

S2 NetBox User Guide

Created from S2 NetBox Help Version 4.8.01

February 2016



S2 Security Corporation

One Speen Street

Suite 300

Framingham MA 01701

www.s2sys.com

S2 Support: 508 663-2505

Document # NB-UG-16

© S2 Security Corporation 2004-2016. All rights reserved.

This guide is protected by copyright and all rights are reserved by S2 Security Corporation. It may not, in whole or in part, except insofar as herein directed, be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form without prior written consent of S2 Security Corporation.

Third party trademarks, trade names, product names, and logos may be the trademarks or registered trademarks of their respective owners.

The following are trademarks or registered trademarks of S2 Security Corporation:

- S2 NetBox®, S2 NetBox® Plus, S2 NetBox® Extreme, S2 NetBox® Enterprise
- S2 Enterprise® Select, S2 Enterprise® Ultra, S2 Enterprise® Ultra 2
- S2 MicroNode™, S2 MicroNode™ Plus
- S2 Magic Monitor™
- S2 Global®
- S2 NetVR®, S2 NetBox® VR, S2 NetBox® VR Quatro
- S2 Mobile Security Officer®
- S2 Pronto®, S2 Pronto® 2, S2 Pronto® VR

S2 CumulusSM is a service mark of S2 Security Corporation.

Table Of Contents

Getting Started	1
The Home Page.....	1
The Page Bar	2
The Navigation Palette	2
The Command Palette.....	5
The About Dialog Box	6
Changing Your Password.....	7
Valid Password Rules.....	8
Tips for Strong Passwords.....	8
System Setup Checklist	9
Using Help	10
How do I get to Help?	10
Help Conventions	10
Navigating and Printing Help.....	10
Video Tutorials	11
Monitoring the System	13
Monitoring the Activity Log	13
Navigating to a Person Record from the Activity Log.....	14
About Activity Log Messages	14
Reason Codes	15
Filtering Activity Log Entries	16
Applying Text Filters	17
Applying Category Filters	17
Adding Duty Log Messages to the Activity Log	18
Monitoring Cameras.....	18
Monitoring NetVR Cameras.....	20
Monitoring Multi-Camera Views.....	22
Monitoring NetVR Multi-Camera Views	23
Monitoring Floorplans.....	26
Monitoring High Availability (HA) Status	27
Using the Monitoring Desktop.....	29
Filtering the Data Shown on a Tab	29
Events Tab.....	29
Activity Log Tab	30
Cameras Tab.....	30
Camera Views Tab	30
Camera Monitor Tab.....	30

Floorplans Tab	31
Threat Level Widget	32
Portal Unlock Widget	32
Photo ID History Widget	32
Cameras Widget.....	32
Granting Passback Grace.....	33
Unlocking Portals and Viewing Their Status	33
Switching a Portal to a Locked or Unlocked State.....	36
The Widget Desktop	37
Using the Widget Desktop.....	37
Summary of the Available Widgets	38
About Widget Properties	39
Moving, Sizing, Minimizing, and Closing Widgets	40
Changing a Widget's Unique Properties.....	41
Changing a Widget's Scope Properties	42
Scope Properties You Might Be Able to Change	43
More About Individual Widgets.....	44
Administering the System	65
Arming and Disarming Alarm Panels	66
Data Operations	66
Overview of Data Operations	66
Performing Data Operations Tasks	68
Automatic Data Operations	69
Data Operations Results	70
Managing Evacuations	72
Using the Forensic Desktop	73
Starting a Forensic Search	74
Working with Forensic Cases.....	75
Using the Forensic Desktop Tools.....	75
Searching Recorded Video	76
Composing Forensic Cases.....	88
Printing and Exporting Forensic Cases	90
Handling Lost Cards.....	91
People Administration	92
Adding People to the System	92
Finding and Changing Person Records	93
Managing Email Distribution Groups	114
Creating and Printing Photo ID Badges	114
Report Administration	122

Configuration Reports.....	122
History Reports	125
People Reports.....	136
Setting Up Automatic Email Distribution of Custom Reports	142
Enabling Copy to Clipboard in the Mozilla Firefox Browser.....	142
Scheduling Actions.....	143
Scheduling Actions Across Time Zones.....	146
Setting Threat Levels	147
Utility Administration.....	149
Backing Up the System Data	149
About Archive Files.....	150
Configuring Duty Log Messages.....	150
Deleting Photo ID Layouts	151
Uploading Photo ID Layouts.....	151
System Data for Photo ID Layouts.....	152
Configuring the System	155
System Setup Checklist	155
Access Control.....	157
Setting Up Access Levels	158
Specifying Card/Keypad Formats	160
Customizing Credential Attributes.....	164
Creating Credential Profiles	165
Elevator Access Control	166
Defining Keypad Commands	175
Setting Up Locations.....	176
Person Record Setup	177
Portal Setup.....	180
Setting Up Double Card Presentation Mode.....	189
Reader/Keypad Setup.....	192
Configuring Regional Anti-Passback	196
Creating a Temporary Credential Policy.....	198
Access Control Utilities.....	198
Alarms	204
Alarm Filter Setup	205
Alarm Panel Setup.....	207
Creating Alarm Workflow Policies	209
Event Setup	210
Input Setup	217
Configuring DMP Intrusion Panels.....	223

Output Setup	224
Video	226
Creating Camera Definitions.....	227
Creating Camera Groups.....	229
Setting the Camera Menu Order	229
Creating Camera Preset Positions	230
Setting Up Camera Tours.....	231
Setting Up Camera Types	232
Setting Up Multi-Camera Views	233
NetVR Appliances	234
NVRs/DVRs.....	237
Magic Monitors.....	250
Creating Evacuation Plans	251
Floorplans	252
Composing Floorplans.....	252
Creating Floorplan Groups.....	254
Uploading Floorplan Background Images	255
Network Resources	255
Setting Up an LDAP Server.....	256
Domain Name Server Settings.....	257
Setting Up Remote Logging	257
Setting Up an Email Server for the Controller	259
FTP Backup Settings.....	259
Setting Up the Network Storage Location.....	261
Setting Up the Network Time Server.....	262
Site Settings.....	263
Creating Custom Menus.....	264
Mercury Panel Setup.....	265
Network Controller Setup.....	278
Network Node Setup	293
Partition Setup	300
ASSA ABLOY Remote Lockset Setup	306
Reports.....	323
Activating a Software License File.....	324
Creating Rules to Change System Behavior	325
Creating User Roles.....	326
NetVR Appliances	331
System Maintenance.....	334
Backing Up the System Data	335

About Archive Files	336
Restoring the System Data.....	336
Managing System Health	337
Managing Storage	338
Updating the System Software	343
System Maintenance Utilities.....	344
Threat Levels	347
Adding, Changing, and Deleting Threat Levels	347
Setting the Threat Levels Menu Order	348
Threat Level Settings.....	349
Setting Up the Threat Level Escalator App	350
Setting Up Threat Level Groups.....	352
Using Threat Levels to Change System Behavior	353
Effects of Applying a Threat Level Group: Example.....	356
Time	357
Creating Holidays	357
Setting the Network Controller Time.....	358
About Time Specs	359
Creating Time Specs.....	361
Creating Time Spec Groups.....	363
Widget Desktops	363
Composing Widget Desktop Layouts.....	364
Grouping Widget Desktop Layouts.....	366
Summary of the Available Widgets	366
Widget Properties You Can Configure	367
Configuring a Widget's Common Properties.....	368
Configuring a Widget's Unique Properties.....	369
Configuring a Widget's Scope Properties	370
Summary of the Widget Scope Properties	372
More On Configuring Specific Widgets	374
How Groups are Used in the System	390
Index	395

Getting Started

This section provides information on the following topics.

The Home Page	Accessing the default Home page to view system activity, issues that might require attention, and video.
The Page Bar	Accessing top-level controls that are used to open the navigation palette and the command palette.
The Navigation Palette	Accessing pages you have permission to view based on your user role.
The Command Palette	Accessing a Logout link and controls for performing common tasks and access control functions.
Changing Your Password	Changing the password you use to log into the security management system.
System Setup Checklist	View the steps required to set up the system.
Using Help	Accessing, navigating and printing context-sensitive help.


The Home Page

The Home page is the first page you see after logging in. To return to the Home page from anywhere in the application, click this button in the [page bar](#):



On the default Home page you can:

- Use the **Activity Log** widget to view recent activity related to system events.
- 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 appear on the Home page.

If your system includes a NetVR integration use the Configure Viewer  drop down list in the upper right corner of the Video Stream widget to select a camera matrix and camera to view.

NOTE: To set a different page as your Home page, go to that page and select **Set as Home** from the [command palette](#). You will still be able to view the default Home page by selecting **Monitor : Monitoring Home Page**.

See also: [Monitoring the Activity Log](#)

[Using the Monitoring Desktop](#)

[Filtering Activity Log Entries](#)

[Using the Widget Desktop](#)

[The Auto-Monitor Widget](#)

[Using the Forensic Desktop](#)

The Page Bar

The page bar appears at the top of the application window. It includes:

- **Top-level controls.** These are used to open the [navigation palette](#) on the left side of the screen. The navigation palette provides access to pages you have permission to view based on your user role.
- **A command palette control.** This is used to open the [command palette](#) on the right side of the screen. The command palette provides a Logout link and controls for performing common tasks and access control functions.
- **System information.** The company name as it appears on the System tab of the [Network Controller page](#), and for a partitioned system, the name of the active [partition](#) if it is different.
- **Status information.** The number of [active alarms](#) in the system and the current [threat level](#). If there are active alarms, the count will be shown on the alarm status button:



Clicking the button opens the [Monitoring Desktop](#), where information about the events associated with active alarms is available on the Events tab.








NOTE: If your System Upgrade and Support (SUSP) license is about to expire or has already expired, you will be alerted by an Activity Log message and a blinking icon in the page bar. For information on obtaining a new license and acknowledging the alert to disable the blinking icon, see [Managing System Health](#).


The Navigation Palette

The navigation palette provides access to pages you have permission to view based on your user role. It is accessed via top-level controls that appear on the left side of the [page bar](#).

About the Top-Level Controls


Depending on your user role, some or all of the following top-level controls will be available on the page bar.

Top-Level Control	Displays in the Navigation Palette	Available To
Home Page 	The default home page	All users
Custom Menu 	Controls for accessing a custom set of pages that has been assigned to you Selecting this control displays the name of the custom menu.	Users to whom custom menus have been assigned
Monitor 	Controls for accessing the monitoring pages	Users with permission to view one or more of the monitoring pages
Administration 	Controls for accessing the administration pages	Users with permission to view to one or more of the administration pages
Configuration 	Controls for accessing the configuration pages	Users with permission to view one or more of the configuration pages
Search 	A text box for performing searches (See Searching for a Page below.)	All users
Recent 	Controls for accessing recently displayed pages	All users, after at least one page has been viewed during the current session

Up to five top-level controls can appear on the page bar at one time. If additional controls are available, hovering over the More Controls button  displays them in a drop-down list. When you select a control from the list, it swaps places with the last visible control on the page bar.

Opening the Navigation Palette

Each of the top-level controls (except the Home Page control) behaves in one of the ways described below, depending on whether you select it or hover over it:

- Selecting the control opens the navigation palette and pins it to the work space. The page displayed in the work space is shifted to the right so none of its contents are obscured. A small triangle appears below the control to indicate that it is pinned: 

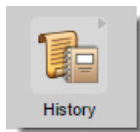
The navigation palette remains visible until you select the control again to unpin it.

- Hovering over the control opens the navigation palette but does not pin it to the work space. The palette disappears when you move away from it.

Navigating to a Page

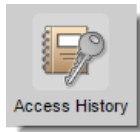
Two types of controls appear in the navigation palette:

- **Navigation controls.** A small arrow appears in the upper right corner of each navigation control. Selecting the control displays a set of related controls in the navigation palette. For example, selecting this control (under *Administration : Reports*) displays controls for accessing the available History reports:

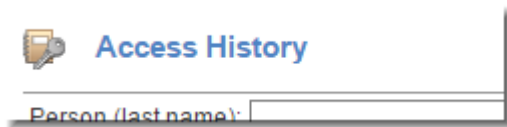


To return to the previous set of controls, click this button  at the top of the navigation palette.

- **Page controls.** Selecting a page control opens the associated page in the work space. For example, selecting this control opens the page for creating Access History reports:





If you get lost after selecting a page control from an unpinned navigation palette, you can click the icon next to the page name to restore that palette:



Searching for a Page

If you do not know where a particular page control is located, you can perform a search to find all controls matching specific text.

To search for a page:

1. Click the **Search** control  on the page bar. If the Search control does not appear on the page bar, hover over the More Controls button  and select it from the drop-down list.
2. Enter text in the search field that appears.
3. Press **ENTER**.

All matching controls appear below the search field. For example, a search for the word "event" returns options for accessing the General Event History page, the Events page, and the Event Groups page.

See also: [The Home Page](#)

[The Command Palette](#)

[Creating Custom Menus](#)

The Command Palette

The command palette is accessed via this control on the right side of the [page bar](#):



When the palette is displayed on the right side of the screen, you can use it to:

- Log out of the system and view information about the user who is currently logged in.
- Perform common tasks such as printing, getting help, and changing your password.
- Perform access control functions without leaving the current page.

The command palette control behaves differently depending on whether you click it or hover over it:

- Clicking the control displays the command palette and pins it to the work space. A small triangle appears below the control, as shown below. The command palette remains visible until you click the control again to unpin it.



- Hovering over the control displays the command palette but does not pin it to the work space. The palette disappears when you move away from it.

The command palette's title bar displays a Logout link and the name and photo of the user who is currently logged in. Below this is a section for performing common tasks, and a section for performing access control functions without leaving the current page.

Commands for Performing Common Tasks

Set As Home Makes the current page your Home page. You will still be able to view the [default Home page](#) by selecting *Monitor : Monitoring Home Page*.



Print Displays the Print dialog box so you can print the current page.



Help Displays [help](#) for the current page.



Tutorials Displays a list of video [tutorials](#) you can view.



About Lets you start an online Support session and export [system information](#) to a CSV file you can share with your S2 Support representative.



Change Password Lets you change your [login password](#).



Commands for Performing Access Control Functions

Threat Level Lets you change the [threat level](#) for all locations or selected locations in the active partition.



Change Partition Lets you select a different [partition](#).



Duty Log Entry Lets you add a [duty log message](#) to the Activity Log.



Unlock Portal Lets you [unlock a portal](#) momentarily or schedule an extended portal unlock.



See also: [The Page Bar](#)

[The Navigation Palette](#)

The About Dialog Box

Select **About** from the [command palette](#).

You can use buttons at the bottom of the About dialog box that appears to:

- Start an online support session.

- Export information from the About page to a CSV file that you can share with your S2 Support representative.

There are two data views available: Licenses and System Information.

Click **Licenses** to see the following:

- **Product Info:** The name of the S2 product you are using.
- **Product Key:** A key containing the system features and limits.
- **Activation Key:** A key containing the system activation date.
- **In Service Date:** The date on which the system came into service.
- **Expiration Date:** The date after which you will no longer be able to upgrade the system until a license renewal is purchased and a new Product Key and Activation Key pair is applied.
- **License Type:** The type of license applied to the system.
- **Licenses:** A list of the system features included with your license.

Click **System Information** to see the following:

- Information about the installed software, such as the version and revision numbers and any applied system updates.
- For a system with an S2 NetVR integration, information about the NetVR server and software.
- **License Identifier:** A number that uniquely identifies the license applied to the system.
- Information about the computer running the security management system: the MAC address, IP address, physical memory size, and hardware platform.

Changing Your Password

Select **Change Password** from the [command palette](#).

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 the Change Password dialog box.

To change your password:

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

NOTE: You will see an error message if any of the following are true:

- The new password is identical to your current password.
- The confirmation password entered at step 3 does not match the new password selected at step 2.
- The new password does not conform to the valid password rules set for your system. See the next section for more information.

Valid Password Rules

- If a **Minimum password length** is set for your system (on the [Network Controller page](#)), a password must include at least the minimum number of characters specified.
- By default, a password cannot contain single or double quotation (' ") marks.
- or -
- If your administrator specified (on the [Network Controller page](#)) that passwords must contain letters, numbers, and special characters, you can use any of the following special characters in your password:

At sign	@	Greater-than sign	>
Ampersand	&	Less-than sign	<
Asterisk	*	Number sign	#
Brackets, curly	{ }	Parentheses	()
Brackets, square	[]	Period	.
Caret	^	Plus sign	+
Colon	:	Question mark	?
Comma	,	Quotes, single	'
Equals sign	=	Quotes, double	"
Exclamation mark	!	Semicolon	;
Forward slash	/	Underscore	_
Hyphen	-	Vertical bar	

Tips for Strong Passwords

- Passwords should be changed periodically. If your administrator has set an expiration period for passwords, you will be required to change your password after the specified number of months have elapsed.
- Do not use passwords that can be easily guessed, such as names of family members or birth dates.
- Your password should contain at least one alphabetic character and one numeric character, even if your administrator has not specified that passwords must contain letters, numbers, and special characters.

See also: [Creating a System User Account](#)

[Setting Up LDAP or Active Directory Server](#)

System Setup Checklist

When setting up your system, complete the steps below in the order given below. The list is ordered to ensure that prerequisite steps are completed first. Use the **Back** button to return here after each step is completed.

