although ID number is not required, supplying a unique Person ID for each person record allows the records to be reliably retrieved, modified, and deleted via data operations.

3. Review the information on the person record tabs, and make any needed changes or additions. For information on each tab, see [Editing a Person Record](#) on page 36.

   If you are using a template, fields on the Access Control tab might be pre-filled.

4. Click **Save**.

5. To add another person, click the **Add Another Person** button.

### Finding and Changing Person Records

Select **Administration : People : Change/delete**.

On this page you can:

- Search for person records to view, edit, or delete.
- Add or change person data including contact and vehicle information, access level, photo, and user role permissions.
- Delete or Undelete a person's record. Note that deleting a person's record does not remove it from the system, but rather deletes it from the active roster. When viewing a deleted record the Delete action button changes to Undelete.
- Use the **Add** link to add people to the system.

### Searching for a Person Record

**To search for a person record by scanning a credential:**

1. Click the **Search by Credential Scan** button at the bottom of the page.

2. If an enrollment reader is not defined for your system, select a reader from the drop-down list and click **Go**.

3. Scan the credential.
4. If the 90 second timeout period expires before you are able to complete the scan, click Go to restart the timer.

5. (optional) Before the timeout period expires, click Stop to stop the timer, then click Go to restart it when you are ready.

   In the list of matching person records, click a name to open the person’s record. If only one record has a matching hot stamp number, that record opens automatically.

6. Make any needed changes to the person record.

7. Click Save.

**To search for a person record by entering search criteria:**

1. To specify your search criteria, you can use any of the available fields:
   - A field marked with an asterisk will find complete exact matches only. For example, if you enter an ID# of 123 and the person's ID# is 1234, no matches will be found.
   - A field not marked with an asterisk can find partial matches. For example, if you enter the first letter of the person’s Last Name, a list of all people whose last names begin with that letter will be displayed.
   - For a person record to be found, it must match the entries in all fields. For example, if you enter the first letter of the person’s Last Name and a Department name a list of all people whose last names begin with that letter AND whose department name also matches will be displayed.

2. Use the **Expiration date before** and **Expiration date after** fields to find people whose person records have expiration dates before or after a specific date.

3. Use the **Template** field to find people whose person records were created from any of the available templates in selected partition(s), from a specific template, or without a template.

4. Use the **Badge Print Count** field to search for people by the number of times their badges have been printed. Enter 0 to find people whose badges have not yet been printed.

5. Use the **Partition** drop-down list to specify the partitions you want to search:
   - Select <all> to include records from all partitions to which you have access. This option will only appear if you have access to multiple partitions.
   - Select <visible> to include records located in other partitions that are visible within the current partition.
   - Select <current> to limit the search to records located in the current partition.
   - Select the name of a partition to limit the search to records located in that partition.

6. To include particular types of records in the search results, select the check box for any of the following records:
Managing People Data

- **Include deleted records**: Records that have been deleted from the system will be included. This check box is selected by default.
- **Include expired records**: Records that have expired will be included.
- **Include only records with non-unique person IDs**: Only records with non-unique person IDs will be included. This is useful for finding and fixing non-unique person IDs prior to enabling the **Enforce unique person IDs** option on the Network Controller page.
- **Include only records that exceed max active credentials**: Records that exceed the maximum number of active credentials a person should have per partition (as set on the Network Controller page) will be included.
- **Include only records for traced persons**: Only records for people whose activity is being traced will be included. The **Trace this person** check box is selected in the person record of such individuals.

7. Click the **Search** button.

   If the search returns a list of names, click on the name of the person whose record you want to view, edit, or delete. If only one record matches the search criteria, that record opens automatically.

   **Note**: If the person record is located in another partition, you will first need to click the **Switch Partition to Edit User** button at the bottom of the record to navigate to the other partition. You are able to edit the record if you have sufficient access rights in that partition. After saving your changes, you can navigate back by clicking the **Switch Partition to Original** button.

8. Make any needed changes to the person record, as described in the following section.

9. Click **Save**.

**Editing a Person Record**

When you select the person whose information you want to change or delete, his or her person record appears. The information you can change for the person is described below.

**To make changes in the basic information section:**

1. **Last Name** and **Activation Date/Time** fields are required entries. You can click on the calendar icon to display a calendar for selecting dates.

2. Enter an **Expiration Date/Time** if you want the person's access to expire automatically at a particular date and time.

   The expiration date and time you set can affect the person’s credentials. See **About Automatic Credential Expiration** on page 44 for more information.

3. If your organization issues ID numbers this can be entered in the **ID# text** box.
Although the ID number is not required, supplying a unique Person ID for each person record allows the records to be reliably retrieved, modified, and deleted via data operations.

4. Modify information on any of the tabs, which are described below.

5. Click Save when you have finished making changes.

The read-only Last Modified Date & Time and Last Modified User fields, which are updated whenever a user modifies the person’s data, show the current date and time and the user name used to log into the current session, respectively.

Note: Depending on how the person record is configured for your system, you may see fewer tabs than are described below. In addition, the User-defined tab may have been given a unique name and custom data fields.

Access Control Tab

On the Access Control tab you can assign a PIN; assign regional anti-passback privileges; assign an extended unlock period; issue, revoke, and temporarily disable cards; assign and remove access levels; and assign an email distribution list for notification on expiration of credential, access level, and/or a person record. For more information, see Changing a Person’s Access on page 45.

Photo ID Tab

If your system is licensed for photo ID badging you will see a Photo ID tab. On this tab you can upload, save, and delete photo ID images and digital signatures, and create and print access badges. Each image file uploaded must have a unique name and must end with the extension .jpeg or .jpg. It must be no larger than 80 KB; or on an Extreme or Enterprise system, no larger than the current photo ID size limit option on the Network Controller page.

User-defined Tab

On the User-defined tab, there are 20 fields you can customize and use for data you need to capture for people in the system. If the person record was created from a template, some or all of these fields might be pre-filled.

Contact Tab

The information on the Contact tab is optional. It is intended only for reference by the security management system user.

Other Contact Tab

The information on the Other Contact tab is optional. It is intended only for reference by the security management system user.
Vehicles Tab

The information on the Vehicles tab is optional:

- The **License #** field is for the state issued license plate number.
- The **Tag #** field is for the company issued parking permit number.

The **Tag #** field can be used to search for a person record. If your organization does not issue parking tag numbers you can enter license plate numbers in the **License #** field and search on that field to determine who owns a particular vehicle.

Login Tab

A user name and password are entered on the Login tab only if the person is a security management system user.

**To enter login information for a user:**

1. Enter a **User Name**.

2. If you have configured an LDAP server for single sign-on password authentication, select the **Login using directory services domain passwords** check box. DO NOT enter passwords here.

3. If you are NOT using an LDAP server for single sign-on password authentication, have the user enter his or her password in both the **Password** and **Re-enter Password** fields.

4. Select the appropriate **User Role** for this person. The default user roles are described below.

5. To restrict the alarms to which this person has access, select an **Alarm Filter Group**. When this person is logged in and monitoring the Alarm Workflow widget, he or she will be able to view only alarms matching the criteria defined by one or more of the alarm filters in the group.

6. Select a default Widget Desktop layout for this person from the **Default Widget Desktop** drop-down. This is the layout that will appear automatically when the person is logged in and opens the Widget Desktop.

7. Click **Save**.

There are four levels of user roles for security application users. From lowest to highest they are:

- **Master partition monitor**: Users with this role can use all available Monitor functions, within the **Master** (default) partition only.

- **Master partition administer**: Users with this role can use all available Monitor and Administration functions, within the **Master** (default) partition only.

- **Master partition setup**: Users with this role may use the functions of the Setup, Administration, and Monitor menus, within the **Master** (default) partition only.
• **Full system setup:** Users with this role may use all available functions of the Setup, Administration, and Monitor menus with all partitions.

In addition to the roles above, users with setup privileges can assign **Custom User Roles** created using the **Setup : Site Settings : User Roles** page.

**Note:** The Main Menu is built dynamically for each user who logs in. It will show only those menus, cameras, access levels, elevators, floor plans, events, and person record information that the user has permission to view or use based upon their assigned user roles.

---

**Partitions Tab**

The Partitions tab appears in person records only if the system has multiple partitions.

- If the person record has been made visible in all other partitions, the tab displays a note to that effect.

  Depending on how the system is configured, administrators in those partitions will either have full access to the person record, including full editing rights, or **limited access**. If they have limited access, they will be able to search for the person record, open it, and assign or remove any of the access levels defined in their own partitions. They will not be able to edit any other information in the person record, such as the person's contact and login information.

- If the person record has been made visible only in the partitions listed on this tab, you can use the procedure below to give administrators in these partitions limited access to the person record.

**To grant and revoke limited access to a person record:**

1. Run a search to locate the person record.
2. Click the **Partitions** tab in the person record.

   The Partition drop-down list includes all other partitions in which you have at least administrator privilege, or in which the **Make this partition name visible to all administrators in other partitions** check box is selected on the Network Controller page.

3. Select a partition whose administrators should be granted limited access to this person record.
4. Enter the date and time when the limited access should expire.

   **Note:** Click the calendar icon to select the date. If you do not enter an expiration date, administrators in the selected partition will have permanent limited access to the person record.

5. Click **Save**.
6. To revoke a partition’s limited access before it expires, click the **Delete** icon to the left of the entry, click **Yes** to confirm, and then click **Save**.
Note: When searching for the person record, administrators who have been granted limited access will need to select the partition where the record resides before running the search.

Example: Suppose that Thomas, an employee working in the home office, is about to begin a three-month assignment in a remote office. As the administrator of the Home Office partition, you can give Megan, the Remote Office partition's administrator, limited access to Thomas's person record for that period. She will then be able to assign Thomas the access levels he will need to enter and navigate the remote facility. Once Thomas's temporary assignment is completed, Megan can remove her partition's access levels from Thomas's person record.

Recent Activity Tab
The Recent Activity tab provides a list of recent system activity generated by the person whose record you are viewing.

Managing a Person’s Credentials
Select Administration : People, enter a name and click Search.
On the Access Control tab of a person record you can:
• Issue a new credential using a reader or using a keyboard entry.
• Issue a new credential for use with remote locksets.
• Revoke a credential
• Disable a credential
• Issue and return temporary credentials. See Handling Temporary Credentials on page 49.

For information on the automatic expiration of active credentials, see About Automatic Credential Expiration on page 44.

Issuing New Credentials

To issue a new credential using a reader:
1. Click the Access Control tab in a person record.
2. Click the Add New Credential button.
3. Enter the hot stamp number printed on the credential into the Hot stamp # box.
4. Select a format from the Credential Format drop-down list.

Only formats that are enabled will appear in the list. To enable a credential format, a user with setup privileges must select its Enabled checkbox on the Card/Keypad Formats page.
5. (optional) Select a different status for the credential from the Status drop-down list. See To disable a credential below for more information.

6. (optional) If credential profiles are enabled for the site, select a profile from the Profile drop-down list. The profile will define the maximum number of days of non-use before the credential will expire.

7. (optional) To set an expiration date for the credential, click the Expiration Date calendar icon and select a date from the calendar that appears. Each night the controller will check for and delete expired credentials.

   To remove an expiration date from a credential, click the date and then press DELETE.

8. Click the Read button to read the credential.

9. In the Issue Credential Using Reader dialog box, check to make sure the enrollment reader you are using is selected in the drop-down list, then click Go.

10. Present the credential to the reader. The encoded credential number appears in the Encoded # box.

    **Note:** If auto-incrementing of encoded credential numbers is enabled for your system, the value that appears in the Encoded # field will be one number above the highest value for any encoded number in the database.

    If the person already has the maximum number of active credentials set for your system, you will see an error message. To add the new credential, you will need to either revoke or disable one of the person's currently active credentials.

11. Click Save.

**To issue a new credential using a keyboard entry:**

1. Click the Access Control tab in a person record.

2. Click the Add New Credential button.

3. Enter the hot stamp number printed on the credential into the Hot stamp # box, and enter the encoded credential number into the Encoded # box.

    **Note:** If auto-incrementing of encoded credential numbers is enabled for your system, the value that appears in the Encoded # field will be one number above the highest value for any encoded number in the database.

    If the person already has the maximum number of active access credentials set for your system, you will see an error message. To add the new credential, you will need to either revoke or disable one of the person's currently active credentials.

4. Select a format from the Credential Format drop-down list.
Only formats that are enabled will appear in the list. To enable a credential format, a user with setup privileges must select its Enabled checkbox on the Card/Keypad Formats page.

5. (optional) Select a different status for the credential from the Status drop-down list. See To disable a credential below for more information.

6. (optional) If credential profiles are enabled for the site, select a profile from the Profile drop-down list. The profile will define the maximum number of days of non-use before the credential will expire.

7. (optional) To set an expiration date for the credential, click the Expiration Date calendar icon and select a date from the calendar that appears. Each night the controller will check for and delete expired credentials.

To remove an expiration date from a credential, click the date and then press DELETE.

8. Click Save.

To issue a new credential for use with remote locksets:

1. Click the Access Control tab in a person record.

2. Click the Add New Credential button.

3. Enter the hot stamp number printed on the credential in the Hot Stamp # field and enter the encoded credential number in the Encoded # field.

   – or –

   For a PIN-only credential, enter the 6-digit PIN into both the Hot Stamp # field and the Encoded # box.

Notes: If auto-incrementing of encoded credential numbers is enabled for your system (under Misc. Information on the Network Controller page), the value that appears in the Encoded # field will be one number above the highest value for any encoded number in the database.

   If the person already has the maximum number of active credentials set for your system, you will see an error message. To add the new credential, you will need to either revoke or disable one of the person's currently active credentials.

4. Select a format from the Credential Format drop-down list. For a PIN-only credential, select Remote Lockset PIN Only.

Only formats that are enabled will appear in the list. To enable a credential format, a user with setup privileges must select its Enabled checkbox on the Card/Keypad Formats page.

Note: The Remote Lockset PIN Only format is intended for remote locksets configured with card readers only. It can be assigned to a remote lockset configured with both a reader and keypad, however, if you assign a PIN to the user. The user will need to enter the PIN twice at the lockset to unlock it.
5. (optional) Select a different status for the credential from the **Status** drop-down list. See *To disable a credential* below for more information.

6. (optional) If credential profiles are enabled for the site, select a profile from the **Profile** drop-down list. The profile will determine the maximum days of non-use before the credential will expire.

7. (optional) To set an expiration date for the credential, click the **Expiration Date** calendar icon and select a date from the calendar that appears.

   Each night the controller will check for and delete expired credentials. To remove an expiration date from a credential, click the date and then press **DELETE**.

8. (optional) Select a type from the **Remote Lockset User Type** drop-down list. Once a credential has been assigned any remote lockset user type other than **Regular Access Card**, it will no longer be usable as an access card.

   **Note:** Be sure to test any credential that will be used with remote lockset magnetic stripe readers before giving it to the user. Occasionally, a magnetic stripe reader will fail to read a credential that can be successfully read by other readers. When this happens, the user receives no beep or confirmation that the credential was not read, and no information about the access attempt is recorded.

9. Click **Save**.

### Revoking and Disabling Credentials

Revoking a credential is permanent. For a revoked credential to function again, you will need to use one of the procedures in the previous section for issuing a new credential.

Disabling a credential is temporary. You should consider disabling the credential of a person whose credential has been forgotten, lost, or stolen and to whom you are issuing a temporary credential. If the disabled credential is found, you can select it and change its status back to **Active**.

**To revoke a credential:**

1. In the list of credentials, select the credential you want to revoke.

2. Click this icon ![Revoking a Credential](revoking.svg) to revoke the credential.

3. Click **Yes** in the Revoke Credential dialog box.

   The credential is immediately removed from the system and ceases to function.

**To disable a credential:**

1. In the list of credentials, select the credential you want to disable.

2. On the **Status** drop-down list, change the Active setting to any of the following:
Managing People Data

- Clear*
- Damaged*
- Disabled
- Forgotten*
- Lost*
- Not Returned*
- Not Used
- Not Validated*
- Returned*
- Stolen*
- Suspended*

**Important:** The nine settings followed by an asterisk (*) above might have been customized for your system. For any of these nine settings, an administrator might have used the Credential Attributes page to change its name and description and to specify that all credentials to which the setting is applied should remain functional. For this reason, the Status drop-down list might look different from the list above, and applying certain of these settings to a credential might not disable it.

3. Click **Save**.

   The credential will not function until its status is changed back to **Active**.

   You can run a **Credential Audit** report to view existing credentials by their current status settings.

**About Automatic Credential Expiration**

In certain situations, the controller automatically expires active credentials. The automatic credential expiration affects only credentials with a status of Active or Temporary. If the system has active credentials with customized status values, they will not be affected.

The controller automatically expires credentials during its daily system checks, whenever it finds:

- A credential whose Expiration Date has passed. The credential's status is changed from Active or Temporary to Expired or Temporary Expired, respectively.

   To reactivate the credential, a user will need to edit the person record in the UI and move the credential's Expiration Date to the future. When the record is saved, the expired credential will change back to Active or Temporary.
• A person record whose Expiration Date/Time has passed. The person's Active credentials are changed to Expired. If the person has an active Temporary credential, its status is changed to Temporary Expired.

To reactivate the credentials, a user will need to edit the person record in the UI and move its Expiration Date/Time to the future. When the record is saved, the expired credentials will change back to Active and Temporary.

**Note:** Programmatically moving an active record's Expiration Date/Time to the past (via the API or Data Operations feature) has the same effect as a UI edit. Each of the person's active credentials will be changed to Expired or Temporary Expired during the daily system check.

However, programmatically moving an expired record's Expiration Date/Time to the future does not reactivate the person's credentials as a UI edit would. For the credentials to be reactivated, the programmatic edit would need to include changing each credentials' status back to Active or Temporary.

---

**Changing a Person’s Access**

Select **Administration : People**, enter a name and click **Search**.

On the **Access Control** tab of a person record you can:

• Assign, edit, and remove temporary and permanent access levels.
• Set or remove an activation date or expiration date for an access level.
• Assign regional anti-passback privileges.
• Exempt an individual from credential non-use rules.
• Trace a person’s activity.
• Assign an email distribution group to be used notification of credential, access level, and person record expirations.
• Assign a PIN.
• Assign an extended unlock period.