IMPORTANT: The first time you log into the system after configuring initial settings for the controller, as described in the [Initial Software Setup Guide \(PDF\)](#), be sure to change the default password for the administrator account (admin). Select Support/Utilities : [Change Password](#). Give the new password for the admin account to the network administrator or security director.

(1) Entering Site Settings:

- [Network Controller](#)
- Network Nodes

(2) Setting up Time Specs:

- [Holidays](#)
- [Time Specs](#)

(3) Setting up Alarms:

- [Outputs](#)
- [Output Groups](#)
- [Events](#)
- [Inputs](#)
- [Input Groups](#)
- [Alarm Panels](#)

(4) Setting up Access Control:

- [Card Formats](#)
- [Person Sections](#)
- [Readers](#)
- [Reader Groups](#)
- [Portals](#)
- [Portal Groups](#)
- [Elevators](#) and [Floors](#)
- [Floor Groups](#)
- [Access Levels](#)

(5) Setting up Cameras:

- [Types](#)
- [Definitions](#)
- [Menu Order](#)
- [Presets](#)
- [Views](#)
- [Video Management Systems](#)

(6) Setting up Floorplans:

- [Upload](#)
- [Compose](#)

(7) Setting up Network Resources:

- [Domain Name Server](#)
- [Email Settings](#)
- [Network Storage](#)
- [Time Server](#)

(8) System Maintenance:

- [Back Up Database](#)
- [Manage Storage](#)

See also: [Setup Page](#)


[Initial Software Setup Guide \(PDF\)](#)

[Network Node Hardware Installation Guide \(PDF\)](#)

The hardware installation guide for your system.

Using Help

How do I get to Help?

- Select **Help** from the [command palette](#).
- If you see this icon  on a page, click it to get specific help for a particular option or set of options.

NOTES: Some features described in help may be unavailable in certain product variants.

Depending on your browser, opening a PDF from help might cause the help window to move behind the main browser window. To display help again, press ALT+TAB, hold down the ALT key, and select S2 Security Help from the list of running programs.

Help Conventions

The help system is context-sensitive. When you click **Help** from any page in the application:

- If a help topic is available for the current page, it appears in the help window.
- If no help topic is available for the current page, the default help topic appears in the help window.


To assist you in finding specific fields, buttons, and other elements in the application, their names are displayed in **bold blue** within help topics.

Navigating and Printing Help

The navigation pane appears on the left side of the help window.

- By clicking the **Contents** and **Search** buttons, you can switch between the help table of contents and the search feature:



- To hide the navigation pane, click the close button . 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 on the right side of the help window.
- To use the search feature, enter the word you want to search for 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.

You can also use the buttons displayed at the top of each help topic to navigate and print help:

- **Back:** Brings you back to the previous topic.
- **Index:** Displays the Index.
- **Print:** Displays the Print dialog box so you can print the current help topic.

Video Tutorials

Select **Tutorials** from the [command palette](#).

In the list that appears, click any of the links to play a video tutorial in a separate window.

You can also play a video tutorial by selecting it from this tool in the upper right corner of the [Forensic Desktop](#):



Monitoring the System

This section provides information on the following topics.

Activity Log	Viewing recent activity related to system events.
Cameras	Viewing individual camera views.
Camera Views	Viewing multi-camera views.
Floorplans	Viewing the state of alarms and other system resources on a floorplan.
High Availability Status	Viewing the status of your High Availability (HA) configuration. The HA Status page will appear only if your system is licensed for HA.
Home Page Monitoring	Viewing the default Home page.
Monitoring Desktop	Viewing system information using a static-format display.
Passback Grace	Gracing an individual from an anti-passback violation on his or her next card access. This option appears only if <i>Show Passback Grace as Menu Option</i> is selected on the Network Controller page .
Portal Status	Viewing a list of portals and their status, unlock a portal, and schedule a portal unlock.
Widget Desktop	Viewing system information using a custom, real-time display.

NOTE: To set the page you are currently viewing as your Home page, select **Set As Home** from the [command palette](#).



See also: [Composing Widget Desktop Layouts](#)

[Anti-Passback Applications \(PDF\)](#)

Monitoring the Activity Log

Select **Monitor : Activity Log**.

The Activity Log lets you view recent activity related to system events. When you first open the Activity Log, it lists 301 of the most recent events. If you remain on the page, additional events appear in the list, until up to 1,000 of the most recent events are listed.

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

You can use the Activity Log to monitor activity from this page and from the following locations:

- The [Monitoring Desktop](#), which includes two Activity Log tabs.

- The [Widget Desktop](#). If the Activity Log widget is not already displayed on the desktop, you can add it for the current monitoring session.
- The default [Home page](#), which includes an Activity Log widget.

NOTE: During a monitoring session, you can filter the current list of log entries to focus on specific information. See [Filtering Activity Log Entries](#) for more information.

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 in an event listed in the Activity Log 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 when it is accessed from elsewhere in the application will apply when it is accessed from the Activity Log.

About Activity Log Messages

The messages associated with the events lists in the Activity Log 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 requests in the active partition by individuals whose activity is being [traced](#).
- Black is used for all other messages.

Activity Log messages contain message text and a number of variables, as described below.

Times

Each Activity Log message begins with the controller time—the time the event was communicated to the Network Controller. If **Always show device & controller times in Activity Log** is enabled on the [Network Controller page](#), the time when the event actually occurred on the node is displayed in square brackets to the right of the controller time.

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>, <threatlevel>, and <alarmpanel>. 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 variables such as <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 [<reason code>] messages for "Access denied" and "Access granted" log entries are described 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.

Reason codes for "Access denied" log entries:

- [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. You will also see this reason code if the credential is used at a reader configured for a Mercury panel but the data format is not defined as a "Mercury-supported" format.
- [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 at the 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 on the [Network Controller page](#).
- [PIN] - The person entered an invalid PIN.
- [PASSBACK VIOLATION] - This credential was presented to enter a region where the cardholder is 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.

Reason codes for "Access granted" Log Entries

- [DURESS] - A cardholder presented his or her credential 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 a credential that was 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.

See also: [Access History Reports](#)

[Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Entering Duty Log Comments into the Activity Log](#)

Filtering Activity Log Entries

While 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 containing a specific text string.
- **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 belonging to a particular category.

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

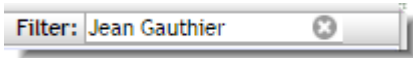
NOTES: If filters were not enabled for an Activity Log widget when it was created, that instance of the widget will not have text and category filtering capabilities.


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 uppercase or lowercase characters.

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



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 end 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.
- **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 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.
- **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.
- **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 successful access requests.
- **Access Denied**: Select to view only entries for unsuccessful 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.

See also: [Monitoring the Activity Log](#)

[Using the Monitoring Desktop](#)

[The Home Page](#)

[Using the Widget Desktop](#)

Adding Duty Log Messages to the Activity Log

Select **Duty Log Entry** from the [command palette](#).

To add a duty log message to the [Activity Log](#), you can:


- Use the Duty Log Entry dialog box that appears to enter your message, or to select a preset message if any have been configured. The message will be appended to a new event in the Activity Log.
- While viewing the Activity Log, append a duty log message to an existing event.

NOTE: You can also use the Duty Log Entry widget on the [Widget Desktop](#) to add duty log messages.


To add a duty log message to the Activity Log:

1. After selecting **Duty Log Entry** from the command palette, do one of the following:
 - Enter your message into the **Enter duty log message** text box.
 - If there are preset messages available on the **Use Duty Log Response** drop-down list, select a message from the list.

2. Click **OK**.

A new event, *Duty log entry by <username>*, is added to the Activity Log. Click the clipboard icon () that appears at the end of the event to view your duty log message.

3. To append a duty log message to an event listed in the Activity Log, double-click the event, enter the message in the dialog box that appears, and click **Save**.

Click the clipboard icon () that appears at the end of the event to view your duty log message.

See also: [Configuring Duty Log Responses](#)

[Duty Log Reports](#)

[Monitoring the Activity Log](#)

[Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Composing Widget Desktops](#)

Monitoring Cameras

Select **Monitor : Cameras**.

On this page you can select any camera defined in the system to monitor a live camera view. You can select an IP camera or an NVR/DVR camera.

For information about NetVR camera monitoring functions, see [Monitoring NetVR Cameras](#).

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.)

Use the controls described below to review recorded video, aim the camera, move it to its home position, zoom in and out, and adjust the speed of camera movement.



Click to display VCR controls at the bottom of the camera widget. You can use these VCR controls to review recorded video.

NOTE: The VCR icon will appear only if you are viewing a video management system (VMS) camera.



Click to display PTZ controls.



Click to move the camera to its preset home position.



Click an arrow to move the camera one step in that direction.

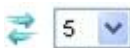
NOTE: If the camera is connected to a ViconNet or Salient NVR, a single click starts the camera movement and a second click is required to stop the camera movement. If the camera moves too quickly for accurate positioning, select a lower speed number from the camera speed drop-down. (See below.)



Click to zoom in.



Click to zoom out.



Select the camera movement speed. The slowest speed is 1; the fastest is 10.

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.

See also: [Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Creating Camera Preset Positions](#)

[Setting Up Camera Types](#)

[Setting the Camera Menu Order](#)

[Composing Widget Desktop Layouts](#)

[Setting Up Digital Video Recording](#)

[Monitoring NetVR Cameras](#)

Monitoring NetVR Cameras

Select **Monitor : Cameras**.

On this page you can select a NetVR camera for viewing.

To monitor a live camera view:

- Select any camera in the system from the **Cameras** menu.

NOTE: Live motion-detected video is indicated by a blue outline of the viewer window.



Click the Live Video icon to adjust the Quality and Rate of the viewer display. These settings can be reduced for monitoring use without affecting the recorded video.

- **Quality – Best** indicates the resolution provided by the camera for live or recorded video.
- **Rate – Max** indicates the frame rate as recorded.



Click the camera name in the title bar to select from various camera, camera tour, and camera presets options.

- Select a camera from the menus available under All Cameras or Favorites icon.
 - Select a Camera Group or a NetVR Appliance from the menu under the Categories icon.
 - Select a pre-defined group of cameras from the Tour menu.
 - Select an available preset for the selected camera from the Preset menu.
- NOTE:** The **Preset** option is only visible for PTZ cameras that support presets.
- Change the sort order between Manual (camera menu order), Alphabetical, or Reverse Alphabetical.

- Click the camera name in the title bar to close the menu window.



If PTZ controls are available for a specific camera, click the PTZ Controls icon to the right of the camera name in the title bar to display the controls on the viewer image:



pan and tilt arrow: direction and speed indicator



zoom in



zoom out

NOTE: The size of the arrow changes as it is dragged further from the center to indicate that the speed of the camera movement is increasing.



To view recorded video, click any video icon associated with an event in the Activity Log. Playback begins from the time of the event.

Playback controls are displayed in the viewer:



play



pause



playback head

2012-01-05 20:31:52.29

If the date and time display is configured when the individual camera is set up, a date and time stamp—for example, *yyyy-mm-dd hh:mm:ss.ss*—is shown on the top or bottom of the viewer as specified during the configuration.



Click the Go to Forensic Desktop icon to research video recorded by this camera.



Click the Go Live icon to return to viewing live video.

NOTE: If the camera does not have PTZ capabilities, no PTZ controls will be available for that camera.

See also: [Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Creating Camera Preset Positions](#)

[Setting Up Camera Types](#)

[Setting the Camera Menu Order](#)

[Composing Widget Desktop Layouts](#)

[Monitoring NetVR Multi-Camera Views](#)

[Setting Up Digital Video Recording](#)

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: You can also monitor a quad view on the **Camera Views** tab of the [Monitoring Desktop](#) or on the [Widget Desktop](#), in any widget that been set to the **Quad View** type.

To monitor NetVR multi-camera views, see [Monitoring NetVR Multi-Camera Views](#).

To move any camera in a multi-camera view:

1. Click anywhere in the title bar above the pane displaying the camera view you wish to adjust. The pane will highlight with an outline to show that it is selected.
2. Click this icon  to display the **Camera Preset** drop-down list. From the **Camera Preset** drop-down list, select the preset position you want to see displayed. (This drop-down list automatically fills with the presets of the selected camera.)



Click to display VCR controls at the bottom of the camera widget. You can use these VCR controls to review recorded video.

NOTE: The VCR icon will appear only if you are viewing a video management system (VMS) camera.



Click to display PTZ controls.



Click to move the camera to its preset home position.





Click an arrow to move the camera one step in that direction.




NOTE: If the camera is connected to a ViconNet or Salient NVR, 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. (See below.)

 Click to zoom in.

 Click to zoom out.

 Select the camera movement speed. The slowest speed is 1; the fastest is 10.

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.

TIP: If you are using Internet Explorer and a monitor that is too small to display all camera views, increasing the size of the widget and then using its scroll bars may cause the display to begin flashing. If this happens, press **F11** on the keyboard.

See also: [Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Composing Widget Desktop Layouts](#)

[Setting Up Camera Views](#)

[Creating Camera Preset Positions](#)

[Monitoring NetVR Multi-Camera Views](#)

Monitoring NetVR Multi-Camera Views

Select **Monitor : Camera Views**.

On this page you can select a **NetVR 2x2** view, which displays up to four camera views simultaneously, or a **NetVR 1+7** view which displays up to eight camera views simultaneously, one of these featured in a larger window or "Spot Monitor". The views for multiple cameras are defined in **Configuration : Video : Camera Views**.

See [Monitoring Multi-Camera Views](#) for information about using the **Quad view**, which displays up to four individual IP cameras simultaneously, or for information about controlling non-NetVR cameras in a mixed-type **Quad view**.

NOTE: You can also use the Camera Views tab of the Monitoring Desktop or the Camera View widget on the Widget Desktop to monitor a **Quad view**, **NetVR 2x2** view, or **NetVR 1+7** view.

To monitor a camera in a multi-camera view:

- Select any NetVR camera view in the system from the **Camera Views** menu.



Click the Live Video icon to adjust the Quality and Rate of the viewer display. These settings can be reduced for monitoring use without affecting the recorded video.

- **Quality – Best** indicates the resolution provided by the camera for live or recorded video.
- **Rate – Max** indicates the frame rate as recorded.



Click the camera name in the title bar to select from various camera, camera tour, and camera presets options.

- Select a camera from the menus available under All Cameras or Favorites icon.
- Select a Camera Group or a NetVR Appliance from the menu under the Categories icon.
- Select a pre-defined group of cameras from the Tour menu.
- Select an available preset for the selected camera from the Preset menu.

NOTE: The **Preset** option is only visible for PTZ cameras that support presets.

- Change the sort order between Manual (camera menu order), Alphabetical, or Reverse Alphabetical.
- Click the camera name in the title bar to close the menu window.



If PTZ controls are available for a specific camera, click the PTZ Controls icon to the right of the camera name in the title bar to display the controls on the viewer image:



pan and tilt arrow: direction and speed indicator



zoom in



zoom in

NOTE: If the camera does not have PTZ capabilities, no PTZ controls will be available for that camera.

If the date and time display is configured when the individual camera is set up, a date and time stamp—for example, *yyyy-mm-dd hh:mm:ss:ss*—is shown on the top or bottom of the

viewer as specified during the configuration.

2012-01-05 20:31:52.29

If the date and time display is configured when the individual camera is set up, a date and time stamp—for example, *yyyy-mm-dd hh:mm:ss:ss*—is shown on the top or bottom of the viewer as specified during the configuration.



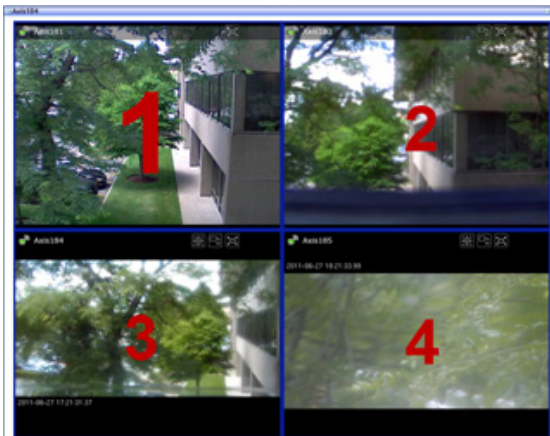
Click the Go to Forensic Desktop icon to research video recorded by this camera.



To enlarge a camera view, click the Enlarge View icon to the right of the camera name in the title bar, to switch the selected camera from a standard **NetVR 2x2** or **NetVR 1+7** layout view to an expanded window view. Click the Shrink View icon to return to the standard layout view.



To swap a camera into the #1 viewer position (upper left, as shown below) in a **NetVR 2x2** or **NetVR 1+7** multi-camera view, click the Spot Monitor icon to the right of the camera name in the title bar. If a small viewer does not display the Swap icon in the title bar, click the video image to swap it into the #1 position.



NOTE: Controls are displayed in the title bar of the viewer cells as space allows.

See also: [Monitoring Multi-Camera Views](#)

[Monitoring NetVR Cameras](#)

[Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Creating Camera Preset Positions](#)

[Setting Up Camera Types](#)

[Setting the Camera Menu Order](#)

[Composing Widget Desktop Layouts](#)

[Setting Up Multi-Camera Views](#)

[Setting Up Digital Video Recording](#)

Monitoring Floorplans

Select **Monitor : Floorplans**.

On this page you can:

- View any floorplan currently configured in the system.
- See the locations of system resources such as portals, cameras, inputs, outputs, and temperature sensors.
- Use a floorplan link to switch to a different floorplan.
- Momentarily unlock a portal.
- Schedule an extended lock or unlock of a portal.
- Display thumbnail images from cameras.
- View the current status of an alarm.
- Perform scheduled disarming of inputs.
- Perform scheduled activations and deactivations of outputs.
- Display temperature graphs for each temperature point.

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

NOTE: You can also use the Floorplans widget on the [Widget Desktop](#) to monitor floorplans.

To monitor a floorplan:

1. Select the floorplan you want to monitor from the **Floorplan** drop-down list.
2. Click the icon for any system resource on the floorplan to display its type and name in the **Type** and **Name** text boxes.
NOTE: 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 momentarily unlock the portal or schedule an extended 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 activated, the icon for that alarm turns red.

To schedule actions from a floorplan:

1. Select a floorplan from the **Floorplan** drop-down list.
2. Hold down the left mouse button on the icon for a portal, input, or output and select **Schedule Action** from the popup menu. A **Scheduled Action** dialog box appears.

NOTE: Selecting **Momentary 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, **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 hours and minutes you specify 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.
 - **After:** The action will end once the specified number of hours and minutes past the action's start time have elapsed.
7. Click **Save**.

Example: For an input, 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.

See also: [Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Composing Floorplans](#)

[Uploading Floorplan Background Images](#)

[Composing Widget Desktop Layouts](#)

Monitoring High Availability (HA) Status

Select **Monitor : HA Status**.

On this page you can:




- [View status information for an HA implementation.](#)
- [Configure HA if it does not appear to be configured.](#)
- [Investigate and fix problems that may occur.](#)

For information on the hardware installation process for an HA implementation, see [Exacta High Availability Server Installation \(PDF\)](#).

To view HA status information:

1. Select **Monitor : HA Status**.
- or -


Click the HA status icon in the application window header bar. The icon will change depending on the current status of the High Availability (HA) implementation:

-  **HA : Normal**
 -  **HA : Unconfigured**
 -  **HA : Degraded**
2. If the HA status is normal, the status settings should be as follows:
 - **Name:** Shows the names of the two HA servers: **node 0** and **node 1**.
 - **Primary:** Shows which server is currently the primary HA server. This setting will be **true** for the primary HA server and **false** for the secondary HA server.
 - **Standing State:** Shows the current state of the HA servers. This setting will be **normal** for both servers unless there is a problem.

To configure HA if it does not appear to be configured:



If this page displays a message indicating that High Availability does not appear to be configured, complete the following steps.



1. Select **Configuration : Site Settings : Network Controller**, then click the link in the **Initmode Settings** section to go to the Initmode page.
2. Enter the IP address of the HA server pair in the **Avance IP Address** field.
3. Click **Save**.
4. Click **Reboot** and click **OK** to confirm the reboot.

Once the system has rebooted, the HA status icon should change to  **HA : Normal** and you should see HA status information on this page.

NOTE: If you believe you have configured HA correctly, but it still does not appear to be configured, contact Technical Support for assistance.

To investigate and fix a problem:

If a problem with the HA implementation causes a failover, the HA status icon will change to  **HA Unconfigured** for a few seconds, then to  **HA Degraded**. The **Primary** setting for node 1 will change to **true**.

1. Click the **Avance Management Portal (login required)** link to go to Avance Management portal, where you can investigate and fix the problem.
2. Once the problem is fixed, the HA icon will change from  **HA Degraded** to  **HA : Normal** after a few seconds. The **Standing State** setting for both servers will return to **normal**.


Using the Monitoring Desktop

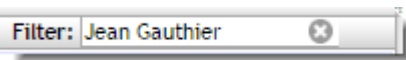
Select **Monitor : Monitoring Desktop**.

The Monitoring Desktop provides a fixed display for monitoring the system. It has tabs and widgets for monitoring various system functions, such as the Activity Log, events, portals, and camera views. These are described below.

Filtering the Data Shown on a Tab

For any tab or widget that has a **Filter** box in its upper right corner, you can enter text in the box to narrow down the data currently shown on that tab. Text filtering is not case sensitive; you can enter uppercase or lowercase characters.

Filtering begins as you start to type. For the remainder of the current monitoring session (or until you enter different text or click the Clear Filters icon ) , the page will show only data matching the text you entered. For example, to see only entries containing the name "Jean Gauthier" on the Activity Log tab, apply the filter shown below.



The Activity Log tab provides a second option for filtering its data. From the **Filter by category** drop-down list, you can select a category of event types, such as **Access Control** or **Devices**, to view only entries for events of that type. See [Filtering the Activity Log](#) for more information.

NOTE: You can use the tearoff line that appears in the upper right corner of the Monitoring Desktop to open it in a separate window, so you can continue to use it as you work with other pages in the application.

Events Tab






You can use the Events tab (or the Events widget on the [Widget Desktop](#)) to view information about all active events in the system. An active event is one that has at least one active alarm.

Counts showing the number of active events and the number of unacknowledged events are shown at the top of the tab. For each count, the number of active alarms associated with these events is shown in square brackets.

Below this, the list of active events is sorted in priority order by default. To reverse the sort order, click the Priority column header. You can also click the Date/Time column header to sort on that column.

An event will appear in the list until all of its active alarms have been resolved. For an alarm to be resolved, it must be acknowledged (if acknowledgement is required according to the associated [event definition](#)) and its underlying cause must be cleared.

To investigate and acknowledge an event, you can do any or all of the following:

- Click this icon  if it appears in the Name column 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 of the event's actions are resolved, or until the **Maximum Duration** specified in the [event definition](#) elapses and the event auto-acknowledges.
- Click Clear  to clear all active actions for the event. This will appear for an event only if both **Allow Clear Actions** and **While Active?** are selected in the [event definition](#).

Activity Log Tab

You can use the Activity Log tab to view recent entries in the log of system activity.

For more information see: [Monitoring the Activity Log](#).

Cameras Tab

You can use the Cameras tab to monitor any camera configured in the system.

For more information see: [Monitoring Cameras](#).

For more information on NetVR cameras see [Monitoring NetVR Cameras](#).

Camera Views Tab

You can use the Camera Views tab to monitor any configured four-camera Quad view, or NetVR 2x2 view or NetVR 1+7 view for NetVR systems.

For more information see: [Monitoring Multi-Camera Views](#).

For more information on NetVR cameras see [Monitoring NetVR Multi-Camera Views](#).

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 a camera monitor:

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



The icon changes to this button:



2. Click the button to bring the Camera Monitor tab forward and display the selected video stream or image.
3. Click controls on the Camera Monitor tab to perform the following actions:



Display VCR controls at the bottom of the camera widget. You can use these VCR controls to review recorded video.

NOTE: This control will appear only if you are viewing a video management system (VMS) camera.



Display PTZ controls.



Move the camera to its preset home position.



Move the camera one step in the directory of the arrow.



NOTE: If the camera is connected to a ViconNet or Salient NVR, 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. (See 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.

For information on performing actions and using controls for NetVR cameras, see [Monitoring NetVR Camera Views](#).

Floorplans Tab

You can use the Floorplans tab to monitor any floorplan configured in the system.

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

For more information, see [Monitoring Floorplans](#).

Threat Level Widget

You can use the Threat Levels widget to view and change the current threat level. For more information, see [Setting Threat Levels](#).

Portal Unlock Widget

You can use the Portal Unlock widget to momentarily lock or unlock a portal, switch a portal to a locked or unlocked state, disable or enable a portal, and schedule an extended lock or unlock of a portal. For more information, see [The Portal Status and Portal Unlock Widgets](#).

Photo ID History Widget

You can use the Photo ID History widget to view a recent history of cardholders who have presented their credentials to readers in the system. For more information, see [The Photo ID History Widget](#).

Cameras Widget

By default, the Cameras widget displays the first two cameras in the [Camera Menu order](#) configured for your system. You can select any camera defined in the system.

See also: [Using the Widget Desktop](#)

[Composing Widget Desktop Layouts](#)

[Monitoring the Activity Log](#)

[Filtering Activity Log Entries](#)

[Monitoring Cameras](#)

[Monitoring Multi-Camera Views](#)

[Setting Up Events](#)

[Setting Up Camera Views](#)

[Creating Camera Preset Positions](#)

[Monitoring Floorplans](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Granting Passback Grace

Select **Monitor : Passback Grace**.

On this page, system users with at least an Administrator 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 card holders, if both of following settings are selected (in the Web Site section of the Network Controller page): **Show Passback Grace as Menu Option** and **Show Region and Passback Grace info in the Roster and People reports**.

Granting passback grace to cardholders:

1. Select **Monitor : Passback Grace**.
2. 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.
3. Click **Search**.

A report containing the search results is displayed below the form. The report shows each person's name and current location.

4. To grace an individual cardholder, click the **Grace** button for that person. To grace all card holders listed in the report, click the **Grace all shown** button.

NOTE: A **Grace pending** button appears for any card holder 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.

See also: [Configuring Regional Anti-Passback](#)

[Creating Custom User Roles](#)

[Anti-Passback Applications \(PDF\)](#)

Unlocking Portals and Viewing Their Status

Select **Monitor : Portal Status**.

The Portal Status page lists all portals in the active partition that are associated with enabled nodes. You can use the page to:

- View a portal's current location, state (such as Ready, Disabled, or Forced), and unlock schedule. Note that you cannot view the current state of an [ASSA ABLOY online remote lockset](#).
- View the current threat level for any portal whose [location](#) has a different threat level than the active partition's default location.
- [Momentarily unlock a portal](#). You can also do this using the **Unlock Portal** command in the [command palette](#).
- [Switch a portal to a locked or unlocked state](#). This removes the portal from the automatic control of any [scheduled action](#), [double card read](#), or [portal group](#) time spec currently in effect for the portal. It also suspends any [event action](#) defined for the portal.


- [Disable or enable a portal](#). Disabling a portal locks it and temporarily removes it from the system's control.
- [Schedule an extended lock or unlock of a portal](#). You can also do this using the [Portal Status widget](#) or the [Schedule Action](#) page.

To filter the list of portals:


1. Enter text in the Filter box at the top of the page. Filtering begins as you start to type.



Text filtering is not case sensitive; you can enter uppercase or lowercase characters.



2. To further narrow down the list, enter additional text in the Filter box.
For the remainder of the monitoring session (or until you enter different text or click the Clear Filters icon ) the page will show only portals matching the text you entered.

To momentarily unlock a portal:

1. Locate the portal in the list.
2. Click **Momentarily Unlock Portal**  in the Action column.
The portal unlocks for its configured unlock duration.



NOTE: An online remote lockset will be taken out of panic mode if necessary, then returned to panic mode at the end of the unlock duration.

To disable or enable a portal:

1. Locate the portal in the list.
2. To disable the portal, click **Disable Portal**  in the Action column.
The portal is temporarily removed from the system's control.
3. To enable the portal, click **Enable Portal**  in the Action column.
The portal is returned to the system's control.

NOTE: It may take several minutes to enable an [ASSA ABLOY online remote lockset](#). This is because all of its credentials and time specs, which were removed when it was disabled, must be restored.

To schedule an extended unlock of a portal:



1. Locate the portal in the list.
2. Click **Edit Schedule**  in the Action column to display a list of scheduled actions for the selected portal.
3. To add a scheduled action, click add .
4. In the Scheduled Actions dialog box, select **Lock** or **Unlock** from the **Action** drop-down list.
5. For the **Uses Time** setting:

- Select **System Time** if you want the start and end times to be based on the time zone set for the controller
- Select **Local Site Time** if you want the start and end times to be based on the time zone set for the local node.

For example, suppose that the controller is in the Eastern time zone and the node is in the Central time zone (one hour earlier). To have the action start at 9 a.m. you can either enter the start time as 09:00:00 and select Local Site Time, or enter the start time as 10:00:00 and select System Time.

- 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.
- 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.
- In the **Comment** box, enter any comments you want to appear in the list of scheduled actions for the portal.
- Click **OK** to close the Scheduled Actions 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.

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

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.

See also: [Setting Up Portals](#)

[Setting Up Portal Groups](#)

[Scheduling Actions for Inputs, Outputs, and Portals](#)

[Enabling and Configuring Remote Locksets](#)

[Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[The Portal Unlock and Portal Status Widgets](#)

Switching a Portal to a Locked or Unlocked State

Select **Monitor : Portal Status**.

On this page you can:

- Use the **Lock Portal** button to put an unlocked portal into a locked state.

Clicking this button for a portal locks it and removes it from the control of any [scheduled Unlock action](#), [double card read](#), or portal group [time spec](#) currently in effect for the portal. It also suspends any [Unlock Portal event action](#) defined for the portal.

- Use the **Unlock Portal** button to put a locked portal into an unlocked state.

Clicking this button for a portal unlocks it and removes it from the control of any [scheduled Lock action](#), [double card read](#), or portal group [time spec](#) currently in effect for the portal. It also suspends any [Lock Portal event action](#) defined for the portal.

To switch a portal to a locked or unlocked state:

1. 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.

2. 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](#).

See also: [Setting Up Portals](#)

[Setting Up Portal Groups](#)

[Unlocking Portals and Viewing Their Status](#)

[Scheduling Actions for Portals, Inputs, and Outputs](#)

[Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[The Portal Unlock and Portal Status Widgets](#)

The Widget Desktop

Using the Widget Desktop

Select **Monitor : 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 your default layout. Each widget has a special function, such as displaying system activity, unlocking portals, or delivering real-time web content from another system.

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.

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: Changes you make to a layout while in monitoring mode are not saved across monitoring sessions. Once you close the Widget Desktop, the layout reverts to its original appearance. Additional layouts may be available from the Desktop menu in the lower left corner of the page. If you need a custom layout, and you do not have setup privileges in the active partition, see your security management system 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.

To display your default Widget Desktop layout:

- Select **Monitor : Widget Desktop**. Your default Widget Desktop layout appears automatically.

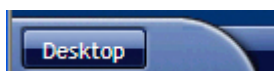
NOTE: Your default Widget Desktop layout is the layout that is currently selected on the Login tab of your person record.

To select a different Widget Desktop layout:

1. If the **Load Layout** option appears on the Desktop menu in the lower left corner of the page, select it to open the Load Layout dialog box.
2. 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:

1. Click **Desktop** in the lower left corner of the page to display the Desktop menu.



2. Select the widget you want to add

To select a different partition to monitor:

1. Click the name of the active 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 active partition until you select a different one, either from the Widget Desktop again or from the [Select Partition](#) page.

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 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:



2. Make any changes you want to the current layout, or any available layout, and then save the layout. See [Composing Widget Desktop Layouts](#) for instructions.
3. When you have finished, select **End Compose Mode** from the Desktop menu to return to monitoring mode.

To exit the Widget Desktop:

- Make a new menu selection to navigate to a different page.

See also: [Summary of the Available Widgets](#)

[About Widget Properties](#)

[Using the Monitoring Desktop](#)

[Filtering the Activity Log](#)

Summary of the Available Widgets

Select **Monitor : Widget Desktop**.

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 but is not displayed 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:

- **Activity Log:** See [Monitoring the Activity Log](#).
- **Alarm Workflow.** See [About the Alarm Workflow Widget](#).
- **Auto-Monitor:** See [The Auto-Monitor Widget](#).
- **Camera View:** See [The Camera View Widget](#).
- **Clock:** See [The Clock Widget](#).
- **DMP Intrusion Panels.** See [The DMP Intrusion Panel Widget](#).
- **Duty Log Entry:** See [Entering Duty Log Messages into the Activity Log](#).
- **Elevator Status:** See [Managing Floor Access Using the Elevator Status Widget](#).
- **Events:** See [Using the Monitoring Desktop to Monitor the System](#).
- **Explorer:** See [The Explorer Widget](#).
- **Floorplans:** See [Monitoring Floorplans](#).
- **Passback Grace:** See [The Passback Grace Widget](#).
- **Photo ID History:** See [The Photo ID History Widget](#).
- **Portal Status** and **Portal Unlock:** See [The Portal Status and Portal Unlock Widgets](#).
- **Statistics Block:** See [The Statistics Block Widget](#).
- **Status:** See [The Status Widget](#).
- **Threat Level:** See [The Threat Level Widget](#).

See also: [Using the Widget Desktop](#)

[About Widget Properties](#)

About Widget Properties

Select **Monitor : Widget Desktop**.

When you load a [Widget Desktop](#) layout, the initial attributes of its widgets, and the extent to which you can change these attributes for the current monitoring session, will depend on how the layout creator set the widget properties.

Widget properties fall into the following categories:

- **Common properties** are shared by all widgets. By configuring these properties for a widget, a layout creator determines whether the widget will appear on the Widget Desktop when the layout is loaded; the initial position, size, and state (either open or minimized) of the widget; and whether users will be able to move, size, minimize, and close the widget for individual monitoring sessions.

For information on changing a widget's common properties for a monitoring session, see [Moving, Sizing, Minimizing, and Closing Widgets](#).

- **Scope properties** are shared by most widgets. By configuring these properties for a widget, a layout creator determines the partitions from which the widget displays data, the types of data it displays, and whether users will be able to change its scope for individual monitoring sessions.