**Notes:** In a person record that was creating using a template, values on the Access Control tab may have been filled in automatically. For example, the person might have been assigned a default set of access levels.

Access levels and anti-passback privileges are assigned to people, not to access cards and other credentials. All credentials issued to a particular person will have the same access levels as the person. Each person in the system is limited to a maximum of 32 access levels.
To assign, edit, and remove access levels:

1. Click the Access Control tab in a person record.
2. In the list of access levels, select each access level you want to assign from the Available box, then click the right arrow button to move it to the Selected box.

   Use SHIFT-click to select multiple access levels at once.
3. (optional) If Otis Compass is enabled, do either or both of the following, and then click Save.
   - Select a floor from the Default elevator stop (floor) drop-down list. This setting determines the floor to which the user will be directed.
   - To enable flags that are sent directly to the elevator control system, select any or all of the following check boxes: VIP, TD08, TD10, TD20, TD40, and TD80. The effect of enabling these flags depends on the configuration of the elevator control system.
4. To remove an access level from the person record, select it and click the left arrow button to move it back to the Available box.
5. Click Save.

To set or remove an activation date or expiration date for an access level:

1. Click the Access Control tab in a person record.
2. In the list of access levels, double-click anywhere in the row for the access level you want to edit.
3. To set an activation date, click the calendar icon in the Activation Date column, select a date from the calendar that appears, and then press ENTER.
4. To set an expiration date, click the calendar icon in the Expiration Date column, select a date from the calendar that appears, and then press ENTER.
5. To remove an activation date or expiration date from the access level, double-click anywhere in its row, drag to select the date you want to remove, press DELETE, and then Press ENTER.
6. To have the system automatically remove the access level once it expires, select Yes from the Auto-remove drop-down list. Each night, the controller will check for and delete expired access levels.
7. Click Save.

Note: If the Save button is dimmed, press ENTER to make it available.

To assign regional anti-passback privileges:

1. Click the Access Control tab in a person record.
2. In the lower left corner, select an entry from the **Regional anti-passback privileges** drop-down list to determine how this person’s passback violations should be handled:
   - **(none)**: The person will have no special anti-passback privileges. Violations will be handled according to the Passback violations and Tailgate violations behaviors selected on the **Regions** page.
   - **Exempt**: The system will ignore violations.
   - **Soft Always**: The system will log each violation, but allow access.
   - **Hard Always**: The system will deny access in the case of a violation.

   **Note**: Mercury panels support only the **(none)** and **Exempt** settings.

   These anti-passback privileges are assigned to the person, not to the person’s credentials. They will take precedence over the specified Tailgate and Passback violation behaviors selected on the **Setup : Access Control : Regions** page.

3. Click **Save**.

**To exempt an individual from credential non-use rules:**

If credentials are set to be disabled after a specific number of days of non-use, you can exempt individuals from this rule.

1. Click the **Access Control** tab in a person record.
2. Select the **Exempt from credential non-use rules** check box.
3. Click **Save**.

**To trace a person's activity:**

1. Click the **Access Control** tab in a person record.
2. To trace this person's activity in the current partition, select the **Trace this person** check box.
3. Click **Save**.

   Whenever this person makes a valid or invalid access request in the current partition, a message will appear in the Activity Log. The message text will be displayed in bold, and in the color selected for **Trace person log color** on the Network Controller page.

   If an event is selected for **Trace person event** on the Network Controller page, the event will be triggered whenever this person makes a valid or invalid access attempt in the current partition. These event activations will be logged in the Activity Log and you can report on them by setting a Trace people filter for a custom history report.

**To assign an email distribution group for expiration notification:**

1. Click the **Access Control** tab in a person record.
2. If a **Notify on expirations** drop-down list appears at the bottom of the page, select an email distribution group from the list.

When this person record, or any credential or access level assigned to this person, is about to expire, members of the selected group will be notified a specific number of days prior to the expiration.

3. Click **Save**.

**Note:** You will see the **Notify on expirations** drop-down list only when the expiration notification feature is enabled for your system.

---

To assign a PIN:

1. Click the **Access Control** tab in a person record.

2. Enter a four- to six-digit number in the **PIN** text box in the lower right corner of the tabbed page.

**Note:** Most Wiegand keypads support four digit PINs. Bit-burst keypads support PINs of any length.

3. Alternatively, click the icon next to the text box to enter an automatically generated PIN containing the number of digits specified for **Auto-generated PIN digits** on the Network Controller page (**Setup : Site Settings : Network Controller**).

4. Click **Save**.

**Note:** If the security administrator has enabled the **Keypad timed unlock** feature for a portal that has a reader/keypad device, a cardholder is able to present his or her credential at the portal, and then enter his or her assigned PIN followed by the number sign (#) and the number of minutes (1-99) the portal should remain unlocked. For example, entering **#20** after the PIN will unlock the portal for 20 minutes.
To assign an extended unlock period:

1. Click the Access Control tab in a person record.
2. If this person requires extra time to get through a door (because of a disability, for example), select the Use Extended Unlock check box.
   Whenever this person accesses a portal, it will remain unlocked for the number of seconds specified by the Extended Unlock Time specified in the portal definition.
3. Click Save.

Handling TemporaryCredentials

Handling temporary credentials for cardholders who have forgotten or misplaced their credentials can be a time-consuming and error-prone process. To address this problem, the system provides a workflow for quickly and accurately issuing temporary credentials, returning them, and reactivating the missing credentials.

This workflow is available in person records when the “Enable temporary credential workflow” check box is selected on the Network Controller page. If you have sufficient permissions, you can use it to:

- Issue a temporary credential, which will remain active for the expiration period specified in your system’s Temporary Credential policy.
- Extend the expiration period for a temporary credential (if the Temporary Credential policy allows extensions).
- Return temporary credential(s) and optionally reactivate missing credential(s) immediately.
- Reactivate missing credential(s).

Note: Status settings applied to credentials at various steps in the workflow make it possible to create a Credential Audit report showing the current state of missing and temporary credentials in the system.

To issue a temporary credential:

1. Select the Access Control tab in the person record.
2. Click Issue Temporary Credential. A dialog box for scanning temporary credentials appears.
3. If an enrollment reader is not defined for your system, select a reader from the drop-down list and click Go.
4. Present the temporary credential to the enrollment reader.
   If “Disable missing credentials” is selected in your system’s Temporary Credential policy, all other credentials currently issued to the person become disabled. Attempting to use such a credential will result in an "Access denied" Activity Log entry with the reason code: Missing [DISABLED].
To extend the expiration period for a temporary credential:

If “Allow expiration extension” is selected in your system’s Temporary Credential policy, you are allowed to extend a temporary credential.

1. Select the Access Control tab in the person record.
2. Click **Extend Temporary Credential**. An extension dialog box appears.
3. If an enrollment reader is not defined for your system, select a reader from the drop-down list and click **Go**.
4. Present the temporary credential to the enrollment reader.
5. Click **Save**.

The credential’s new expiration period will be the same as if you had issued a new temporary credential. It will extend past the current date for the number of days specified in your system's Temporary Credential policy. Once the credential expires, its status will change from Temporary to Temporary Expired.

**Note:** If a person record expires, its active credentials will be expired automatically. See About Automatic Credential Expiration on page 44 for more information.

To return temporary credential(s) and optionally reactivate the missing credential(s):

1. Select the Access Control tab in the person record.
2. Click **Return Temporary Credential(s)**.

All temporary credentials currently issued to the person are removed from the system.

If “Missing credentials must be read for reactivation” is not selected in your system’s Temporary Credential policy, all of the person’s missing credentials are reactivated (their status changes to Active) and the workflow is complete.

3. If a read is required to reactivate missing credentials, a reactivation box appears. To reactivate the missing credentials immediately:
   - If an enrollment reader is not defined for your system, select a reader from the drop-down list and click **Go**.
   - Present a missing credential to the reader. The credential’s status changes from Missing to Active.
Present each additional missing credential when the dialog box reappears (once for each missing credential).

– or –

Click Cancel to close the dialog box and reactivate the missing credential at a later time, using the procedure below.

4. Click Save.

To reactivate missing credential(s):

You can reactivate a person’s missing credentials only if no temporary credentials are currently issued to the person.

1. Select the Access Control tab in a person record.
2. Click Reactivate Missing Credential(s). A reactivation dialog box appears.
3. If an enrollment reader is not defined for your system, select a reader from the drop-down list and click Go.
4. Present a missing credential to the reader. Its status changes from Missing to Active.
5. Present each additional missing credential when the dialog box reappears (once for each missing credential), or click Cancel if you want to reactivate additional credentials at a later time.
6. Click Save.

Handling Lost Credentials

Select Administration : Lost Cards.

If a credential is found and turned in, you can determine the identity of the cardholder.

To determine the identity of a cardholder:

1. In the Hot stamp # text box, enter the number on the credential and click the Search button.
2. If there is no number printed on the credential, click the Use Reader link to display a small reader window.
3. Select a reader from the Reader drop-down list and swipe the credential through that reader.
   The credential number fills the Hot stamp # text box.
4. Click the Search button.
Revoking Credentials

In the Access Control section of a person record you can issue a new credential, revoke a credential, temporarily disable a credential, and assign access levels for any person in the system.