For information on changing a widget's scope for a monitoring session, see [Changing a Widget's Scope Properties](#).

- **Unique properties** are particular to a given widget. Like the other widget properties, a layout creator can specify whether users will be able to change these properties for individual monitoring sessions.

For information on changing a widget's unique properties for a monitoring session, see [Changing a Widget's Unique Properties](#).

See also: [Using the Monitoring Desktop](#)

[Summary of the Available Widgets](#)


[The Auto-Monitor Widget](#)

Moving, Sizing, Minimizing, and Closing Widgets

Depending on how a [Widget Desktop](#) layout was set up, you may be able to customize it by moving, sizing, minimizing, and closing its individual widgets. The extent to which you can modify a particular widget will depend on how the layout creator set its properties. For example, you might be able to move and size a particular widget, but not minimize or close it.



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.


To move, size, minimize, or close a widget:

1. For each widget you want to change, complete any of the steps that follow.
2. If the move icon  appears when you hover over the widget's title bar, drag the title bar to move the widget to a new location.
3. If sizing handles appear in each corner of the widget, drag any edge or corner of the widget to change its size.

NOTES: Some widgets have a minimum size below which they cannot be resized. Camera View widgets have a fixed 4 x 3 aspect ratio. If you make a Camera View widget wider, for example, it will make itself taller to maintain this aspect ratio.

Some widgets have a minimum size below which they cannot be resized. NetVR Camera View widgets have a fixed aspect ratio of either 4:3 or 16:9, depending on the aspect ratio specified in the camera widget properties. If you make any Camera View widget wider, for example, it will make itself taller to maintain its aspect ratio.

4. If the minimize button  appears in the upper right corner of the widget, click the button to minimize the widget to a button on the desktop tray.
5. If the close button  appears in the upper right corner of the widget, click the button to remove the widget from the layout.

NOTE: If the properties  button appears in the upper left corner of the widget, you can click it to change various properties of the widget for the current monitoring session.

6. Once you have finished using the selected layout, you can close it by displaying a different layout, exiting the **Widget Desktop** page, or logging off from the system. The modified layout reverts to its original appearance.

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.

See also: [Summary of the Available Widgets](#)

[About Widget Properties](#)


[Using the Widget Desktop](#)

[Using the Monitoring Desktop](#)

Changing a Widget's Unique Properties

Unique widget properties are particular to a given widget. Depending on how a [Widget Desktop](#) layout was set up, you might be able to change the unique properties of individual widgets for the current monitoring session.

To change a widget's unique properties:

1. Click this icon  in the upper left corner of any of the following widgets:
 - **Auto-Monito**r: See [The Auto-Monitor Widget](#).
 - **Alarm Workflow**: See [About the Alarm Workflow Widget](#).
 - **Camera View**: See [The Camera View Widget](#).
 - **Clock**: See [The Clock Widget](#).
 - **Explorer**: See [The Explorer Widget](#).
 - **Passback Grace**: See [The Passback Grace Widget](#).
 - **Photo ID History**: See [The Photo ID History Widget](#).
 - **Statistics Block**: See [The Statistics Block Widget](#).
 - **Status**: See [The Status Widget](#).
 - **Threat Level**: See [The Threat Level Widget](#).

NOTE: If the icon does not appear on a widget, you cannot change its properties.

2. After changing the properties you want, click **OK**.

See also: [Moving, Sizing, Minimizing, and Closing Widgets](#)

[Changing a Widget's Scope Properties](#)

[Summary of the Available Widgets](#)

[Using the Widget Desktop](#)


[Using the Monitoring Desktop](#)

Changing a Widget's Scope Properties

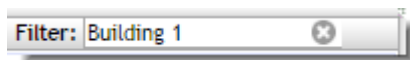
Depending on how the creator of a [Widget Desktop](#) layout configured a widget, you might be able to change the scope of the data it displays during the current monitoring session. For example, you might be able to change the widget's display to show:


- Data from all partitions to which you have access.
- Data from one or more of the partitions to which you have access.
- Specific types of data only.
- Data matching specific text only.

To change a widget's scope properties:

1. Click this icon  in the upper left corner of the widget to open its **Properties** dialog box.
NOTE: If the icon does not appear on a widget, you will not be able to change its properties.
2. If the **Show multiple partitions** check box appears at the top of the dialog box, select it to have the widget display data from all partitions to which you have access.
When you select the check box, a Partition filter appears below it.
3. To narrow down the data to specific partitions, use the Partition filter's right-arrow button to move those partitions from the Available list to the Selected list.
NOTE: If an administrator changes your permissions to give you access to additional partitions, you may need to log out and then log in again to view the new partition data.
4. For any other available filtering property you want to change, select a different filter from its drop-down list.
5. If a **Text filter** box appears in the dialog box, enter text in the box to further narrow down the data shown in the widget.
Text filtering is not case sensitive; you can enter uppercase or lowercase characters.
6. Click **OK**.
For the current monitoring session, the widget will display data only from the partitions you specified. The data from these partitions will be filtered to include only information matching the criteria and/or text you specified.

If you specified a text filter the text you entered will appear in the Filter box on the widget's title bar, as shown below.



You can apply another text filter by entering new text, and you can clear all text filters by clicking the Clear Filters icon .

See also: [Moving, Sizing, Minimizing, and Closing Widgets](#)

[Changing a Widget's Unique Properties](#)

[Summary of the Available Widgets](#)

[Using the Widget Desktop](#)

[Using the Monitoring Desktop](#)

Scope Properties You Might Be Able to Change

The following table shows the widgets that have [scope properties](#) you might be able to change for a monitoring session, depending on how the creator of the [Widget Desktop](#) layout configured them. For each widget that can display filtered data, the table lists the filters that might be available for narrowing down the data.

Widget	Multiple Partition Viewing	Filtering	Available Filters
Activity Log	X	X	Partition Log entry type Reader group Text
Alarm Workflow	X	X	Partition Priority filtering level Priority filtering method Text
Auto-Monitor			
Camera View	X	X	Partition View type Text
Clock			
DMP Intrusion Panel	X	X	Partition
Duty Log Entry			
Elevator Status	X	X	Partition Text
Events	X	X	Partition Priority filtering level Priority filtering method Text
Explorer			
Floorplans			
Passback Grace	X	X	Partition
Photo ID History	X	X	See note below

Portal Status/Portal Unlock	X	X	Partition Text
Statistics Block	X		Partition
Status	X		
Threat Level	X	X	Partition

NOTE: The scope of the data displayed in the Photo ID widget will always match that of the Activity Log widget to which it is anchored. For more information, see [The Photo ID History Widget](#).

See also: [About Widget Properties](#)

[Moving, Sizing, Minimizing, and Closing Widgets](#)

[Changing a Widget's Scope Properties](#)

[Changing a Widget's Unique Properties](#)

[Summary of the Available Widgets](#)

[Using the Widget Desktop](#)

More About Individual Widgets

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 active 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 up to 10 of the oldest alarms that are either unowned or are owned by another operator. The **My Alarms** view includes alarms that are owned by the operator who is currently logged in. The following information appears for each alarm:

- **Priority/Color:** The priority and color specified in the associated 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 became active.
- **Partition:** The partition in which the alarm became active. If this column does not appear, the widget was configured to show only alarms from the active partition.
- **Name:** The **Operator short msg**, if one was entered in the associated event definition.


- **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.
- **State:** The current state of the alarm: Active, Escalated, or Urgent. 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.
- **Owner** (Offered Alarms view only): The name of the alarm's current owner. If the alarm has no owner, <Unassigned> appears in this column.

The **Offered Alarms** and **My Alarms** views are separated by a splitter bar, shown below, which you can drag up and down to change the amount of vertical space each view occupies within the widget. By clicking the blue tab in the center of the splitter bar, you can collapse or expand the Offered Alarms view:



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 on a different column, click that column header.

Changing the Widget Properties

If the creator of the Widget Desktop layout has made the Alarm Workflow widget configurable, you can change its [common properties](#) and you can click this icon  in the widget's upper left corner to change 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 are updated in the **State** column.

See also: [Monitoring and Resolving Alarms](#)

[Configuring the Alarm Workflow Widget](#)

[Using the Widget Desktop](#)

[Setting Up Events](#)

[Creating Alarm Workflow Policies](#)

Monitoring and Resolving Alarms in the Alarm Workflow Widget

You can use the [Alarm Workflow widget](#) to monitor and resolve *alarms*—individual activations of events defined in the system. Multiple alarms can be active for an event at one time, and an event will remain active until all of its alarms have been resolved.

For an alarm to be resolved, it must be acknowledged (if acknowledgement is required according to the associated [event definition](#)) and its underlying cause must be cleared.

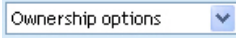
Controls in the Alarm Workflow widget let you:

- [Indicate your availability for handling alarms.](#)
- [Adopt alarms and optionally acknowledge them at the same time.](#)
- [Add duty log messages to alarms.](#)
- [Clear ongoing actions on alarms.](#)
- [Acknowledge alarms that you have adopted.](#)

To indicate your availability:

- 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 clear and select this check box as your availability changes.


To adopt, and optionally acknowledge, alarms:

1. In the **Offered Alarms** view, select the alarm(s) you want to adopt.
A blue border appears around each selected alarm. To deselect it, click it again.
2. Display the **Ownership options** drop-down list , or right click anywhere in the view.
3. Select one of the following:
 - **Adopt Alarm.** Moves the selected alarms to the **My Alarms** view and adds your name to the Owner column.
 - **Adopt and Acknowledge.** Adopts and acknowledges the selected alarms. Any alarm whose cause has been cleared is removed from the system. Any alarm whose cause has not been cleared is moved to the **My Alarms** view and displayed in italics.
 - **Adopt and Clear Actions.** Adopts the selected alarms and clears their ongoing actions.
4. If a duty log entry is required to acknowledge any of the alarms, enter a message in the dialog box that appears and click **Save**.
5. If prompted, click **Yes** to confirm that you want to perform all selected actions or click **No** to cancel all actions.

NOTE: A Clear Actions request will clear an alarm's ongoing actions only if **Allow Clear Actions** is selected in the associated event definition.

To add a duty log message to alarms:

1. In the **Offered Alarms** or **My Alarms** view, click the alarm(s) for which you want to add the duty log message.
A blue border appears around each selected alarm. To deselect an alarm, click it again.
2. Click the **Add Duty Log** button. You might need to scroll to the bottom of the view to see it.
Tip: In the **My Alarms** view, you can also right-click and select **Add Duty Log** from the menu that appears.
3. In the Duty Log Entry dialog box, enter your message and click **Save**.

A duty log entry is added to the Activity Log. Monitors will be able to click the clipboard icon () in the entry to view your message.

To clear ongoing actions on alarms you have adopted:

1. In the **My Alarms** view, click the alarm(s) for which you want to clear ongoing actions.
A blue border appears around each selected alarm. To deselect an alarm, click it again.
2. Click the **Clear Actions** button, or right-click anywhere in the view and select **Clear Actions** from the menu that appears.
3. If prompted, click **Yes** to confirm that you want to perform all selected actions, or click **No** to cancel all actions.

NOTE: A Clear Actions request will clear an alarm's ongoing actions only if **Allow Clear Actions** is selected in the associated event definition.

To acknowledge alarms you have adopted:

1. In the **My Alarms** view, click the alarm(s) you want to acknowledge.
A blue border appears around each selected alarm. To deselect an alarm, click it again.
2. Click the **Acknowledge** button, or right-click and select **Acknowledge** from the menu that appears.
3. If a duty log message is required to acknowledge any of the alarms, enter a message in the dialog box that appears and click **Save**.
Any alarm whose cause has been cleared is removed from the system. Any alarm whose cause has not been cleared is displayed in italics.

See also: [About the Alarm Workflow Widget](#)

[Using the Widget Desktop](#)

[Setting Up Events](#)

[Creating Alarm Workflow Policies](#)

The Auto-Monitor Widget

The Auto-Monitor widget provides a quick view of issues that might require attention, such as process failures or access control issues. It is available in selected versions of the security management system, both on the [Home page](#) and on the [Widget Desktop](#) when you are composing new layouts.






For each type of event that has occurred, the Auto-Monitor widget displays a notification indicating the number of such events that are currently active—or in the case of Recent Access Denied Activity notifications, the number that have occurred within a specific time period. Once an active event is resolved, the notification disappears.

You can point to a notification to display an informational tooltip. As shown in the example below, the tooltip shows details about each event, such as the date and time it occurred and the name of the affected device.

4 Device(s) have lost communication

```
0000002410300001 at 11/05/2010 15:20:33
0000002469012740 at 11/05/2010 15:20:33
260000000C054A27 at 11/05/2010 15:20:33
4A000000131EAF27 at 11/05/2010 15:20:33
```


The icon and font color displayed for a notification indicates the event type, as described in the following table.

Notification	Color	Meaning
 Unacknowledged Events	Red	One or more events requiring acknowledgement have not yet been acknowledged.
 Node Communication Loss	Red	One or more Network Nodes or MicroNodes have lost communication.
 Door Forced Open	Red	One or more portals are in the forced open state.
 Door Held Open	Yellow	One or more portals are in the held open state.
 Recent Access Denied Activity	Yellow	One or more of the Invalid Access types configured for the widget have occurred within the Invalid Access History time period configured for the widget. NOTE: Clicking a NOT IN NODE or BIT MISMATCH message opens the Card Decoder window.


Configuring the Auto-Monitor Widget

The Auto-Monitor widget has unique properties that you can configure for the current Widget Desktop layout and allow users to configure for individual monitoring sessions.

To configure the Auto-Monitor widget:

1. Click this icon  in the upper left corner of the widget.
2. In the **Tip placement** drop-down list, select the location where you want the informational window to appear when users point to notifications.
3. Select the check box for any of the event types that should be displayed in the widget.
4. If you select any of the **Invalid Access** types, select a time period on the **Invalid Access History** drop-down list.

Invalid accesses of the selected types will be displayed in the widget for the specified time period.

5. Click **OK**.
6. If you want Widget Desktop users to be able to configure these settings for individual monitoring sessions, click this icon  in the upper left corner of the widget, and make sure the **Configurable** check box is selected.


See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)


[Summary of the Available Widgets](#)

[About Widget Properties](#)


The Camera View Widget

When [composing a Widget Desktop layout](#), the layout creator can click this icon  in a specific Camera View widget to configure its properties and behaviors. The following options are available:

- **Allow multiple partition viewing** and **Allow filtering**: For information on setting these properties, see [Configuring a Widget's Scope Properties](#).
- **Allow camera to be manually changed**: Displays a drop-down that allows users to select a specific camera or camera view for the widget.
- **System sets widget title**: Allows the system to display the camera name in the title bar of the widget, rather than a name entered in the **Title** text box above. This ensures that if the camera changes, the widget title will reflect the change.
- **Is a camera monitor**: Sets the widget as a camera monitor, which can accept camera views and recorded video from other video widgets. A camera monitor 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.
- **Is the default camera monitor**: Sets the widget as the default camera monitor. Unless another monitor is specified for receiving a video stream, this widget will receive it.
- **Switch to linked camera on an event**: When events are configured, specific cameras can be linked to the event. With this setting, the widget will automatically switch to the event-linked camera when the event is activated.
- **Show person photo ID on access at location**: Sets the live Camera View widget to automatically display (fade in and out) the person's stored photo ID upon "valid access" Activity Log entry, within camera view linked to a reader portal. Both the Activity Log and Camera View widgets must be open on the Widget Desktop for the stored Photo ID to be displayed upon an associated "valid access" reader entry.
- **Photo ID display duration in seconds**: When Auto Display (fade in and out) is configured, this setting determines the duration of the photo ID display.
- **Play video event when activity log icon is clicked**: If an event is configured to record video, the Activity Log displays a camera icon. When this property is set, the widget will display the event-recorded video when the activity log camera icon is clicked.
- **Monitor to which to send video**: Specifies the camera monitor to which the widget will send video when you click the camera-to-monitor icon, if there are multiple camera monitors. If this property is not set, the default camera monitor will receive the images.

In addition, the layout creator can click this icon  in the upper left corner of a specific Camera View widget to set the following properties as its defaults in the current layout:

- **Show multiple partitions:** When selected, specifies that the widget will display data from all partitions to which a user has access. To narrow down the data to specific partitions, the layout creator can select from a list of available partitions.
- **View Type:** Specifies whether the camera will show a single-camera view or a four-camera (Quad) view.
- **Text Filter:** Specifies the text that will be used to filter the data displayed in the widget.
- **Selection:** Specifies a camera for the widget.
- **Show multiple partitions:** When selected, specifies that the widget will display data from all partitions to which a user has access. To narrow down the data to specific partitions, the layout creator can select from a list of available partitions.
- **Aspect Ratio:** The available NetVR options are **Standard-def 4:3** / **Wide Screen 16:9**
- **Variable View Type:** The available NetVR options are **Single Camera** / **Quad View** / **NetVR 2x2** / **NetVR 1+7**
- **Selection:** The available NetVR options appear in a list of defined views.

If the layout creator has made the Camera View widget configurable, monitors will be able to click the same icon  to change these default properties.

NOTE: Once a Camera View widget is set as a camera monitor, as the camera to which an event-linked camera switches, or as the camera that plays event-recorded video, only the **Single Camera** view type can be selected for the widget.

TIP: On a monitor that is too small to display all four cameras in a quad view, increasing the size of the widget and then using its scroll bars may cause the display to begin flashing. If this happens, press F11 on the keyboard.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)


[About Widget Properties](#)

[Configuring a Widget's Common Properties](#)

[Using the Forensic Desktop](#)

The Clock Widget

When the Clock widget is displayed on the Widget Desktop, it shows the current Network Controller time in digital or analog format. If an alarm is set for the clock, the widget plays the configured sound and displays any configured text message at the scheduled time.

If the creator of the Widget Desktop layout has allowed the Clock widget to be configured, monitors can click this icon  in the widget's upper left corner to change its unique properties:

- **Format:** Determines whether the clock has an analog or digital display.
- **Number Style (Analog):** For an analog display, determines the number style. The choices are arabic numerals, uppercase roman numerals, lowercase roman numerals, and tick marks.
- **Hour Color, Minute Color, and Second Color:** Determine the color used to display hours, minutes, and seconds, respectively. Clicking the box for any of these properties displays a color wheel for entering RGB values automatically.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The DMP Intrusion Panel Widget

When the Intrusion Panel widget is open on the Widget Desktop, it displays a tile for each DMP intrusion panel in the system. Monitors can use the widget to view configuration and status information for the panels. Administrators with setup privileges can use the widget to:

- [Arm or disarm an area associated with a panel.](#)
- [Bypass a faulted zone in an area associated with a panel.](#)
- [Activate or deactivate an output associated with a panel.](#)

NOTE: For information about integrating a Digital Monitoring Products (DMP) XR500 Series or XR550 Series control panel into a security management system (SMS), including important information about the ports that must be available for communications between the DMP panel and the SMS, see [Tech Note 18: DMP Intrusion Panel Integration](#).


To view available DMP intrusion panels:

1. If the Intrusion Panel widget is not open on the Widget Desktop, select it from the **Desktop** menu in the lower left corner of the page.

If the widget is not listed on the menu and you have setup privileges, switch to Compose mode and add the widget to your current layout. Otherwise, ask someone who has setup privileges to add the widget for you.

The tile for each panel indicates how many of the associated areas are fully armed, partially armed (containing faulted zones), and disarmed. If there is an error condition on a panel, one or more of the panel status icons will appear on the panel's tile:

Panel Status Icon Meaning

AC Power 	Panel power is low
Alarm	Panel is in alarm The panel tile will be red.



Battery Panel battery is low



Communications Panel has a communications problem



Tamper Panel tamper alert

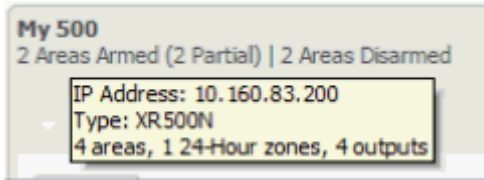


2. Click the tile for a panel to open the associated Panel Detail widget.

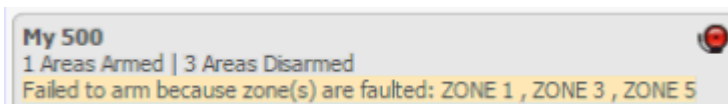
The Panel Detail widget displays detailed status information for the panel. It also includes options for controlling the panel by arming and disarming areas, bypassing and resetting zones, and activating and deactivating outputs. These procedures are described below.

To view the areas associated with a DMP intrusion panel:

1. In the Intrusion Panel widget, click the tile for a panel to open the associated Panel Detail widget.
The panel name and a summary of its fully armed, partially armed, and disarmed areas are displayed at the top of the widget.
2. Hover over the panel name to view the panel type and configuration:



Below the panel name, you might see a message reporting one or more execution errors. This message is in addition to information reported in the Activity Log. For example, if an area fails to arm, a message with a yellow background will appear:



The message will disappear once other activity occurs.

The areas associated with the panel are shown on a collapsible menu. The menu entry for each area shows the total number of faults for that area. If the area is in alarm, its name and fault count are shown in bold red: **AREA 1 [1 fault]**

Status icons displayed for each area indicate its current state:

Area Status Icon Meaning

Armed



Area is armed

Disarmed



Area is disarmed

In-Schedule



Area is armed due to a schedule

NOTE: If an area is partially armed, a text label indicates the number of areas armed over the total number of areas.

- The first entry on the collapsible menu is expanded to show a list of the zones in that area. To see the zones in a different area, click its entry.

Each zone's name indicates its current alarm status: If a zone is in alarm, its name is shown in bold red.

For zones that have errors, status icons indicate their current states:

Zone Status Icon Meaning

Battery



Zone battery is low

Missing



Zone is missing

Open or Short



Zone circuit is in the open or short state

Trouble



Undefined zone problem

To arm or disarm an area associated with a DMP intrusion panel:

- In the Panel Detail widget, click the menu entry for the area you want to change.
- Select one of the following options from the drop-down menu:
 - Normal:** (default) The area will fail to arm if any zones are faulted.
 - Bypass Faulted Zones:** Faulted zones will be bypassed automatically, allowing the area to be armed. Each of the bypassed zones will display the label *Bypassed*.

- **Force Arm:** Faulted zones will be switched to a "ready to be armed" state and each will be armed as soon as it is no longer faulted.
3. Click **Arm**.
Once the change takes effect on the panel, the area's Arm button changes to Disarm.
 4. To disarm an area, click its **Disarm** button.

To bypass a faulted zone in an unarmed area:

1. In the Panel Detail widget, click the menu entry for the unarmed area. You cannot bypass a faulted zone in an area that is armed.
2. Click the **Bypass** button for a faulted zone to switch it to the bypassed state. The Bypass button changes to Reset.

NOTE: You cannot bypass a 24-hour zone.

To activate or deactivate an output associated with a DMP intrusion panel:

1. In the Panel Detail widget, click the output you want to change.
2. Click the **Activate** or **Deactivate** button for the output.

Once the change takes effect on the panel, the button toggles to the opposite state, indicating that the output is now activated or deactivated. This may take a few minutes.

See also: [Configuring DMP Intrusion Panels](#)

[Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

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 of floor-select buttons in elevators you have permission to view.


For elevators on standard nodes, configured for *No Floor tracking* or *Floor tracking*, if your [user role](#) gives you Free Access privileges for the elevators in an elevator group, you can use the widget to manage access to those elevators. You can:

- [Enable momentary free access](#) for a floor-select button. This will give people temporary access to the floor without valid credential reads.



This functionality is also available for elevators on Mercury panels configured for *No floor tracking*.

- [Schedule an extended period of free access or controlled access](#) for a floor select button. This will give people either free access to the floor, or access via valid credential reads, for a specific period of time.

To enable momentary free 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 **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 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.
The Edit Schedule button will not appear in the Action column for an elevator associated with a Mercury panel.
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. For the **Uses Time** setting:
 - Select **System Time** if you want the start and end times to be based on the time zone set for the controller.
 - Select **Local Site Time** if you want the start and end times to be based on the time zone set for the local node.

For example, suppose that the controller is in the Eastern time zone and the node is in the Central time zone (one hour earlier). To have the action start at 9 a.m. you can either enter the start time as 09:00:00 and select Local Site Time, or enter the start time as 10:00:00 and select System Time.

6. 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.
7. 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.
8. In the **Comment** box, enter any comments you want to appear in the list of scheduled actions for the elevator output.
9. 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-select button will enter the free access state immediately and will remain in that state for one hour and thirty minutes.

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

See also: [Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[Composing Widget Desktop Layouts](#)

[About Widget Properties](#)


[Naming Floors to Be Managed By Elevator Access Control](#)

[Defining Elevators](#)

[Creating Elevator Floor Groups](#)

The Explorer Widget

When the Explorer widget is displayed on the Widget Desktop, it acts essentially as a browser window, delivering content from a web site in real time. For example, the widget can display content from a corporate web site or a local weather site.

If the creator of the Widget Desktop layout has allowed the Explorer widget to be configured, monitors can click this icon  in the widget's upper left corner to change its unique properties:

- **Type:** The type of web site displayed in the widget. The choices are: **Web**, **Secure Web**, **FTP site**, or **about** (to use an internal URI scheme, such as about:blank, rather than a URL).
- **URL:** The URL for the web site displayed in the widget.
- **Refresh Time:** The interval at which the widget will attempt to reload the web page. The choices are: **Never**, **1 minute**, **5 minutes**, **15 minutes**, or **1 hour**.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Passback Grace Widget

When the Passback Grace widget is displayed on the Widget Desktop, monitors can use it to grace card holders from passback and tailgate violations. Once an individual is "graced," his or her next card read will be allowed and no violations will be triggered. For subsequent card reads, all previous anti-passback rules will be in effect for the individual.

To allow monitors to find specific card holders to be graced, the widget includes fields for specifying search criteria, such as **First Name**, **Last Name**, and **Access Level**. When a monitor runs a search, the search results are listed at the bottom of the widget. The monitor can either click any of the **Grace** buttons within the list to grace individual card holders, or click the **Grace all shown** button to grace all card holders in the list.

The creator of a Widget Desktop layout can specify the following unique properties for the Passback Grace widget:

- **Number of search fields:** The specified number determines how many search fields are available on the widget for entering search criteria.
- **Allow user to select search fields:** When selected, monitors can change individual search fields by selecting different search criteria from their drop-downs. For example, a monitor who wants to search for card holders by access level rather than ID number can select **Access level** from the **ID#** field's drop-down.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)


[Summary of the Available Widgets](#)

[System Monitors and Passback Grace](#)

[About Widget Properties](#)

The Photo ID History Widget

When the Photo ID History widget is displayed on the Widget Desktop, it provides a recent history of cardholders who have presented their credentials to readers in the system. For each new access request, a box is added to the upper left corner of the widget. The box shows the cardholder's name and ID photo, the name of the reader, and the date and time the credentials were read. Depending on how the widget was configured for the selected layout, the box might also display information from one of the user-defined fields displayed in the cardholder's [person record](#).

Clicking the cardholder's name for a particular access request opens a Personal Information widget in which his or her person record is displayed. Clicking the icon to the right of the cardholder's name  opens a Duty Log Entry widget, which can be used to enter [duty log comment](#) into the Activity Log.


The boxes displayed in the Photo ID History widget are color coded:

- A blue box indicates that access was granted.
- A red box indicates that access was denied.
- A gray box indicates that access was denied and the cardholder is unknown.
- A box in the color selected for **Trace person log color** on the Network Controller page indicates that the cardholder's activity is currently being [traced](#).


Each instance of the Photo ID History widget is anchored to an Activity Log widget, which is the source of its access data. When the widget for the source Activity Log is added to the current layout, the information in the Photo ID History widget is updated automatically.

NOTE: Just as in the Activity Log, a monitor can click the [PASSBACK](#) or [TAILGATE](#) message displayed for a cardholder in the Photo ID History widget to grace that person from passback and tailgate violations.

About the Widget's Unique Properties

For any instance of the Photo ID History widget, the layout creator can click this icon  in its upper left corner and configure the following properties:

- **Cache size:** Specifies the number of cardholders to be displayed. The cache size can be set to any number from 100 to 2500. Whenever there are more cardholders displayed than can be shown in the widget, a scroll bar appears so a monitor can scroll through the list.
- **Note field:** Specifies a user-defined field whose value should appear for an access request, if that field is filled in on the cardholder's person record.
- **Show incomplete accesses:** Specifies whether incomplete access requests will appear in the widget.

In addition, the layout creator—or a monitor if the widget has been made configurable—can click this icon  and configure the following properties:

- **Source Activity Log:** Anchors this instance of the widget to a particular Activity Log widget, which will be the source of its access data.
- **Show only most recent access request:** Replaces the widget's current view showing a history of recent access requests with a new view showing only the most recent access request. In this view, the cardholder's ID photo is displayed in a larger size, to make identification easier.

See also: [Monitoring the Activity Log](#)

[Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Portal Status and Portal Unlock Widgets

When the Portal Status and Portal Unlock widgets are displayed on the Widget Desktop, you can use them to work with portals in the following ways:

- View a portal's current location, state, and unlock schedule. Note that you cannot view the current state of an [ASSA ABLOY online remote lockset](#).
- View the current threat level for any portal whose [location](#) has a different threat level than the partition's default location.
- [Momentarily unlock a portal](#). (You can also do this using [the Portal Status page](#) or the **Unlock Portal** command in the [command palette](#).)

- [Switch a portal to a locked or unlocked state](#). This removes the portal from the automatic control of any [scheduled action](#), [double card read](#), or [portal group](#) time spec currently in effect for the portal. It also suspends any [event action](#) defined for the portal.
- [Disable or enable a portal](#). Disabling a portal locks it and temporarily removes it from the system's control.
- [Schedule an extended lock or unlock of a portal](#). (You can also do this using the [Portal Status page](#) or the [Schedule Action page](#).)

If an ASSA ABLOY online remote lockset that has been put into a locked state by a scheduled action is unlocked by an event, it does not return to the locked state once the event ends.

NOTE: If [Allow filtering](#) is enabled for either widget and the widget is configurable, you can enter text in the **Filter** box to narrow down the list of portals, making it easier to find the one you want.

To momentarily unlock a portal:

1. Do either of the following:
 - In the Portal Status widget, locate the portal in the table.
 - In the Portal Unlock widget, select the portal from the drop-down list.


To make it easier to find a portal in the drop-down list, you can narrow down the list by changing the **All Portals** setting to **Favorites** or **Recent**.

2. Click **Momentarily Unlock Portal** .

The portal will unlock for its configured unlock duration.

NOTE: An online remote lockset will be taken out of panic mode if necessary, then returned to panic mode at the end of the unlock duration.

To switch a portal to a locked or unlocked state:

1. Do either of the following:
 - In the Portal Status widget, locate the portal in the table.
 - In the Portal Unlock widget, select the portal from the drop-down list.
2. To switch the portal to a locked state, click **Lock Portal** .


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. To switch the portal to an unlocked state, click **Unlock Portal** .


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.

To disable or enable a portal:



1. Do either of the following:
 - In the Portal Status widget, locate the portal in the table.
 - In the Portal Unlock widget, select the portal from the drop-down list.
2. To disable the portal, click **Disable Portal** .

The portal is temporarily removed from the system's control.

3. To enable the portal, click **Enable Portal** .
- The portal is returned to the system's control.

NOTE: It may take several minutes to enable an [online remote lockset](#). This is because all of its credentials and time specs, which were removed when it was disabled, must be restored.

To schedule an extended unlock of a portal:



1. Do either of the following:
 - In the Portal Status widget, locate the portal in the table.
 - In the Portal Unlock widget, select the portal from the drop-down list.
2. Click **Edit Schedule**  to display a list of scheduled actions for the selected portal.
3. To add a scheduled action, click add .
4. In the dialog box that appears, select **Lock** or **Unlock** from the **Action** drop-down list.
5. For the **Uses Time** setting:
 - Select **System Time** if you want the start and end times to be based on the time zone set for the controller.
 - Select **Local Site Time** if you want the start and end times to be based on the time zone set for the local node.

For example, suppose that the controller is in the Eastern time zone and the node is in the Central time zone (one hour earlier). To have the action start at 9 a.m. you can either enter the start time as 09:00:00 and select Local Site Time, or enter the start time as 10:00:00 and select System Time.

6. 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.
7. 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 Date/Time.

- **After:** The action will end once the number of specified hours and minutes past the action's start time have elapsed.
8. In the **Comment** box, enter any comments you want to appear in the list of scheduled actions for the portal.
 9. 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.



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

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 customize the Portal Unlock widget:


1. To limit the number of portals displayed on the portal selection drop-down list, do either of the following:
 - Select **Favorites** from the leftmost drop-down to display only the portals on the Favorites list
 - Select **Recent** from the leftmost drop-down to display only the portals you have selected most recently.

Your changes will remain in effect until you change the selection from the drop-down list, or close the widget or the selected layout.

2. To modify the Favorites list, select a portal and do either of the following:
 - Click this icon  to add the portal to the Favorites list.
 - Click this icon  to remove the portal from the Favorites list.

Your changes to the Favorites list are permanent.

To customize the Portal Status widget:

1. Click this icon  in the upper left corner of the widget.
2. Select the **Always Show Threat Level** check box.

For every portal shown, the widget will now display the current threat level at the portal's location.

See also: [Monitoring the Activity Log](#)

[Unlocking Portals and Viewing Their Status](#)

[Composing Widget Desktop Layouts](#)


[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Statistics Block Widget

When the Statistics Block widget is displayed on the Widget Desktop, monitors can use it to view various system information. For example, they can view statistics on unacknowledged alarms and devices in communication failure.

If the creator of the Widget Desktop layout has made the Statistics Block widget configurable, monitors can also click this icon  in the widget's upper left corner to specify which of the following are displayed in the widget:

- **Local Time:** The current Network Controller time.
- **System Uptime:** How long the system has been powered up.
- **User:** The current monitor's user name.
- **Logged In:** The time the current monitor logged in.
- **Unacknowledged Alarms:** How many of the active alarms are unacknowledged. For example, 1/5 means that one out of five alarms requires acknowledgement; the rest go away automatically when the underlying condition is fixed.
- **Devices in Communication Failure:** How many of the configured devices are currently in communication failure. For example, 2/9 means that two out of nine devices are in communication failure.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)


[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Status Widget

When the Status widget is displayed on the Widget Desktop, monitors can use it to view the status of all configured nodes and system resources. This information is presented in an expandable, hierarchical format.