Revoking a credential is not temporary. In this respect, it differs from disabling a credential. For a revoked credential to function again you will have to use the procedure for issuing a new credential.

To revoke a current credential:
1. Select Administration : People : Change/delete.
2. Enter a name and/or other search data and click Search.
3. On the Access Control tab locate the credential you want to revoke.
4. The credential Hot Stamp # and Encoded # fields will fill with the credential numbers.
5. Click the Revoke Credential icon for that credential.
6. Click Yes in the Revoke Credential confirmation dialog.
   
   This credential is immediately removed from the system and will not function.

Changing a Password

Select Support/Utilities : Change Password.

Passwords are needed only by users who are allowed to log in to the system.

Note: You can configure an LDAP server for single sign-on password authentication. Passwords would then not be entered here. You CANNOT change an LDAP server password from this page.

To change a password:
1. Enter the Current password. Passwords are case sensitive.
2. Enter the New password.
3. Enter the new password again in the Re-enter password box.
4. Click Save. The new password takes effect immediately.

Notes: If the new password is identical to the current password, you will see an error message. The new password must be different from the current one. If you re-enter the new password incorrectly you will see an error message. A new password must be entered precisely as it was first entered.
Valid Password Rules

Passwords cannot contain quotation marks (‘ ‘) unless the rules have been customized to include special characters in the required password configuration.

Rules for passwords can be customized in Setup : Site Settings : Network Controller, specifying minimum password length and/or whether the password must contain a combination of letters, numbers, and special characters. More details about the customized password requirements are found in Changing Your Password in the online help.

Tips for strong passwords:

- Passwords should be changed periodically.
- Do not use passwords that can be easily guessed, such as names of family members or birth dates.
- Passwords should contain at least one alpha and one numeric character, or a combination of letters, numbers, and special characters, if so specified.

Managing Email Distribution Groups

Select Administration : People : Email Distribution Groups.

On this page you can create, edit, and delete groups of people that can be used for email distribution.

To create an email distribution group:

1. Enter a descriptive Name for the distribution group, or click add and then enter the name.
2. Enter values in one or more of the available search fields.
   For information on entering search criteria, see Finding and Changing Person Records on page 34.
3. Click Search.
   The names of the people matching your search criteria appear in the Results list.
4. For each person you want to include in the distribution list, select the name in the Results list and click the right-arrow button to move it to the Selected list.
   
   Note: In the Results list, the name of anyone whose email address is derived from a Short Message Service (SMS) address is followed by “[SMS]”.

5. To remove a person from the Selected list, select the name and click the Remove from list button to move it back to the Results list.
6. Click **Save** when the Selected list includes the set of people you want in the distribution group.

**Note:** Because email distribution lists refer to their members’ person records, a member whose email address changes will continue to receive email distributed by the group.

---

**Creating and Printing Photo IDs**

Multiple hardware and software products have been integrated to provide image capture and photo ID printing features from within this security application. Install the software and drivers from the CD provided and refer to the printable *Photo ID Badging Install and Setup Guide* from its link in the online help.

**Note:** Photo ID printing features work with Internet Explorer only. Other browsers do not support the ActiveX controls required for these features.

On the photo ID tab you can:

- Capture ID photos and save them to person records.
- Print a photo ID badge.
- Request printing of a photo ID badge.
- Print photo ID badges from the request queue.
- Capture and save digital signatures.

**To capture ID photos and save to a person’s record:**

**Note:** Make sure that the Logitech QuickCam settings are set to an image size of no more than 640x480, and that **Face Tracking** is set to **Follow Me**. This will ensure that the image size remains under the maximum 30K.

1. Select **Administration : People**.
2. Add a new person to the system or search for an existing person.
3. Click the **Photo ID** tab.
4. Select from the **Badge** drop-down the badge design you want to use.
5. Click the **Photo ID** button and the **Photo IDs** pop-up window appears.

**Note:** If the photo ID image window does not appear, turn off the pop-up blocker or add the Network Controller site to the allowed site list.

6. In the **Photo ID** window, click **Capture Image**, and the **Select Image Source** window appears.
7. Select **Microsoft WDM Image Capture (Win32)** and click **OK**. The **Capture** window and the Logitech QuickCam application bar appear.
8. Ensure that the person is properly within the picture frame and click the capture button:

Note: The software will perform “face-finding” and crop the image. This helps to ensure that the photo ID is less than the maximum allowed 30K.

9. If the picture is acceptable click OK. If not, click the continue button and recapture the photo.

10. The Capture window closes and the Photo IDs window redisplay with the image placed in the badge design. Confirm that the person's image is correctly captured and click Save Image.

11. The captured image appears in the person record. Click the Close button in the Photo IDs window.

12. Scroll to the bottom of the person record and click Save.

Note: In a person record, you can right-click on the image and select Save Picture as. You can then save this image separately as a jpg or bmp file.

To print a photo ID badge at your workstation:

The photo ID printer must be connected to your workstation with a USB cable. See the manufacturer documentation for guidance on hardware setup.

The printer's Windows driver listed above must be installed on your workstation. See the manufacturer documentation for guidance on software and driver installation.

1. In a person record, click the Photo ID tab.

2. From the drop-down in the Badge box, select the layout you want to use.

3. Click Photo ID. A small photo ID window appears.

4. In the photo ID window, click Print Photo ID. The Print dialog box appears.

5. From the Name drop-down list, select the photo ID printer, and click OK. Retrieve the badge from the printer tray.

6. In the photo ID window, click Close.

7. In the person record, be sure to click Save. This saves the captured image and selected badge design with the person's record.

Note: If you do not have a badge printer attached to your computer you can queue the print request for printing later at a computer that has an attached badge printer.
To request printing of a photo ID badge:

1. In a person record, click the **Photo ID** tab.
2. Place a check in the **Request Photo ID** checkbox.
3. Click **Save**.
4. Select **Administration : Reports : People : Request Photo ID Report** and verify that this report lists your request.

**Note:** Any badge printing requests in the queue can be printed as described in the following procedure.

To print requested photo ID badges:

The printer must be connected to your workstation with a USB cable. See the manufacturer documentation for guidance on hardware setup.

The printer's Windows driver listed above must be installed on your workstation. See the manufacturer documentation for guidance on software and driver installation.

1. Select **Administration : Reports : People : Request Photo ID Report**. This report lists all currently outstanding photo ID print requests.
2. Click the printer icon in the **Action** column (the rightmost column) for the badge you want to print. A small photo ID window appears.
3. In the photo ID window, click **Print Photo ID**. The **Print** dialog box appears.
4. From the **Name** drop-down list, select the photo ID printer, and click **OK**. Retrieve the badge from the printer tray.
5. In the photo ID window, click **Close**.

Deleting Photo ID Layouts

Select **Administration : Utilities : Badge Layout Delete**.

With this page you can delete badge layouts that have been uploaded to the controller.

To delete a badge layout:

1. Select the check box to the right of each of the badge layouts you want to delete,
2. Click **Delete File(s)**.
Uploading Photo ID Layouts

Select **Administration : Utilities : Photo ID Layout Upload**.

With this page you can upload badge layouts to the controller for use in creating and printing badges.

Photo ID layouts must first be created using EPI Designer. EPI Designer is part of the EPI Builder SDK from ImageWare® Systems, Inc. For details regarding security system data that can be used in photo ID layouts, see *System Data for Photo ID Layouts* in the online help.

**To upload a photo ID layout:**

1. Click the **Browse** button to browse to the location of your photo ID layout files.
2. In the Browse dialog box select the photo ID layout file you want to upload and click **Open**.
3. Click **Save**.

---

**Note:** Photo ID layout files must end with the .dgn extension and can be no larger than 600K.
Creating Reports from System Data

The Administration : Reports menu provides a variety of system information reports.

<table>
<thead>
<tr>
<th>Choose this:</th>
<th>To do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Create reports on the current configuration of system resources.</td>
</tr>
<tr>
<td>History</td>
<td>Create reports on system activity history.</td>
</tr>
<tr>
<td>People</td>
<td>Create reports on access information pertaining to people.</td>
</tr>
</tbody>
</table>

Configuration Reports

Select Administration : Reports : Configuration.

As Built

To run an As Built report, select a node from the Network Node drop-down and click Run report. A new browser window will open and display an image of each application blade in the node and the specific resources configured for that blade. You can print this report.

Cameras Report

The Cameras report displays all camera configuration information.

Camera Presets Report

The Camera Presets report displays configured presets for each camera in the system. These presets must be set at each camera web site.

Elevators Report

The Elevators report displays elevator configuration information. This includes the node to which each elevator’s inputs and outputs are wired, the reader used to control access to the elevator, the input corresponding to the elevator’s duress/emergency button, and the inputs and outputs corresponding to its floor-select buttons.
**Floor Groups Report**

The Floor Groups report displays all configured floor groups for use in elevator control.

**Holidays Report**

The Holidays report displays holiday specification information.

**Portals Report**

The Portals report displays portal definition information.

**Portal Groups Report**

The Portal Groups report displays all portal groups, the portals included in each, and the assigned threat level group.

**Reader Groups Report**

The Reader Groups report displays defined groups of readers.

**Remote Locksets Report**

The Remote Locksets report displays the following information for each remote lockset: name, IP address, synchronization status, serial number, last completed update time, firmware version, battery voltage, assigned Remote Lockset profile, and number of stored cardholders.