Within the hierarchy, the icons displayed for a given resource and its node change depending on the current status of the resource. For example, when a blade needs attention, its icon and the icon for its node change from green balls to yellow triangles. If the blade fails, both icons change to red triangles.

If the creator of the Widget Desktop layout has made the Status widget configurable, monitors can click this icon  in the widget's upper left corner to specify the style it uses to display status information. The available **Style** settings are:

- **Node | Portal/Alarm Panel/Elevator | Resources:** With this setting, the widget display is based on each node's logical resources, such as its portals and their configured resources.
- **Node | Blade | Resources:** With this setting, the widget display is based on each node's physical resources, such its blades and their configured resources.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Threat Level Widget

The Threat Level widget is displayed on the Monitoring Desktop and in the default Widget Desktop layout. Monitors can use the widget to view the current threat level for the default location in the active partition. Administrators can also use the widget to change the threat level for any or all locations in the active partition.

In a Widget Desktop layout that includes the Threat Level widget, the information it displays depends on how it was configured for that layout. The widget might show the current threat level for:

- The default location in the active partition
- The default location and all of its sub-locations in the active partition
- The default location in selected partitions
- The default location and all of its sub-locations in selected partitions.

To use the Threat Level widget to change the current threat level:


1. Open the **Monitoring Desktop** or **Widget Desktop**.
2. In the **Threat Level** widget, click the button for the location whose threat level you want to change.
The Set Threat Level dialog box appears.
3. If a password is required to change the current threat level, enter it in the **Password** text box.
4. Select the threat level you want to apply.
5. Make sure the correct location is selected in the **Applies to location** drop-down list.
6. To apply the change to all sub-locations of the selected location, select the **Also apply to sublocations** check box.


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

7. Click **OK**.

In the Threat Level widget, the buttons for all affected locations change to reflect their new threat level.

To configure the Threat Level widget for a Widget Desktop layout:

1. Select **Configuration : Widget Desktops : Compose**.
2. In the **Load Layout** dialog box, select the layout you want to configure.
3. Click this icon  in the upper left corner of the **Threat Level** widget.
4. In the Properties dialog box, select the check box for any of the [common widget properties](#) you want the widget to have. If you want users to be able to configure the widget, be sure to select the **Configurable** check box.

5. To allow users to view threat level information for multiple partitions, select the **Allow multiple partition viewing** check box.
6. Click **OK**.
7. Click this icon  in the upper left corner of the widget.
8. If you want the widget to display threat level information for multiple partitions, select the **Show multiple partitions** check box.
9. In the Partition filter that appears below the check box, move the partitions you want the widget to display from the Available list to the Selected list.
10. To have the widget display all sub-locations of the selected partitions, select the **Show Locations** check box.
11. Click **OK**.

TIP: To see the way the widget will look when viewed in the current layout, click **Desktop** in the lower left corner of the Widget Desktop and click **Preview** to switch to Preview mode. To return to Compose mode, click **End Preview**.

See also: [Setting Threat Levels](#)

[Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

[Setting Up Partitions](#)

[Setting Up Locations](#)

Administering the System

This section provides information on the following topics.

Arm Alarm Panel	Arming and disarming alarm panels. This option will be available only if at least one alarm panel is defined in the system.
Data Operations	<p>Adding person records (including access level, credential, and user-defined person record information) to the system and modifying and deleting existing person records.</p> <p>Data Operations features are available only to users whose user roles include Data Operations permissions.</p>
Email Groups	Creating, editing, and deleting groups of people that can be used for email distribution.
Evacuations	Starting an evacuation plan to activate a regional evacuation and ending an active evacuation plan.
Forensic Desktop	<p>Searching recorded video to identify relevant clips and compose video cases.</p> <p>The Forensic Desktop will be available only if a NetVR appliance has been configured on the NetVR Appliances page.</p>
Lost Cards	Determining the owner of a lost card.
People Add	Adding people to the system.
People Search	Searching for people in the system. Viewing, changing, and deleting person records.
Reports	Creating reports on the current configuration of system resources, on system activity, and on people-related access information.
Schedule Action	Creating a scheduled action to lock or unlock a portal or portal group, arm or disarm an input or input group, activate or deactivate an output or output group, or enable free access or controlled access for an elevator floor or floor group.
Utility	Performing database backups, photo ID layout upload and delete.

See also: [Changing a Person's Access](#)

[Decoding Cards](#)

[Creating Evacuation Plans](#)

[Configuring Regional Anti-Passback](#)

[Data Operations Guide \(PDF\)](#)

[S2 Mobile Security Officer User Guide \(PDF\)](#)

Arming and Disarming Alarm Panels

Select **Administration : Arm Alarm Panel**.

With this page you can arm or disarm an alarm panel.

To arm or disarm an alarm panel:

1. The Administration Arm Alarm Panel page displays a table listing all alarm panels configured in the system, their current state, 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. When prompted, confirm the requested action.
4. If you are arming the panel the [Panel arming warning output](#) activates for the Warning duration.

See also: [Setting Up Alarm Panels](#)

[Setting Up Alarm Panel Arm/Disarm Behavior](#)

[Setting Up Alarm Panel Events](#)

[Setting Up Events](#)

Data Operations

Overview of Data Operations

The Data Operations feature allows you to add person records (including access level, credential, and user-defined person record information) to your system and modify and delete existing person records. With the Data Operations feature, you can:

- Manually upload (import) tab- or comma-separated (CSV) text files (Import files).
- Manually download (export) CSV text files (Export files).
- Automatically process Import files at scheduled intervals from a pre-configured NAS location.
- Monitor data import operations for errors using the operating log that is produced for each operation.

See: the [Data Operations Guide \(PDF\)](#) for detailed information on how to create a Data Operations Import file, a description of valid input data fields, formatting, syntax, error reporting, and example files.

NOTE: Data Operations features are available only on systems that have at least 2 GB of memory.

Initially Populating Your System with Person Records

When a new system is installed, it is necessary to create persons and card credential data for all persons who will require access. You could enter the data one person record at a time using the S2 interface.

An alternative method would be to produce a master Import file that contains all the person record data that will be required to populate your system using an external application such as Microsoft Excel or Access which are designed to expedite and facilitate the data creation and management process.

Once this file had been created, you can use Data Operations to Import the file and populate your system with person records for each employee.

Updating Your Person Records

Periodically, it will be necessary to update your person records with additional data as new hires come on board, employees leave, and modifications are required to existing records. If these updates are infrequent, they can be managed easily using the Data Operations feature.

For a variety of reasons, such as mergers and acquisitions or changes in security policies, you may be required to do bulk updates on a periodic basis. Data Operations provides an efficient method by which this can be performed as follows:

An external application or an individual creates an Import file which contains modifications that will update the person records on your system.

You use the Data Operations Import feature to Import the file manually via the S2 user interface to update person records.

Examples

Examples of how Data Operations might be used include:

- A user or external application creates an Import file from a database or work order external to an S2 system. The S2 administrator uses Data Operations to import the file and update person records.
- An Export file is generated with specific person record data for each employee. A user or external applications accesses the Export file and updates a database external to the S2 controller.
- An automatic import of a file created by an external application or user and placed in a pre-configured NAS location. Data Operations polls the NAS location at a user-defined interval and updates the person records of an S2 system.

For More Information

See the [Data Operations Guide \(PDF\)](#) for detailed information on how to create a Data Operations Import file, a description of valid input data fields, formatting, syntax, error reporting, and example files.

See [Performing Data Operations Tasks](#) for information on:

- Adding person records (including access level, credential, and user-defined person record information) to your system by importing a user-created data operations import file.
- Creating a Data Operations Export file that contains selected data from each person record in your system.

- Setting up a NAS storage location for processing import files at scheduled intervals.

See [Automatic Data Operations](#) for information on:

- Adding the periodic polling for import files from a NAS storage location.
- Modifying Data Operations parameters related to processing files in the NAS storage location.
- Deleting an automatic operation.

See [Data Operations Results](#) for information on viewing a data operations import source file and error information.

- Adding the periodic polling for import files from a NAS storage location, modifying Data Operations parameters related to processing files in the NAS storage location, and deleting an automatic operation.
- Viewing a data operations import file source file and error information.

Performing Data Operations Tasks

Select **Administration : Data Operations**.

Click the **Upload File**, **Export**, and **NAS Settings** buttons to perform Data Operations tasks.

To upload a Data Operations Import file:

1. Click **Upload File**.
2. Select an item from the drop-down list, enter a value, or select a checkbox:
 - **Name**: the user-defined name of the Import file.
 - **Description**: optional description of the Import file.
 - **Upload File**: the path name of the Import file or use the Browse button to locate the Import file.
 - **Pre-validation**: select the checkbox to enable the pre-validation feature which will stop the import operation when the Pre-validation Max Error number of allowed errors is detected.
 - **Pre-validation Max Errors**: the number of allowed errors encountered before the Import operation is stopped.
3. Click **OK** to upload the file.

To create an Export file:

1. Click **Export**.
2. Enter a **Name** for the Export file.
3. Enter a value for **Max Records**. Max records is the maximum number of person records that will be processed. Use this value to limit the number of records that are processed.
4. Select the **CSV** (comma-separated value) or **TSV** (tab-separated-value) output format to specify the format of the Export file.

5. Select the **Open in new window** check box if you want the Export file to opened in a new window.
6. Select the data headers that represent the person record data you want included in the Export file.
7. For each data header you want included in the Export file, select it in the Available list and click the right arrow (>) to move it to the Selected list. To deselect a header, select it and click the left arrow (<) to move it back to the Available list.
The system will generate an Export file with only the person record data you have selected. If the **Max Records** text field is left empty, the system will generate an Export file containing all the person records in your system.
8. Click **OK** to close the dialog box.

To set up NAS storage:

1. Click **NAS Settings**.
2. Enter the **Server IP Address** of the NAS storage server.
3. Enter the **Share Name**, the name of the network share on the computer on which the NAS storage is located.
4. Enter the **Username** and **Password** required to login to the NAS storage server.
5. Click **OK** to close the dialog box.

See also: [Overview of Data Operations](#)

[Automatic Data Operations](#)

[Data Operations Results](#)

[Data Operations Guide \(PDF\)](#)

Automatic Data Operations

Select **Administration : Data Operations**.

Select the **Add**, **Edit**, or **Delete** buttons to add an automatic operation for a NAS storage location, to edit parameters that are currently assigned to the automatic operation, and to delete an automatic operation.

The Automatic Operations window displays the following information for each configured automatic operation listed:

- **Name**: the user-defined name of the operation.
- **Description**: optional description.
- **Directory**: the path name for the Import files.
- **Interval**: the time interval for polling the NAS Storage for new Import files.
- **Pre-validation**: when true, the import operation is stopped when the **Pre-validation Max Error** number of allowed errors is detected.
- **Max Errors**: the number of allowed errors encountered before the Import operation is stopped.

- **Owner:** the owner of the file.
- **Last Run Time:** the last scheduled time that an Import operation was performed.
- **Next Run Time:** the next schedule time that an Import operation will be performed.
- **Status:** the status of the last operation.

To add an automatic operation for a NAS storage location:

1. Click **Add**.
2. Select an item from the drop-down list, enter a value, or select a checkbox for the **Name**, **Description**, **Directory**, **Interval**, **Pre-validation**, and **Pre-validation Max Errors**.
3. Click **OK** to close the dialog box.

To edit an Import file:

1. Select the automatic operation you want to edit from the list in the Automatic Operations window.
2. Click **Edit**.
3. Select an item from the drop-down list, enter a value, or select a check box:
 - **Name:** the user-defined name of the operation.
 - **Description:** optional description.
 - **Directory:** the path name for the Import file.
 - **Interval:** the time interval for polling the NAS Storage for new Import files.
 - **Pre-validation:** select the checkbox to enable the pre-validation feature which will stop the import operation when the Pre-validation Max Error number of allowed errors is detected.
 - **Pre-validation Max Errors:** the number of allowed errors encountered before the Import operation is stopped.
3. Click **OK** to close the dialog box.

To delete an Import file:

1. Select an automatic operation you want to delete from the list in the Automatic Operations window.
2. Click **Delete**.
3. Click **OK** to delete the file, or **Cancel**.

See also: [Overview of Data Operations](#)

[Performing Data Operations Tasks](#)

[Data Operations Results](#)

[Data Operations Guide \(PDF\)](#)

Data Operations Results

Select **Administration : Data Operations**.

Select the **View Source**, **View Errors**, and **Delete** buttons to view the Import file source text, to view errors and status information generated by uploading an Import file, and to delete the result from the Data Operations Results window, respectively.

The Results window displays the following information for each Import file listed:

- **Name:** the user-defined name of the import operation.
- **Description:** optional description.
- **Directory:** the path name of the Import file or use the Browse button to locate the Import file.
- **Start/End Time:** the start and end time of the data operation.
- **Elapsed Time:** the elapsed time of the data operation.
- **Status:** the status of data operations processing of the Import file.
- **Errors/Lines:** the number of errors generated during Import file processing and the total number or lines that were processed.
- **Failure Info:** information that explains why the Import processing failed.
- **Source:** the name of the source Import file.
- **Method:** the method by which the file was accessed (for example, via Upload).
- **Delete:** use to delete multiple results.
- **Status:** the status of the operation.

To view the Import file source text:

1. Select the result from the list in Data Operations Results window.
2. Click **View Source**.
The View Source window opens and displays the contents of the Import source file.
3. Click **OK** to close the View Source window.
4. Click **Download** to download a copy of the Import source file.

To view errors generated by Import file processing:

1. Select the result from the list in Data Operations Results window.
2. Click **View Errors**.
The View Errors window opens and displays the **Line #** in the Import file where the error occurred, the **Line Text**, and the **Error** generated from processing of the Import file.
3. Click **OK** to close the View Errors window.
4. Click **Download** to download a copy of the error file.

NOTE: If you attempt to import person record data into a system in which an access level name is duplicated across partitions, person records that include an access level with that name will not be imported. In the Results window, you will see the error message: *Cannot resolve access level: '<accesslevelname>'* for each of those person records. To import the data, you can either specify the access level name as "partitionname:accesslevelname" in the import file or give the access level a unique name in each partition.

To delete a result from the Data Operations Results window:

1. Select the Import file you want to edit from the list of files in Data Operations Results window.

2. Click **Delete**.
3. Click **OK** to delete the Import file from the Data Operations Results window, or **Cancel**.

See also: [Overview of Data Operations](#)

[Performing Data Operations Tasks](#)

[Automatic Data Operations](#)

[Data Operations Guide \(PDF\)](#)

Managing Evacuations

Select **Administration : Evacuations** to display the following options.

Choose this	To see information on
Start Evacuation Plan	Activating a regional evacuation by starting an evacuation plan.
End Evacuation Plan	Ending an active evacuation plan.

See also: [Creating Evacuation Plans](#)

[Configuring Regional Anti-Passback](#)

[S2 Mobile Security Officer User Guide \(PDF\)](#)

In the event of an emergency or disaster, you can start an evacuation plan to initiate an evacuation.

NOTE: You can also use the Mobile Security Officer™ (MSO) App running on an iPad to start an evaluation plan. For more information, see the [S2 Mobile Security Officer™ User Guide \(PDF\)](#).

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:
 - Run the [Roll Call](#) or [Occupancy](#) report and periodically refresh the report results.
 - In the MSO, click **Mustering** to get a dynamic view of the evacuation's progress.

See also: [Ending Evacuation Plans](#)

[Creating Evacuation Plans](#)

[S2 Mobile Security Officer™ User Guide \(PDF\)](#)

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 evaluation plan. For more information, see the [S2 Mobile Security Officer™ User Guide \(PDF\)](#).

To end an evacuation plan:

1. Select the name of the plan you want to end.
2. Click **End Evacuation Plan**.
3. 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.

See also: [Starting Evacuation Plans](#)

[Creating Evacuation Plans](#)

[S2 Mobile Security Officer™ User Guide \(PDF\)](#)

Using the Forensic Desktop

To open the Forensic Desktop from the Home page, click the **Forensic Desktop** icon in the **User Tasks** widget:



- or -

Select **Administration : Forensic Desktop**.

The Forensic Desktop provides tools you can use to select and research recorded video, identify relevant clips and compose a case folder for an event, print images, and save and/or export the case.

NOTE: The Forensic Desktop will not be available on your system until the NetVR appliance has been configured on the [NetVR Appliances](#) page.

NOTE: If your system has multiple partitions, the partition in which the NetVR appliance is configured must be selected in order for you to use the NetVR surveillance and forensic functions.

The Forensic Desktop can also be accessed directly from any NetVR camera view by clicking the Forensic Desktop icon in the camera's title bar:



NOTE: The **Video Accelerator** is a lightweight service application that is required for NetVR web-based video. If the Video Accelerator has not been installed in advance, you will be prompted to install it to view any NetVR video.

Starting a Forensic Search

By default, the Forensic Desktop displays thumbnails of the cameras available for selection to build a case. You can also click the **Camera List** tab to display the thumbnails.

NOTE: The default camera thumbnails are static images generated from the first frame of the appliance's first appearance, and are stored on the web server. These saved thumbnails have no timestamp. You can right-click a camera thumbnail to replace the static image with either the player image or a live image as the new key frame.