Clicking the Name link for a lockset takes you to the configuration page for the associated node. Clicking the Status link for a lockset takes you to the associated pending/transferred data summary report.

**Resources Report**

Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.

**Threat Levels Report**

The Threat Levels report displays all configured threat levels including the description and color assignment.
Threat Level Groups Report

The Threat Level Groups report displays all configured threat level groups and the threat levels assigned to them.

History Reports

Reports on the Administration : Reports : History menu let you retrieve data from archives when the requested report data is no longer active on the controller. In version 3.2 and above the controller maintains an active database of over 100,000 Activity Log records. Older data is kept in archive files both on the controller and on network attached storage devices. You can set up an FTP site or network attached storage (NAS) for this data.

<table>
<thead>
<tr>
<th>Choose this:</th>
<th>To do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access History Report</td>
<td>See reports tracing access attempts.</td>
</tr>
<tr>
<td>Audit Trail Report</td>
<td>See report of changes to the database over specified period of time.</td>
</tr>
<tr>
<td>CSV Export Report</td>
<td>Exports events from the Activity Log as a comma-separated values (CSV) file.</td>
</tr>
<tr>
<td>Custom Report</td>
<td>Create and run a custom report.</td>
</tr>
<tr>
<td>Duty Log Report</td>
<td>Run a report showing duty log comments.</td>
</tr>
<tr>
<td>General Event History</td>
<td>See reports on specific events from the Activity Log.</td>
</tr>
<tr>
<td>Portal Access Count</td>
<td>See reports on the number of portal accesses for an individual.</td>
</tr>
</tbody>
</table>

Access History Report

Select Administration : Reports : History : Access History.

On this page you can create reports to trace system access requests. The default Access History report searches the security database and archive files and returns information on every access request received by the system.

Before running the report, you can set search parameters to limit the results to particular people, event types, time periods, portals, and elevators. You can also limit the number of records the report will return.

To create an access history report:

2. To return only requests from anyone with a particular last name, enter that name in the Person field.
3. To return only valid or invalid requests, select Valid accesses or Rejected accesses, respectively.
4. To return only requests received during a specific period of time, select one of the following:
   - **Today** to return only requests received today.
   - **Yesterday** to return only requests received yesterday.
   - **Month(s)** to return only requests received from the first day of the month you select on the **From** drop-down list through the last day of the month you select on the **To** drop-down list.
   - **Custom Period** to return only requests received from the date you enter in the **From** field through the date you enter in the **Thru** field.

5. To return only requests received at a particular portal, select the portal name from the **At (portal name)** drop-down list.

6. To return no more than a certain number of requests, enter that number in the **Maximum Records** field.

7. Click **Search**.
   
The results are displayed in a table. For each access request, the table shows the date and time the request was received on the Controller and on the node, the person who made the request, the location where the request was received, and a description of the event type, such as “Access granted” or “Access denied (Unknown)”.

8. Click any column header to sort the data on that column. Click the header multiple times to switch between an ascending and descending sort order.

9. To view the report in PDF format, click the **PDF** link. To export the report as a comma-separated values (CSV) file, click the **CSV** link.

---

**Audit Trail Report**

Select **Administration : Reports : History : Audit Trail**.

With this page you can request a report showing changes made to the security database over a specified period of time. For each transaction listed in the report results, you can view information such as when the transaction occurred, who made the changes, the fields that were modified, and the original and new values.

To narrow down the report results, you can filter the search, either by the person whose record was changed or by the area of the system configuration that was modified. You can also select a specific partition from which you want to retrieve data and the maximum number of transactions you want to retrieve.

**To create an Audit Trail report:**

1. Select **Administration : Reports : History : Audit Trail**.

2. Click the **From (date)** calendar icon and select a start date for the report.

3. Click the **Thru (date)** calendar icon and select an end date for the report.
   
   You can also enter dates by typing them in the text boxes. If you do not enter a start date, the system will search back through the entire history.
available in archives. If you do not enter an end date, the system will use the current date.

4. (optional) On the Changed by drop-down list, select the name of the user whose changes you want to retrieve.

5. (optional) To apply a filter to narrow down the report results, do either of the following:
   - Enter the Last Name and/or First Name of the user whose person record you want to audit for changes.
   - Select Configuration and then select the area of the system configuration (such as nodes, portals, or events) you want to audit for changes.

6. If your system has multiple partitions, select the Partition from which you want to retrieve data.

   If you do not select a partition, the report results will include data from all partitions.

7. In the Limit to text box, enter the maximum number of transactions you want to retrieve. The default is 3,000 transactions.

   Setting the limit to 5,000 or more transactions is not recommended, because it may increase the time required for the system to generate and display the report results.

8. Click Run Report.

   Depending on your system and the number of transactions that must be displayed, it may take several minutes for the system to generate and display the report results.

9. To make the report results available for pasting into other applications, click Copy to Clipboard.

   To use the Copy to Clipboard button in the Mozilla Firefox browser, you must first enable the button.

10. To print the report results, click Print to display the Print dialog.

When you define and run an Audit Trail report, the results are displayed in a table. The table includes a row for each transaction matching the report criteria you specified. The rows are sorted in descending order by date, with most recent transaction appearing at the top of the report.

Information about each transaction is displayed in the following columns:

- **DATE/TIME**: The date and time the transaction occurred.
- **USER**: The user who made the changes.
- **DATA**: The database table in which the changes were made.
- **FIELD**: A field associated with the transaction. A given field might have been changed as part of the transaction, or it might be included in the results only to provide context for the changes.
Creating Reports from System Data

- **ACTION**: For each change associated with the transaction, the type of change that was made: an **INSERT**, **UPDATE**, or **DELETE**.

- **ORIGINAL VALUE**: For any field included in the results, the field value prior to the transaction.

- **NEW VALUE**: For any field that was changed, the field value after the transaction was completed. For fields that were not changed, `<n/c>` appears in this column.

You can expand a row to view more detail:

- To expand a single row, click the arrow to its left.
- To expand every row in the table, click the **Expand All** button.

### CSV Export Report

Select **Administration : Reports : History : CSV Export**.

With this page you can export a report containing events from the Activity Log as a comma-separated values (CSV) file. The CSV file contains the following information for each event:

- Partition (if the **Include activity from all partitions** check box is selected)
- Person ID
- Node Date/time
- Date/time
- Description
- Last Name
- First Name
- Node UID
- Node Name
- Location
- Reader
- Card Number

**To create a CSV Export report:**

1. Select **Administration : Reports : History : CSV Export**.
2. Click the **From (date)** calendar icon and select the start date for the report.
3. Click the **Thru (date)** calendar icon and select the end date for the report.
4. Select the **Include activity from all partitions** check box if you want the report to include data from all partitions, rather than from the selected partition only.
Creating Reports from System Data

This option is available only if you are in the Master partition and you have the full system setup user role. If the check box is selected, the report data will include a Partition column showing the partition in which each event occurred.

5. Click Export.
6. In the File Download dialog box, click Open to open the CSV file or click Save to save it.

Custom History Report

Select Administration : Reports : History : Custom Report.

On this page you can:

- Create custom history report definitions and save them for later re-use.
- Edit or delete saved custom report definitions.
- Run saved custom report definitions to get output in the defined output format (HTML, CSV, or PDF).

To create a custom history report definition:

2. If one or more custom history reports are already defined in the system, click New Report at the top of the report list.
3. On the page that appears, enter a Name for the report.
4. (optional) Enter a Title to be displayed with the report results and a Description that explains the report’s use.
5. On the Columns tab, set up the report columns:
   - For the PDF output, specify the Page Orientation (portrait or landscape) and the Page Size (Letter: 8.5 x 11 inches, or A4: 8.26 x 11.69 inches). The default page margins are 0.5.
   - For the HTML output, specify the Height and Width of the report screen display. The default is 700 points high by 600 points wide.
   - To set up the report columns, select from the Available list each data field that you want to display as a column, then click the right-arrow button to move it to the Selected list.
     As you add columns, a report guide displayed at the bottom of the page shows their current order and relative widths. The Remaining Width value indicates how many inches of the PDF page width are still available.
   - To change the column order, select individual entries in the Selected list and use the Move up and Move down buttons to move them up and down the list.
To specify a different column label and/or column width for any of the data fields, select it in the Selected list and edit the values that appear in the Column label and/or Width fields.

After changing a column’s width, you can click the column in the report guide to view it at its new width. Note that in HTML or PDF output, text that does not fit on a single line within a column will wrap automatically.

If the combined column widths exceed the PDF page width, the Remaining Width value will turn red and the report guide will indicate an error. If you save and run the report without first removing and/or downsizing columns, the data that extends beyond the right page margin will be truncated when the results are viewed in PDF format. The HTML view will not be affected.

6. On the Date & Time tab, specify the reporting period:
   
   - For From (date) and Thru (date), enter absolute dates, or select relative dates (such as Yesterday or Last month), to specify the beginning and end of the time period for which records to be included in this report.
   - If you want the reporting period to start or end at a specific time of day, change the entry in the appropriate Time box, using the format HH:MM.
   - For Days of the Week, select the check box for each day of the week to be covered in the report.

   **Note:** If the From (date) is weeks or months prior to the current date, it is likely that some of the relevant data is stored in archive files. The report will still run correctly; however retrieving the data from the archive files will take a few minutes.