Refresh (on the **Camera List** tab) scans the camera list for a specified date and time and updates available thumbnails.





Clear Camera Live Thumbnails restores the original static thumbnails.



All Cameras is the default list. Click **Favorites** or **NetVR Appliances** or **Camera Groups** to access custom camera lists.



Favorites are defined by selecting a camera and clicking on the Add Favorite button . If the selected camera is already a Favorite, the Delete Favorite button  is available.




NetVR Appliances displays the resources in the current system or active partition.



Camera Groups are defined in **Configuration : Video : Camera Groups**.

Use the camera thumbnails and the **Search Clock**  to select a starting point for your search.

- Or begin a search by using an event or play video icon  in the **Activity Log** to select the starting point.
- Or begin a search from an event listed in the Recent Activity tab of a person record.

See [Accessing Recorded Video from a Person Record](#) for more details about the Recent Activity tab.

Use the **Video Clip Player** to create clips to place in the **ScratchPad**.


- Trim the clip to mark start-frame  and end-frame  points.

- Open and use the digital zoom controls on the player menu to analyze the video clip.

Use the **Timeline** tab to further research the event and locate more clips for the case.


- The **Timeline** presents a search of recorded video based on the date/time or event selected.
- The stride drop-down menu allows you to specify the stride (or interval) of the clips. The default is 10 minutes.

The stride specifies the minimum interval to be skipped before the next clip (in frames, seconds, minutes, hours, or days). After each clip found, the system "skips" the stride length selected, then searches to start the next clip.

- The thumbnail size buttons allow you to select the size of the video clips thumbnails displayed.
- Selecting  (on the **Timeline** tab) refreshes the video search based on changes in the criteria chosen.

For detailed steps using the Forensic Desktop features, see [Beginning a Forensic Search](#).

Working with Forensic Cases

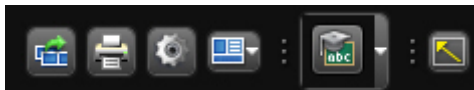
Click the **Case Inspector** tab. Or use the Pane Management drop-down menu  to open the **Saved Clips** or **ScratchPad** window.







After researching video associated with an event or time, a case can be saved and/or exported. All previously saved cases are cataloged in the case library in alphabetical order by case name. Each case is represented by a thumbnail with a user-defined keyframe screen display on the thumbnail, along with a case name, information on number of saved clips and comments, and the last modification data.


For more details about creating video cases, see [Composing Forensic Cases](#).




Using the Forensic Desktop Tools

You can use tools in the upper right corner of the Forensic Desktop to export case clips, print images from case clips, change user options, manage panes, and switch between a full screen view and the browser view.



- Click  to export one or more of the clips in the Case Inspector tab for further research and archiving.
- Click  to print an image from a case clip. For more information, see [Printing and Exporting Forensic Cases](#).
- Click  and select an option from the menu that appears to hide or show the Activity Log, Saved Clips, or ScratchPad pane.
- Click  to select a video tutorial, which will begin playing in a separate window automatically.
- Click  to open a full screen view of the Forensic Desktop. From the full screen view, click  to return to the browser view.

You can also click the Settings button  to display a **Track Settings** dialog box for configuring the following options:

- **Auto synchronize Timeline to search criteria** - enabled by default. Whenever the **Timeline** thumbnails become out of sync with the **Search Clock**, the system automatically makes the **Timeline** tab active and refreshes the thumbnails.
If you disable this option, the thumbnails will not be refreshed unless the **Timeline** tab is active. The Refresh button  will appear on the **Timeline** tab to indicate the thumbnails are out of sync with the **Search Clock**. You can manually synchronize the thumbnails to the **Search Clock** by clicking  on the tab.
- **Auto refresh Camera List thumbnails** - disabled by default. This option is used for multi-camera searches. When it is disabled, the Refresh button  will always appear on the **Camera List** tab so you can manually refresh its thumbnails when a search is performed.
If you enable this option, the system will automatically refresh the thumbnails in the **Camera List** when a search is performed. The resulting list will include only cameras that have recorded video within a specific number of hours, minutes, or seconds of the current search time (as indicated by the **Search Clock**). This option is particularly useful when tracking people in a multi-camera search scenario.
- **Search Limit** - default is 1 Hour. With the default setting, whenever the system refreshes the Camera List, the list will include only cameras that have recorded video within 1 hour of the current Search Clock date/time. You can increase or decrease the **Search Limit** to a selected number of hours, minutes, or seconds.

See also: [Beginning a Forensic Search](#)

[Using the Forensic Desktop Activity Log](#)

[Using the Forensic Desktop Video Player](#)

[Creating and Saving Clips](#)

[Using the Forensic Desktop Timeline](#)

[Composing Forensic Cases](#)

[Printing and Exporting Forensic Cases](#)

[Accessing Recorded Video from a Person Record](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Searching Recorded Video

Beginning a Forensic Search

To open the Forensic Desktop from the Home page, click the **Forensic Desktop** icon in the **User Tasks** widget:




- or -

Select **Monitor : Forensic Desktop**.


Using the Forensic Desktop, you can search through recorded video to locate and save images of a specified time, event, location, or activity.

- The **Search Clock** allows you to set a date and time to start the search.
- The **Camera List** tab allows you to select a camera for starting the search.
- The Forensic Desktop **Activity Log** allows you to select an event, a camera, a portal, or a person associated with an event for video research.
- The **Timeline** tab initiates a search of the selected recorded video.

To use the Search Clock to begin searching recorded video:

1. Click the **Search Clock**  to select a date and time for the start of your search.
2. Select a specific date by clicking it in the calendar or selecting it from the **Date** selector; or select a relative date from the **Go To** menu.
3. Select or refine the time by dragging the time slider or selecting a time from the **Time** selector. The **Activity Log** then adjusts to display the start date and time that is selected using the **Search Clock**.
4. Select a camera thumbnail from the **Camera List** tab to search for specific recorded events.

To use the Forensic Desktop Activity Log to begin searching recorded video:


1. Click a date and time in the **Activity Log** to select a starting point. The camera thumbnail associated with the selected **Activity Log** entry is highlighted.
2. Click the camera thumbnail to view the video in the player, if necessary.
3. Click the playback button  in the **Activity Log** to start searching by playing the camera and motion event selected.

To use the Recent Activity tab in a person record to begin searching recorded video:

1. Click the date and time for an event to review recorded video related to that event in the Video Player provided.
2. Click the event description, the person's name, or the portal or reader location to move to the Forensic Desktop for further investigation.

You can use this feature to match a person's ID photo to the individual who accessed a reader or portal. For more information, see [Accessing Recorded Video from a Person Record](#).

To use the Forensic Desktop icon to begin searching recorded video:

- Click the Forensic Desktop icon  in the camera's title bar directly from any NetVR camera view.

If there is no video associated with the time/date or event selected, the player will display a "no video" icon.

See [Using the Forensic Desktop Activity Log](#) for more details about starting a search from the **Activity Log**.

To continue searching recorded video:

- Use the video player to view and trim video clips. See [Using the Forensic Desktop Video Player](#) for details.
- Use the **ScratchPad** to create a storyboard of selected clips. See [Creating and Saving Clips](#) for details.
- Use the **Timeline** tab to refine the search and follow the events you are researching over time, to see what happened next, and using other camera views. See [Using the Forensic Desktop Timeline](#) for details.

See also: [Using the Forensic Desktop](#)

[Using the Forensic Desktop Activity Log](#)

[Using the Forensic Desktop Video Player](#)

[Creating and Saving Clips](#)

[Using the Forensic Desktop Timeline](#)

[Composing a Forensic Case](#)

[Printing and Exporting Forensic Cases](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Using the Forensic Desktop Activity Log

To open the Forensic Desktop from the Home page, click the **Forensic Desktop** icon in the **User Tasks** widget:



- or -

Select **Administration : Forensic Desktop**.

You can use the Forensic Desktop Activity Log to find and retrieve recorded surveillance video associated with specific system activity—such as access events triggered by a particular person or occurring at a particular portal.

By default, the Activity Log shows all recent activity relative to the date and time the Forensic Desktop was last started. This includes events of all types and associated with any person or portal. The most recent events are visible on the screen, and you can scroll up to see earlier activity.

Refining the Information Shown in the Activity Log


As you conduct video research, you can refine the information shown in the Activity Log to focus on specific activity. For example, you can set a new starting point for your search by [selecting a new date and time for the Search Clock](#). The Activity Log will now show all recent activity relative to the new date and time.

You can also use one or more of the following methods to narrow down the list of events currently shown in the Activity Log:

- [Apply a text filter](#) to focus on events matching specific text.
- [Apply an event filter](#) to focus on specific types of events.
- [Click the description for a video event](#) to focus on that event and similar, subsequent video events.
- [Click the date and time for an access event](#) to select it as the starting point for viewing video of all activity at the same location.
- [Click the person name for an access event](#) to focus on that and subsequent events triggered by the same person.
- [Click the portal name for an access event](#) to focus on that and subsequent events at the same portal.

NOTE: Once you have found the video you want, you can use the Forensic Desktop **ScratchPad** to [create and save clips](#), for use in [composing forensic cases](#).

To select a new date and time for the Search Clock:



1. Click **Go to date**  in the upper left corner of the Forensic Desktop.
2. To select a specific date for the Search Clock, click the date in the calendar or select it from the **Date** selector. Alternatively, select a relative time (such as Now, Yesterday, or Last Month) from the **Go To** menu.
3. Select or refine the time of day by dragging the time slider or selecting it from the **Time** selector.
4. Click **OK**.

The Activity Log display changes to show recent activity relative to the new date and time displayed in the Search Clock. Events closest to that date and time are visible on the screen, and you can scroll down to see subsequent activity.

To focus on events matching specific text:

1. Begin entering text into the **Filter** box.
Text filters are not case sensitive; you can enter any combination of uppercase and lowercase letters.



As you type, the list of events changes dynamically to include only those whose descriptions contain the text you have entered so far. When you finish entering text, only events matching the entire text string are shown.

2. Click **Apply filter on server**  to search the controller's Activity Log and return additional matching events occurring after the initial event shown in the filtered list.
3. Click **Clear filter**  to clear the text filter and restore the unfiltered list of events.

To focus on specific types of events:

1. Select one of the following from the **Events** drop-down list:
 - **<All Events>** (the default) to view activity of all types.
 - **Access Granted/Denied** to view only Access Granted and Access Denied events.
 - **Access Denied** to view only Access Denied events.
 - **Access Granted** to view only Access Granted events.

The Activity Log display changes to show only events of the type(s) you selected. Hovering over these events highlights the corresponding thumbnails in the **Timeline**.



2. Click **Apply filter on server**  to search the controller's Activity Log and return additional matching events occurring after the initial event shown in the filtered list.
3. Click **Clear filter**  to clear the event filter and restore the unfiltered list of events.


To focus on a video event and all similar, subsequent video events:

1. Click the **Video Event: video recording created** link in the video event of interest.

Video events are displayed in green and include a playback button .

The Activity Log display changes to show only this video event and all similar, subsequent video events. Hovering over these events highlights the corresponding thumbnails in the **Timeline**.

2. Click **Apply filter on server**  to search the controller's Activity Log and return additional matching events occurring after the initial event shown in the filtered list.
3. Click **Clear filter**  to clear the event filter and restore the unfiltered list of events.

NOTE: Clicking the playback button  for a video event begins playing the recorded video in the Video Player and resets the Search Clock to that event's date and time.

During or after the playback, you can click the date and time shown at the bottom of the Video Player. This has the same effect as selecting a new date and time for the Search Clock. The Activity Log will now show all recent activity relative to the new date and time.

To select an access event as the starting point for viewing video of all activity at the same location:


- Click the date and time in the access event of interest.



The **Search Clock** changes to that date and time. If there is video associated with the event, the recording is displayed in the **Video Player** and the camera associated with the event is highlighted in the **Camera List**. The **Timeline** displays thumbnails for subsequent events at the same location. Hovering over these events in the Activity Log highlights the corresponding thumbnails.

To focus on an access event and subsequent events triggered by the same person:

1. Click the person's name in the access event of interest.
2. Select one of the following from the drop-down list that appears:
 - **This and all subsequent activity by <personname>** to view this and all subsequent events triggered by this person at any portal.
 - **This and subsequent activity by <personname> at <portalname>** to view this and subsequent events triggered by this person at the same portal.

The Activity Log display changes to show only this event and subsequent events matching your selection. Hovering over these events highlights the corresponding thumbnails in the **Timeline**.



NOTE: Clicking  in the upper left corner of the player window displays the person's photo ID.

3. Click **Apply filter on server**  to search the controller's Activity Log and return additional matching events occurring after the initial event shown in the filtered list.
4. Click **Clear filter**  to clear the text filter and restore the unfiltered list of events.

To focus on an access event and subsequent events at the same portal:

1. Click the portal name in the access event of interest.
2. Select one of the following from the drop-down list that appears:
 - **This and all subsequent activity at <portalname>** - to view this and all subsequent activity at this portal.
 - **This and subsequent activity by <personname> at <portalname>** - to view this and subsequent activity by the same person at this portal.
 - **This and subsequent activity of this type at <portalname>** - to view this and subsequent activity of the same type at this portal.

The Activity Log display changes to show only this event and subsequent events matching your selection. Hovering over these events highlights the corresponding thumbnails in the **Timeline**.

3. Click **Apply filter on server**  to search the controller's Activity Log and return additional matching events occurring after the initial event shown in the filtered list.
4. Click **Clear filter**  to clear the text filter and restore the unfiltered list of events.

See also: [Using the Forensic Desktop](#)

[Beginning a Forensic Search](#)

[Using the Forensic Desktop Video Player](#)

[Creating and Saving Clips](#)

[Using the Forensic Desktop Timeline](#)

[Composing a Forensic Case](#)

[Printing and Exporting Forensic Cases](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Accessing Recorded Video from a Person Record

Select **Administration : People Search**, enter a name, and click **Search** to display that individual's person record.

If you have a NetVR system, the **Recent Activity** tab in a person record lets you quickly:

- View recorded video related to recent activity.
- Move to the Forensic Desktop to build a case related to a recent event.
- Match a person's ID photo to an individual who accessed a reader or portal.

The tab shows recent system activity generated by the person whose record you are viewing. The entry for each Access granted or Access denied event shows the date and time the event was communicated to the controller, a description of the event, the person's name, and the portal or reader location where the event occurred.

The screenshot shows the 'Recent Activity' tab selected. The 'Activity log' window contains the following data:

Date	Time	Description
07/13/2012	18:22:25	Access granted for Night Cleaners 3 at Suite Entrance
07/06/2012	09:14:07	Access granted for Night Cleaners 3 at Stair 1 3rd Floor Emp. Entry
06/27/2012	18:44:46	Access granted for Night Cleaners 3 at Suite Entrance
06/20/2012	13:57:02	Access granted for Night Cleaners 3 at Stair 1 3rd Floor Emp. Entry
06/13/2012	19:00:03	Access granted for Night Cleaners 3 at Suite Entrance
06/12/2012	13:23:38	Access granted for Night Cleaners 3 at Stair 1 3rd Floor Emp. Entry
06/05/2012	18:26:49	Access granted for Night Cleaners 3 at Suite Entrance
06/02/2012	05:03:30	Access denied [TIME] by Night Cleaners 3 at Suite Entrance
05/31/2012	19:28:34	Access granted for Night Cleaners 3 at Suite Entrance
05/31/2012	08:14:26	Access granted for Night Cleaners 3 at Suite Entrance
05/30/2012	19:31:54	Access granted for Night Cleaners 3 at Suite Entrance

The 'Lobby' window shows a video player with a play button and a timeline. The video title is 'Lobby' and the timestamp is '11/2012 19:21'.

To view recorded video for an Access granted or Access denied event:

1. To filter the list of events, enter text in the **Filter** box and/or use the **All Events** drop-down menu to display only **Access Granted** and **Access Denied** events, only **Access Denied** events, or only **Access Granted** events.
2. Locate the event you want to use as the starting point for your search.

3. Click the event date and time to view recorded video for this activity and all subsequent activity at this location in the provided [Forensic Video Player](#).
4. Perform any or all of the following steps to move to the Forensic Desktop and search through recorded video. For more information, see [Using the Forensic Desktop](#).
5. Click the event description ("Access granted" or "Access denied") to search through recorded video for this activity and subsequent activity of this type generated by the same person at the same reader or portal.
6. Click the person's name and make a selection on the drop-down menu to search through recorded video for:
 - This activity and subsequent activity generated by this person at any reader or portal
 - This activity and subsequent activity generated by this person at the same reader or portal
7. Click the reader or portal location for an event and make a selection on the drop-down menu to search through recorded video for:
 - This activity and all subsequent activity at this reader or portal
 - This activity and subsequent activity generated by the same person at this reader or portal
 - This activity and subsequent activity of the same type at this reader or portal

See also: [Using the Forensic Desktop](#)

[Beginning a Forensic Search](#)

[Composing a Forensic Case](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Using the Forensic Desktop Video Player

To open the Forensic Desktop from the Home page, click the **Forensic Desktop** icon in the **User Tasks** widget:






- or -


Select **Administration : Forensic Desktop**.