7. On the People Filter, Location, and Events tabs, specify criteria to be used to narrow down the report results. For more information, see Searching for a Person Record on page 34.

8. On the Run-time Prompts tab, specify the fields users will be prompted to fill in when the report is run:
   
   - In the Fields column, select up to five fields that will require data entry by the report user.
   - In the Prompt column, enter a custom text label for any or all of the selected fields.
   - In the Type column, specify the data entry method (text entry or selection from a drop-down list) for any of the selected fields.
   - In the Width column, enter a specific width (number of characters) for any or all of the selected fields.

   The report results will be filtered based on the data the report user enters in these fields at runtime.

9. On the Output tab, specify any or all of the following: the maximum number of records to be returned, the output format (HTML, CSV, or PDF), and the height and/or width of the report screen display.
10. On the **Schedule** tab:
   - Select the check box for each day of the week you want the report to run.
   - Select the email distribution groups to which you want the report results sent.
   - Select the **To Myself** check box to have the results sent to you.

11. Click **Save**.

12. To run the report, click **Run report**.

   If the defined output format is CSV, you are prompted to open or save the comma-separated values file.

   If the defined output format is HTML or PDF, a separate window opens and displays the results in that format. You can click any column header to sort the data on the column, and you click the header multiple times to switch between an ascending and descending sort order.

13. To delete the report, click **Delete** and click **OK** to confirm the deletion.

14. Click **List** to display a list of the report runs for this report definition.

   On the page that appears, the report runs are listed by date and time. For any run listed, you can use buttons in the Action column to view the results in HTML, PDF, or CSV format, or to delete that run.

### Entering Filter Criteria

When creating a custom history report definition, you can specify filter criteria to narrow down the report results.

**To filter a report by people:**

1. Click the **People Filter** tab and do the following:
   - In the **Fields** column, select up to five data fields the system will use to filter the results. Note that on the drop-down lists, user-defined fields whose labels have not been configured by the system administrator appear as field1, field2, field3, and so on.
   - In the **Comparison** column, select the operator for each data field that the system will use to compare the value you specify with database values for that field. The choices are: **contains**, **is**, **is blank**, **is greater than**, **is less than**, **is not**, **is one of**, **not in**, and **starts with**.
   - In the **Value** column, enter the value for each data field to which the system will compare database values for that field, to determine if there is a match.
   
   For example, to narrow the report results to people whose last names begin with the letter L, select the **Last Name** field, select the **starts with** operator, and enter the value **L**.

   - For the **Report on** option, select **All records visible to this partition** to have all person records that have been made visible in the active partition
included in the report results. Select **Only records native to this partition** to have only person records that are native to the active partition included in the results.

Person records can be made visible in a partition either via the **Share all people with every partition** option on the Network Controller page, or via the **Partitions tab** in the person records themselves.

2. Click **Save**.
   
   The report results will include only people matching your filter criteria.

**To filter a report by location:**

1. Click the **Location** tab.

2. Use the right-arrow buttons ➔ to move portals, readers, elevators, intrusion panels, nodes, portals groups, elevator groups, and reader groups, from the Available lists to the Selected lists.

3. Click **Save**.
   
   The report results will be limited to activity related to the locations you have selected.

**To filter a report by events:**

1. Click the **Events** tab.

2. In the **User** section, use the right-arrow buttons ➔ to move user-defined events and event groups from the Available lists to the Selected lists.

3. In the **System** section, use the right-arrow buttons ➔ to move system-defined events from the Available lists to the Selected lists.

4. Click **Save**.
   
   The report results will be limited to activity related to the events you have selected.

**Duty Log Report**

Select **Administration : Reports : History : Duty Log Report**.

On this page you can request a report showing duty log comments residing in the current security database, including archives, displayed in a four-column table, and view details about each comment and about the Activity Log entry to which it is appended.

**To create duty log reports:**

1. Select **Administration : Reports : History : Duty Log Report**.

2. Click the **From (date)** calendar icon and select a start date for the report.

3. Click the **Thru (date)** calendar icon and select an end date for the report.
You can also enter dates by typing them in the text boxes. If you do not enter a start date, the system will search back through the entire history available in archives. If you do not enter an end date, the system will use the current date.

4. (optional) To apply a filter to narrow down the report results, do either of the following:
   - On the **Operator** drop-down list, select the name of the user whose duty log comments you want to retrieve.
   - On the **Event type** drop-down list, select the type of event for which you want to retrieve duty log comments.

5. In the **Limit to** text box, enter the maximum number of Activity Log entries (with appended duty log comments) you want to retrieve. The default is 3,000 entries.

   Setting the limit to 5,000 or more entries is not recommended, because it may increase the time required for the system to generate and display the results.

6. Click **Run Report**.

   Depending on your system and the number of Activity Log entries that must be displayed, it may take several minutes for the system to generate and display the report results.

7. To print the report results, click **Print** to display the print dialog.

8. To make the report results available for pasting into other applications, click **Copy to clipboard**.

   To use the **Copy to clipboard** button in the Mozilla Firefox browser, you must first enable the button.

9. To expand a single row, click the arrow to its left; to expand all rows, click **Expand all**.

### General Event History Report

Select **Administration : Reports : History : General Event History**.

On this page you can create a variety of reports on system activity. The default General Event History report searches the security database and archive files and returns information on all logged system activity.

Before running the report, you can set search parameters to limit the results to particular time periods, portals, elevators, and event types. You can also limit the number of records the report will return.

**To generate a specific event type report:**

1. Select **Administration : Reports : History : General Event History**.

2. To return only an activity logged during a specific period of time, enter the beginning and end dates in the **From** and **To** date fields, or click the calendar icons and select the dates.
Note: If you do not enter a beginning date for the report, the system will search back through the entire history available in archives.

3. To return only activity at a particular portal, select it from the **At (portal name)** drop-down list.

4. To return only activity at a particular elevator, select it from the **At (elevator name)** drop-down list.

5. To return no more than a certain number of entries, enter that number in the **Limit to** text box.

6. On the **Output** drop-down list, select **HTML** to save the results as an HTML file, or select **CSV** to export the results to a comma-separated values (CSV) file.

7. To return only activity for particular event types, clear the **All event types** check box and select the check box for each event type you want to include in the report.

8. In the **Columns** list, select the number of columns you want for the report.
   
   If you leave the default set of columns selected, the results will include the date and time, the activity occurred, a description of the activity, the user’s name, the location of the activity, and – if there is recorded video associated with the activity – a camera icon you can click to view the video.

9. Click **Run report**.

   If you selected HTML output, the report is displayed directly on this page. You can click the **PDF** link to save it as a PDF file or the **CSV** link to export it as a comma-separated values (CSV) file.

---

**Portal Access Count Report**

Select **Administration : Reports : History : Portal Access Count**.

With this page you can request a report of portal accesses by specific people. You can also specify dates, portals, and a user-defined field from the person detail record.

**To generate a portal access count report:**

1. Select **Administration : Reports : History : Portal Access Count**.

2. Click the calendar icon to select a **From (date)**. This is the start date for the report.

   **Note:** If you do not enter a **From (date)** to specify the beginning date for the report the system will search back through the entire history available in archives.

3. Click the calendar icon to select a **Thru (date)**. This is the end date for the report.
4. Select from the **at Portals** drop-down a specific portal for this report.

5. Select from the **Where** drop-down a specific user-defined field and to the right select a value for this field.

   **Example**: If your person records have a user-defined field called “Department,” you could restrict the report to only those records where the department is “Accounting” or “Manufacturing.”

6. Enter a last name in the **Person (last name)** text box.

7. Click **Run report**.

**People Reports**

Select **Administration : Reports : People**.

**Access Levels Report**

Displays all access levels entered into the system including time specification, reader/reader group, and floor group.

**Credential Audit Report**

Lists existing credentials by their current status settings. For each credential included in the report results, the report also shows the cardholder's name and ID, and the credential number.

Before running the report, you can filter the report results to include only:

- Credentials with particular status settings. In the **Card Status Filter**, move the status settings you want from the Available list to the Selected list.

- Credentials that were not used within a specific number of days from the date they were issued. Enter the number of days in the **List only credentials not used within days** text box.

In addition, if you have full system setup privileges, you can select the **Span All Partitions** check box before running the report to include data from all partitions, rather than from the current partition only.

**Current Users Report**

The Current Users report displays a list of all security system users currently logged in to the security system website.
Creating Reports from System Data

Custom People Report


On this page you can:

- Create custom people report definitions and save them for later re-use.
- Edit or delete saved custom report definitions.
- Run saved custom report definitions to get output in the defined output format (HTML, CSV, or PDF).

To create a custom people report definition:


2. If one or more custom people reports are already defined in the system, click New Report at the top of the report list.

3. On the page that appears, enter a Name for the report.

4. (optional) Enter a Title to be displayed with the report results and a Description that explains the report’s use.

5. On the Columns tab, set up the report columns:
   - For the PDF output, specify the Page Orientation (portrait or landscape) and the Page Size (Letter: 8.5 x 11 inches, or A4: 8.26 x 11.69 inches). The default page margins are 0.5.
   - For the HTML output, specify the Height and Width of the report screen display. The default is 700 points high by 600 points wide.
   - To set up the report columns, select from the Available list each data field that you want to display as a column, then click the right-arrow button to move it to the Selected list.
     - As you add columns, a report guide displayed at the bottom of the page shows their current order and relative widths. The Remaining Width value indicates how many inches of the PDF page width are still available.
     - To change the column order, select individual entries in the Selected list and use the Move up and Move down buttons to move them up and down the list.
     - To specify a different column label and/or column width for any of the data fields, select it in the Selected list and edit the values that appear in the Column label and/or Width fields.

After changing a column’s width, you can click the column in the report guide to view it at its new width. Note that in HTML or PDF output, text that does not fit on a single line within a column will wrap automatically.

If the combined column widths exceed the PDF page width, the Remaining Width value will turn red and the report guide will indicate an error. If you save and run the report without first removing and/or downsizing columns, the data that extends beyond the right page margin.
will be truncated when the results are viewed in PDF format. The HTML view will not be affected.

6. On the People Filter and Access Level tabs, specify criteria to be used to narrow down the report results. For more information, see Searching for a Person Record on page 73.

7. On the Sort Order tab, specify an ascending or descending sort order for up to five fields.

8. On the Run-time Prompts tab, specify the fields users will be prompted to fill in when the report is run:
   - In the Fields column, select up to five fields that will require data entry by the report user.
   - In the Prompt column, enter a custom text label for any or all of the selected fields.
   - In the Type column, specify the data entry method (text entry or selection from a drop-down list) for any of the selected fields.
   - In the Width column, enter a specific width (number of characters) for any or all of the selected fields.

   The report results will be filtered based on the data the report user enters in these fields at runtime.

9. On the Output tab, specify any or all of the following: the maximum number of records to be returned, the output format (HTML, CSV, or PDF), and the height and/or width of the report screen display.

10. On the Schedule tab:
    - Select the check box for each day of the week you want the report to run.
    - Select the email distribution groups to which you want the report results sent.
    - Select the To Myself check box to have the results sent to you.

11. Click Save.

12. To run the report, click Run report.
    - If the defined output format is CSV, you are prompted to open or save the comma-separated values file.
    - If the defined output format is HTML or PDF, a separate window opens and displays the results in that format. You can click any column header to sort the data on the column, and you click the header multiple times to switch between an ascending and descending sort order.

13. To delete the report, click Delete and click OK to confirm the deletion.

14. Click List to display a list of the report runs for this report definition.
    - On the page that appears, the report runs are listed by date and time. For any run listed, you can use buttons in the Action column to view the results in HTML, PDF, or CSV format, or to delete that run.
Entering Filter Criteria

When creating a custom people report definition, you can specify filter criteria to narrow down the report results.

To filter a report by people:

1. Click the People Filter tab and do the following:
   - In the **Fields** column, select up to five data fields the system will use to filter the results. Note that on the drop-down lists, user-defined fields whose labels have not been configured by the system administrator appear as field1, field2, field3, and so on.
   - In the **Comparison** column, select the operator for each data field that the system will use to compare the value you specify with database values for that field. The choices are: **contains**, **is**, **is blank**, **is greater than**, **is less than**, **is not**, **is one of**, **not in**, and **starts with**.
   - In the **Value** column, enter the value for each data field to which the system will compare database values for that field, to determine if there is a match.
     
     For example, to narrow the report results to people whose last names begin with the letter L, select the **Last Name** field, select the **starts with** operator, and enter the value **L**.
   - For the **Report on** option select **All records visible to this partition** to have all person records that have been made visible in the active partition included in the report results. Select **Only records native to this partition** to have only person records that are native to the active partition included in the results.

     Person records can be made visible in a partition either via the “Share all people with every partition” option on Network Controller page, or via the Partitions tab in the person records themselves.

2. Click **Save**.

   The report results will include only people matching your filter criteria.

To filter a report by access level:

1. Click the Access Level tab.

2. Select from the Available list each access level you want to use as a filter, and click the right-arrow button ![right-arrow](> to move it to the Selected list.

3. Click **Save**.

   The report results will include only people with the access levels you have selected.
Occupancy Report

The Occupancy report displays a list of defined Regions. For each region, it shows the number of people currently occupying the region and the maximum number of occupants allowed, if a maximum has been specified.

Photo ID Gallery

The Photo ID Gallery report displays the name and ID photo of each person in the active partition, and the date and time his or her person record was last modified. If the check box *Show persons from other partitions visible to this partition* is selected, the report also includes the pictures and names of people who have been made visible in the current partition.

Click the person's name to go to the detailed person record for that person. Click a letter at the top of the page to narrow down the report results to people whose last names begin with that letter.

Photo ID Requests Report

The Photo ID Request report displays all outstanding photo ID print requests and lists:

- ID
- Name
- Selected photo ID layout
- The person's activation date in the system
- The date of the photo ID print request

You can print photo IDs directly from this report page by clicking the printer icon in the *Action* column. The print photo ID window will appear. Click *Print Photo ID*.

Portal Access Report

The Portals Access report displays the names and access levels of everyone allowed access at the portal you select from the *Portals* drop-down.

Roll Call Report

The Roll Call report lets you select a defined Region from the drop-down and see a list of people currently in that region.
Roster Report

The Roster report displays every person entered into the system and it lists:

- Name
- ID Photo (thumbnail)
- Expiration date
- Date their record was last modified
- User name
- Access level

Select a letter from the alphabet at the top of the page and the report will display only those persons whose last name begins with the selected letter.

You can also choose to Include deleted records by selecting the Yes button. You can exclude deleted records from the report by selecting the No button. By selecting the Only button you can display a report that includes deleted records only.

Time Specifications Report

The Time Specifications report displays all defined time specifications currently in the system. Time specifications define allowed access times. They are used as part of an access level definition.

Start and End times for each time spec are in 24 hour format. As an example, 900 is 9:00 AM and 1700 is 5:00 PM.

Holidays are listed in groups as they were entered.
Setting Threat Levels

Select Administration : Set Threat Level.

If you have administrator access, you can use the Set Threat Level page to set the threat level for all locations or selected locations in the active partition. Depending on how the system threat level settings have been set up, you may need to enter a password to change the threat level.

You can choose to assign a threat level to:

- The default location for the current partition
- The default location and all of its sub-locations
- An individual sub-location
- An individual sub-location and all of its sub-locations

For information about locations, see the security management system online help.

Note: Whenever the default location for the current partition is set to anything other than the Default setting, an icon or a single color representing the current threat level for that location appears in the upper right corner of the application window. The icon or color changes to reflect changes to the location’s threat level.

For example, in a system that uses the default threat level settings, a threat level change from Low to Elevated changes the icon as shown below:

![](Low.png) ![](Elevated.png)

If other users are logged in and viewing the same partition, their threat level icons will be updated within one minute.

Threat level changes might change the behavior of access levels, portals, portal groups, and events.

To set the threat level:

1. Select Administration : Set Threat Level.
2. If a password is required for making threat level changes, enter it in the Password box.
3. Select the threat level you want to apply
4. From the Applies to Location drop-down list, select the location to which you want to apply the threat level. You can apply it to the default location for the current partition or to any of its sub-locations.
5. To apply the threat level change to all sub-locations of the location you
selected at step 4, select the **Also apply to sublocations** check box.

6. Click **Save**.

   The threat level change is written into the Activity Log.

---

**Note:** It is also possible to change the threat level using an event action or an
API command.
Backup System and Other Utilities

Backing Up the Security Database

The system data is regularly backed up to the controller each night at 00:15 hours. The Sunday backup is a Full Backup. Backups on Monday through Saturday are Differential backups.

If an FTP server or NAS drive is configured all backups will be written there as well. We strongly recommend that an FTP site or a NAS server be set up for storing system backups off the controller.

You can perform additional backups whenever you want.

To back up system data:
2. Enter a comment to explain the purpose of this backup.
3. Click Full Backup.
4. When the backup is complete it is listed in the Existing Backups section. You can download a copy of this backup to a disk drive by clicking the get link in the Download? column.

Configuring a NAS (network attached storage):

Note: Once the NAS is properly set up the backup procedure backs up configuration, people, and log data, as well as user photos, floor plan images, badge designs, sound files, and so forth.

The regular nightly backup at 00:15 hours will write to this location if it is properly configured. To properly configure a NAS requires that both Network Administrator and Security System Setup tasks are completed as described below.

Network Administrator tasks:
1. Create a network share on the same sub-net as the network controller.

   Note: The share name may not include spaces.

2. Create a local user account and password (as opposed to a Domain user account) for the network controller to access the network share.
3. Grant the user account share permissions and security permissions for the network share.
Security system setup tasks:

1. Select **Setup : Network Resources : Network Storage**.
2. Complete this page with the information for the share location created above.
3. Click **Save**.
4. Click **Backup Now**.

Configuring an FTP server:

**Note:** Once the FTP server is properly set up the backup procedure backs up configuration, people, and log data, as well as user photos, floor plan images, badge designs, sound files, and so forth.

The regular nightly backup at 00:15 hours will write to this location if it is properly configured. To properly configure an FTP server requires that both Network Administrator and Security System Setup tasks are completed as described below.

Network Administrator tasks:

1. On the FTP Server create a user name, password, and directory for the security system FTP Backups.

   **Note:** A password is optional. The backup directory must be created at the root level of the FTP server.

2. Decide whether Active mode FTP or Passive mode FTP shall be used and ensure that firewalls will not block the needed ports.

   **Note:** When using active FTP, TCP ports 20 and 21 must be open to the FTP server for FTP backups from the Network Controller. When using passive FTP port 20 will not be required.

   Ports must also be left open to the Network Controller for FTP server responses. The network administrator must set up these ports.

Security System setup tasks:

1. Select **Setup : Network Resources : FTP Backup**.
2. Complete this page with the information for the FTP site created above.
3. Click **Save**.
4. Click **Backup Now**.
Arming and Disarming Alarm Panels

Select Administration : Arm Alarm Panel.

Burglar alarm panels can be integrated with your access control system. On this page you can arm or disarm an alarm panel.

To arm and disarm an alarm panel:

   
The page displays a table listing all alarm panels configured in the system, their current states, and any activity information.

2. Click the Arm/Disarm link in the Action column.

   **Note:** You cannot arm a panel if it shows any zone activity.

3. A password challenge is displayed and you must enter your password to arm or disarm the panel.

4. If you are arming the panel, the Panel arming warning output activates for the Warning duration.
Where to Go for More Information

Documentation that you might need for operating your system can be downloaded from the S2 Security web site (http://www.s2sys.com).

After logging into the secure area for integrators and consultants, certified systems integrators can select their product type and software version from Support Central to locate links to manuals, technical notes, software, and utilities.

See the Getting Started section of the security management system online help for answers to frequently asked questions and links to additional technical documentation.

For further assistance, please contact S2 Technical Support at +1.508.663.2505 or support@s2sys.com.
## Index

**A**

- Access Control tab · 37, 45
- Access History report · 60
- Access History Report
  - creating · 60
- access levels · 37, 45
- Access Levels report · 70
- activate outputs · 11
- activation date · 46
- activity for a person
  - trace · 47
- Activity Log · 3
  - numbers · 8
  - reason codes · 9
  - reset_type messages · 9
  - widget · 6
- Activity Log messages
  - names · 8
  - times · 8
- Activity Log tab · 13
  - Monitoring desktop · 13
- add a person · 33
- Administration page
  - General Event History Reports · 68
- alarm
  - color · 19
  - display color · 19
  - escalated · 20
  - offered · 19
  - owned · 19
  - priority · 19
  - SLA violated · 20
- alarm state
  - progress bar · 20
  - timer · 20
- Alarm Workflow
  - configurable · 20
  - widget · 19, 20, 21
- anti-passback
  - regional privileges · 46
- anti-passback rules · 23
- archives · 60
- arming alarm panels · 80
- arming inputs · 11
- As Built report · 58
- assigning an extended unlock time · 49
- Audit Trail report · 61
- Auto-Monitor · 12

**B**

- backing up · 78
- FTP site · 78
- NAS server · 78
- badges · 54
- printing · 56

**C**

- Camera Monitor tab · 14
- Camera Preset
  - drop-down list · 4
- camera speed · 4, 15
- camera view
  - multi-camera · 4
  - quad · 4
- Camera Views tab
  - four-camera view · 14
  - picture-in-picture view · 14
- cameras · 3
  - thumbnail images · 11
- Cameras menu · 3
- Cameras report · 58
- Cameras tab · 14
- category filter · 7
- change person data · 34
- changing password · 52
- close button · 2
- Configuration report · 58
- configuring
  - FTP server · 79
  - NAS server · 78
- Contact tab · 37
- Credential Audit · 44
- credential audit report
  - credentials not used · 70
  - filtering · 70
  - partitions · 70
  - status setting · 70
- Credential Audit Report · 70
- credentials
  - lost · 51
- CSV Export report · 63
- Current Users report · 70
- Custom History report · 64
Index

D

deactivate outputs · 11
delete badge layouts · 56
delete person record · 34
disarming alarm panels · 80
disarming inputs · 11
duty log report · 67
duty log entry
  clipboard icon · 5
duty log message · 21
  alarm workflow · 21
duty log messages · 3
duty log response
  enter duty log message · 5
  preset text entry · 5

E

Elevators report · 58
evacuation plans
  ending · 32
  starting · 31
event
  definition · 20
  policy · 20
Events tab · 15
  acknowledge · 15
  alarms · 15
  Monitoring Desktop · 13
expiration date
  for an access level · 46
  expiration notification, enabling for a person record · 47

F

filtering
  Clear Filter icon · 7, 8
filters
  category filters · 6
  text filters · 6
Flash Player 9.0 · 15
  browser plug-in · 11
  configuring floorplans · 11
  viewing floorplans · 11
Floor Groups report · 59
floorplans
  alarm icon · 11
  camera icon · 11
  cameras · 11
  input icon · 11
  live monitoring · 3, 5, 11
  monitoring · 11
  output icon · 11
  portal icon · 11
  portals · 11
  temperature icon · 11
  temperature sensors · 11
  thumbnail image · 11
  view alarms · 3, 5
Floorplans tab · 15

G

General Event History · 68
granting passback grace · 3

H

help
  contents button · 1
  navigation pane · 1
  Search button · 1
  topic pane · 1
History report · 60
holidays · 75
Holidays report · 59
Home Page · 12
hot stamp number credentials · 42

I

ID number
  person record · 34
inputs
  arming · 11
  disarming · 11
Internet Explorer
  version · 16

K

Keypad timed unlock · 48

L

live monitoring · 3
Live Monitoring menu
  view floorplans · 5
  view system activities · 5
Login tab · 38
Logitech QuickCam · 54
Index

M

messages, color-coded  
Activity Log · 8
Monitor menu  
duty log entries · 3
granting passback grace · 3
live monitoring · 3
partitions · 3
view cameras · 3
viewing and unlocking portals · 3
Monitoring Desktop  
camera views · 13
events · 13
fixed layout · 13
floorplans · 13
tabbed pages · 13
multi-camera view · 3, 4
My Alarms  
table · 21, 22

N

names variables  
Activity Log messages · 8
network loss message · 9
normal reset message · 9
numbers  
Activity Log · 8

O

Occupancy report · 74
offered alarms · 21, 22
online remote lockset · 25
Other Contact tab · 37
outputs  
activate · 11
deactivate · 11
owner  
of alarm · 20

P

partition  
alarm · 19
partitions · 3
administrative functions · 30
configuring resources · 30
credential audit report · 70
monitoring · 18, 30
selecting · 3, 30
Partitions tab · 39
passback  
vioations · 47
passback grace  
granting · 23
passwords  
rules · 53
People menu  
add · 31, 33
change/delete · 31, 33
People report · 70
person record  
about · 36
accessing via Activity Log · 8
creating · 33
Photo ID Gallery report · 74
Photo ID Request report · 74
Photo ID tab · 37
photo IDs  
badges · 54
creating · 54
printing · 54, 55
PIN  
auto-generated · 48
for Keypad timed unlock · 48
four to six digits · 48
PIN text box  
person record · 48
policy  
event · 20
Portal Access Count report · 69
Portal Groups report · 59
portals · 3
Portals Access report · 74
Portals report · 59
power on reset message · 9

Q

quotation marks  
not in passwords · 53

R

Reader Groups report · 59
reason codes  
access denied messages · 9
Activity Log · 9
Recent Activity tab · 40
report  
changes to scheduled actions · See Audit Trail report
reports · 58
Access History · 60
Access Levels · 70
Audit Trail · 61
Camera Presets · 58
Cameras · 58
Configuration · 58
CSV Export · 63
Current Users · 70
Custom History · 64
Duty Log · 67
Elevators · 58
Floor Groups · 59
General Event History · 68
History · 60
Holidays · 59
Occupancy · 74
People · 70
Photo ID Gallery · 74
Photo ID Request · 74
Portal Access Count · 69
Portal Groups · 59
Portals · 59
Portals Access · 74
Reader Groups · 59
Resources · 59
Roll Call · 74
Roster · 75
Threat Level Groups · 60
Threat Levels · 59
Time Specifications · 75
reset_type messages
Activity Log · 9
Resources report · 59
revoking credentials · 52
Roll Call report · 74
Roster report · 75

S

schedule
portal unlock · 3
search
in help · 1
show TOC · 12
software updates
web site · 1
splitter bar · 20
start page · 12
starting and ending evacuation plans · 31
state
of alarm · 20

T

temperature graphs · 11
templates for creating person records · 33
text filter · 7
threat level · 13
threat level groups report · 60
threat levels report · 59
thumbnail images
cameras · 11
time messages
Activity Log · 8
Time Specifications report · 75
topic pane
in help · 2
trace a person's activity · 47

U

undelete person record · 34
unlocking portals · 3, 13
upload badge layouts · 57
user role
monitor · 38
setup · 38, 39
User Tasks widget · 12
User-defined tab · 37

V

Vehicles tab · 38
ViconNet DVR · 4, 15
video stream · 14
Video Stream · 12
view cameras · 13
view history · 13

W

watchdog timer reset message · 9
web site
S2 Security · 1
software updates · 1
specifications · 1
Widget Desktop · 16
background · 18
custom real-time display · 16
default layout · 16
exiting · 19
help icon · 19
layouts · 17
load layout · 18
widgets
definition · 16
properties · 17