Using the Forensic Desktop Video Player, you can view and analyze selected recorded video to locate, trim, and save images of a specified time, event, location, person, or activity.

Once you have a video image in the player, you can use these tools to research recorded video:

1. Click the Play button  to review what is contained in the player's selected clip.
Click the Pause button  to stop the video at any point.


The play head  is shown at the end of the scrub bar. When the clip is paused, the play head can be dragged back and forth to locate the desired portion of the video.

2. Pause the player at the desired start point of the video, click  to mark the start frame for your clip.


The start of the clip is added to the **ScratchPad**.



3. Play again to locate an end point for the clip. Pause, then click  to mark the end point.


Once you have selected both start and end points, the edited clip is shown in the **ScratchPad**.

4. Click Play Next Video Clip button  or Play Previous Video Clip button  to play adjacent clips in a case, the **ScratchPad**, or a selected group of thumbnails in the **Timeline**.

The video fades out and in to show the transition between clips.

5. Click  in the upper left of the player window to display a person's photo ID, if available with this clip.

6. Click , or click on the image in the player, to make the view larger. Click  to restore the player window to the original size.

7. For a closer view, click  to enter the digital zoom mode. Use the digital zoom tools to zoom in and out, pan or move within, or return to original size, of a high resolution video clip.

NOTE: Digital Zoom function brings up the highest resolution video stream available, to provide the highest quality image during playback.



Cancel digital zoom mode



Reset the image scale



Move the image



Double click to zoom out



Single click to zoom in



Click to use zoom selection rectangle to obtain a close up view of an area of the image

8. Click on the player time of the current frame, shown in green under the image, to refresh the start time for the **Activity Log** and to display thumbnails of the other cameras containing video recorded within minutes of your selected clip.
9. Use these techniques for examining video in the player to [create and save forensic cases](#).

See also: [Using the Forensic Desktop](#)

[Beginning a Forensic Search](#)

[Using the Forensic Desktop Activity Log](#)

[Creating and Saving Clips](#)

[Using the Forensic Desktop Timeline](#)

[Composing a Forensic Case](#)

[Printing and Exporting Forensic Cases](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Creating and Saving Clips

To open the Forensic Desktop from the Home page, click the **Forensic Desktop** icon in the **User Tasks** widget:





- or -


Select **Administration : Forensic Desktop**.



Using the Forensic Desktop **ScratchPad**, you can search through recorded video to locate and save edited images of a specified time, event, location, or activity.

The **ScratchPad** is your work area for storyboard editing. Clips are placed (or removed) here to build and save forensic cases.

To edit video clips for building a case:



1. Click the Play button  to review what is contained in the player's selected clip.
Click the Pause button  to stop the video at any point.

The play head  is shown at the end of the scrub bar. When the clip is paused, the play head can be dragged back and forth to locate the desired portion of the video.

2. Click  to mark the start frame for your clip. The start of the clip is added to the **ScratchPad**.
3. Continue playing to locate an end point for the clip. Click  to mark the end point.
Use the scrub bar to adjust your selections for start and end points. Once you have selected both start and end points, the edited clip is shown in the **ScratchPad**.

Trimming the clip allows you to remove irrelevant portions of the video.

4. Add comments to the clips in the **ScratchPad** if desired.


5. Click Play Next Video Clip button  or Play Previous Video Clip button  to play adjacent clips in the **ScratchPad**.


The video fades out and in to show the transition between clips.

NOTE: You can click and drag to select more than one video clip at once. These clips can be played and/or saved as a group.

6. See [Using the Forensic Desktop Timeline](#) for techniques to research video for building a case.
7. Repeat the above steps to edit clips that are needed to build a case file.

To save selected video clips:

1. When you find the video clip or image, or group of clips, for which you are searching, and have them in the **ScratchPad**, click the save icon .
2. In the **Save Clip** dialog box, fill in a new **Case Name**, keep or change the **Clip Name**, and add any comments or description, then click **Save**.

NOTE: You can save the clip into an existing case by selecting the case name from the **Save Clip** drop-down list .

3. Use this method of researching and saving clips to [compose a forensic case](#).

See also: [Using the Forensic Desktop](#)

[Beginning a Forensic Search](#)

[Using the Forensic Desktop Activity Log](#)

[Using the Forensic Desktop Video Player](#)

[Using the Forensic Desktop Timeline](#)

[Composing a Forensic Case](#)

[Printing and Exporting Forensic Cases](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Using the Forensic Desktop Timeline

To open the Forensic Desktop from the Home page, click the **Forensic Desktop** icon in the **User Tasks** widget:



- or -




Select **Administration : Forensic Desktop**.

Using the Forensic Desktop **Timeline** tab, you can search through recorded video to locate and save images of a specified time, event, location, or activity.

To initiate a Timeline search:



1. If it is not selected automatically when you choose a date/time or event, select the **Timeline** tab to initiate a search of the recorded video for the specified date, time, and camera, or by the **Activity Log** selection, using the default stride and thumbnail size.

Click  to refresh the **Timeline** if the date/time/event criteria are changed.

2. Change the **Timeline** settings, as needed, to refine the search.
 - From the thumbnail stride  drop-down menu, specify the stride (minimum interval) to be skipped before the next clip (in frames, seconds, minutes, hours, or days).
After the start point of each clip found, the system "skips" double the stride length selected, then searches for recorded video to start the next clip. Reduce the stride length, if needed, to narrow the clips to smaller segments.
 - Specify the size of the thumbnails by selecting between the larger  or smaller  thumbnail size buttons.
 - The **Timeline** fills rows with available video clips at the selected stride starting from the specified date and time and at the thumbnail size selected.



A yellow vertical bar between thumbnails indicates there is a gap greater than the stride length.

A red vertical bar indicates the end of available video (usually reaching the present time).

NOTE: If the video clip thumbnails extend beyond the number of rows displayed, the red bar may not be seen in the thumbnails tray. Use the scroll down  or scroll up  buttons to advance the thumbnail rows one-at-a-time to examine rows not initially seen in the thumbnail tray.

To expand your research:

1. Use the Forensic Desktop video player to further examine individual video segments. See [Using the Forensic Desktop Video Player](#) for more details.

NOTE: If the **Timeline** is out of sync with the search criteria, click  on the tab to refresh the **Timeline**, beginning at the new start point. If the **Camera List** is out of sync with the **Search Clock**, click  on the tab to refresh the **Camera List**, beginning at the new start point selected. Refreshing synchronizes the available camera thumbnails with the **SearchClock** or selected **Activity Log** event with an associated camera.

2. Click on the video player date/time of the current frame, shown in green under the player image, to refresh the start time for the **Activity Log** reference time and to display thumbnails of the other cameras containing video recorded within minutes of your selected clip.

This feature provides you the ability to easily follow recorded video over time, to see what happened next, using other camera views, building a case by tracking sequential as well as simultaneous events across multiple cameras.

NOTE: Hovering over the **Activity Log** entries highlights the associated camera thumbnails in the **Timeline** as you move the mouse over the entries.

3. Select any additional displayed **Camera List** thumbnails to review these specific additional camera views and further build your forensic case.
4. Repeat the above steps to locate clips that are needed to build a case file.

NOTE: You can click on a thumbnail in the **Timeline** and drag across adjacent thumbnails to select more than one at once. These clips can be played and/or saved as a group.

5. Use these methods of researching and locating the appropriate recorded video to [compose forensic cases](#).

See also: [Using the Forensic Desktop](#)

[Beginning a Forensic Search](#)

[Using the Forensic Desktop Activity Log](#)

[Using the Forensic Desktop Video Player](#)

[Creating and Saving Clips](#)

[Composing a Forensic Case](#)

[Printing and Exporting Forensic Cases](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Composing Forensic Cases

To open the Forensic Desktop from the Home page, click the **Forensic Desktop** icon in the **User Tasks** widget:




- or -

Select **Administration : Forensic Desktop**.

Locate and refine a video clip or clips of interest, as described in [Beginning a Forensic Search](#), then compose forensic cases by saving the selected video to a new case or an existing case.


To start a new case:

1. Save a clip or group of clips:

- Select a clip or drag to select a group of clips in the **ScratchPad**.
 - Click **Save Case**  to save clip(s) to a new case. Display the **Save Case** drop-down list, if needed, to select **Untitled Case**.
2. Fill in the **Save Clip** form with your Case Name, Clip Name, and Comments to be added to the Comment Log.

NOTE: You can accept the default clip name that consists of the date and time.

To add clips to an existing case:

1. Save a clip or group of clips:
 - Select a clip or drag to select a group of clips in the **ScratchPad**.
 - Display the **Save Case** drop-down list .
 - Select the name of an existing case from the list.

NOTE: Cases are stored in the case library in alphabetical order by case name.

2. Fill in the **Save Case** form with the Clip Name, and comments to be added to the comment log.

NOTE: When saving a series of clips in an existing case, the case name will be the same for each clip by default unless changed.

To open an existing case:

1. Click the **Case Inspector** tab.
The saved cases are displayed in the Case Inspector panel.
2. Click on the case thumbnail to select a case.
The contents of the last saved clip in this case are displayed in the Player, so you can continue to investigate from where you last searched.

To build a case:

1. Search for additional clips that represent different dates/times.
2. Search for clips that provide views from other cameras.
3. Use the digital zoom player controls to view details of the recorded video clips.

See [Creating and Saving Clips](#) for more detailed suggestions about building cases. See [Printing and Exporting Forensic Cases](#) for how to print images and export video clips and cases.

See also: [Using the Forensic Desktop](#)

[Beginning a Forensic Search](#)

[Using the Forensic Desktop Activity Log](#)

[Using the Forensic Desktop Video Player](#)

[Creating and Saving Clips](#)

[Printing and Exporting Forensic Cases](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Printing and Exporting Forensic Cases

To open the Forensic Desktop from the Home page, click the **Forensic Desktop** icon in the **User Tasks** widget:




- or -

Select **Administration : Forensic Desktop**.


The Forensic Desktop provides tools for using the cases in the case library to print an image, and to export clips and cases for further research and archiving.

To print an image from a clip:

1. Select a clip from a case folder in the **Case Inspector** tab, the **Saved Clips** panel, the **ScratchPad**, or from a thumbnail in the **Timeline**.
NOTE: The frame of the clip displayed/paused in the player is the image that will be printed.
2. Select Print image from clip player  from the menu bar at the top of the page.

Use the print dialog to select print specifications.

To export a clip or a case:

1. Select a clip or multiple clips from a case folder in the **Case Inspector** tab, the **Saved Clips** panel, the **ScratchPad**, or from a thumbnail in the **Timeline**.
2. Select Export case clips  from the menu bar at the top of the page.
3. Fill in the **Video Clip Export** form.

- Assign a file name.
- Select a video format: either **AVI** or **PS** (MPEG-PS). Choose **AVI** (the default format) for short video segments. Choose **PS** for longer segments with motion-triggered recording.

NOTE: The AVI format does not handle varying frame rates and gaps in recording. Exporting video to AVI for cameras with motion-triggered recording is likely to play back at an apparently slower rate than the original recording. The Program Stream (PS) export format does not have this limitation. Played through the NetVR Player, exported PS/PSI files should play at the original recorded rate.

- Accept or select a case name from the list of case names.

- In the list of clips, select the check box of each clip to be exported, or click **Select All** to export all clips.
- Click **Export**.
- The video file is saved to the folder you configured when you installed the **Video Accelerator**.

NOTE: If you need assistance locating your exported video files, search by the extensions, either .avi or .ps.

To play exported video:

- Play PS files using the **NetVR Player** found under Start/Programs/S2 NetVRClient/S2 NetVR Player.
NOTE: If the NetVR Player is not installed on your PC, use the link on the *Configuration : NetVR Appliance* page to install it.
- Play AVI files using Windows Media Player.

See also: [Using the Forensic Desktop](#)

[Beginning a Forensic Search](#)

[Composing a Forensic Case](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

Handling Lost Cards

Select **Administration : Lost Cards**.

If an access card is found and turned in, you can use the Quick Search feature on this page to determine the identity of the cardholder. To use this feature, your user role must include the **Card - Lookup** permission.

To handle a lost card:

1. In the **Hot stamp #** text box, enter the number printed on the card and click the **Search** button.

A list of cardholders with that card number appears. If you have sufficient permission, you can click a name in the list to view the person record.

- or -

If there is no number printed on the card, click the **Use Reader** link to display a small reader window.

2. Select a reader from the **Reader** drop-down list, and then present the card to that reader.

The card number will fill the **Hot stamp #** text box.

4. Click the **Search** button.

See also: [Specifying Card/Keypad Formats](#)

[Adding People to the System](#)

[Managing a Person's Credentials](#)

[Handling Temporary Credentials](#)

[Decoding Cards](#)

People Administration

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 be added to the system. To add a person, you create a person record.

You can create a person record 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. If the **Add person using template** drop-down list appears at the top of the page, do one of the following:
 - Select the template you want to use from the list of available templates.
 - 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.
 - 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](#) 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 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.

3. Review the information on the tabs and make any needed changes and additions. For information on each tab, see [Editing and Deleting Person Records](#).

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

4. Click **Save**.

If you used a template, the template name appears in the read-only Template field.

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

See also: [Searching for Person Records](#)

[Changing a Person's Access](#)

[Managing a Person's Credentials](#)

[Creating Person Record Templates](#)

[Handling Temporary Credentials](#)

[About Remote Lockset User Types](#)

Finding and Changing Person Records

Searching for Person Records

Select **Administration : People Search**.

On this page you can search for person records that you want to view, edit, or delete. You can:

- [Scan a credential to find person records with matching hot stamp numbers.](#)
- [Enter values in search criteria fields to find person records with matching values.](#)

NOTE: You can also click the **Add** link at the top of this page to [add people to the system](#).

To search 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. See [Editing Person Records](#) for more information.

To search by entering search criteria:

1. Specify your search criteria by filling in any of the available fields on the **People** page.
 - A field marked with an asterisk will find complete, exact matches only. For example, if you enter 123 in the **ID#** field, a person whose ID number is 1234 will not be found.
 - A field that is not marked with an asterisk can find partial matches. For example, if you enter the first letter of a person's last name, all people whose last names begin with that letter will be found.
 - For a person record to be found, it must match the entries in all fields for which you have entered values. For example, if you enter a last name and a department name, only people whose last name AND department name match those entries will be found.
2. Use the **Expiration date before** and **Expiration date after** fields to find people whose person records have expiration dates that are 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 the 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 appear only if you have access to multiple partitions.
 - Select **<visible>** to include records located in other partitions that are visible within the active partition.
 - Select **<current>** to include only records located in the active partition.
 - Select the name of a partition to include only 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 options:
 - **Include deleted records:** Records that have been deleted will be included.
 - **Include expired records:** Records that have expired will be included. This check box is selected by default.
 - **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 a person.
 - **Include only records for persons exempted from PIN entry:** Only records for people who have been exempted from PIN entry at portals with keypads will be included.
7. Click **Search**.
 8. In the list of matching records, click a name to open the person record. If only one record matches your search criteria, that record opens automatically.
 9. Make any needed changes to the person record. See [Editing Person Records](#) for more information.

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 person record to navigate to the other partition. You will then be able to edit the person record, if you have sufficient access rights in that partition. After saving your changes, you can switch back to the original partition by clicking the **Switch Partition to Original** button.

10. Click **Save**.

See also: [Adding People to the System](#)

[Editing Person Records](#)

[People Reports](#)

Editing Person Records


Select **Administration : People : Search**.

After [performing a search](#) to find the person record(s) you want, you can:

- Add or change information in a person record. For example, you can change the person's access levels and credentials, ID photo, contact information, and login information. On the Partitions tab (described below), you can make person records visible to, and available for limited editing by, administrators in other partitions.
- Delete or undelete a person record. Note that deleting a person's record does not remove it from the system, it only removes it from the active roster. When you view a deleted record, the **Delete** action button changes to **Undelete**.

NOTE: If your search resulted in a list of matching person records, buttons that appear in the lower right corner of each record let you quickly move to:

The next or previous record in the list:  or 

The first or last record in the list:  or 

Basic Personal Information

At the top of a person record, you can modify the following fields:

1. 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.
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](#) for more information.

NOTE: The activation date and time, and the expiration time, you set in a person record will be ignored if the person presents his or her credentials at an ASSA ABLOY remote lockset. However, the lockset will check the expiration *date* if one is entered and will allow the person access only until midnight on that date.

3. If your organization issues ID numbers, enter the person's ID number 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.

Access Control Tab

On the Access Control tab you can issue, revoke, and temporarily disable credentials; assign and remove access levels; assign a PIN; assign regional anti-passback privileges; and assign an extended unlock period. You can also assign an email distribution group whose members will be notified when the person record, or any credential or access level assigned to the person, is about to expire. For more information, see [Changing a Person's Access](#).

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 that you upload must have a unique name and must end with the extension .jpeg or .jpg. It must be no larger than 80KB—or on an Extreme or Enterprise system, no larger than the current [photo ID size limit](#).

NOTE: To export a photo ID image, right-click it and use your browser's Save function to save the .jpeg or .jpg file to the desired location.

The read-only **Badge Print Count** field displays the number of times the badge for this person has been printed.

See also: [Photo ID Badging Installation, Setup, and Operations Guide \(PDF\)](#)

[Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Batch Printing Photo IDs](#)

[Capturing and Saving Digital Signatures](#)

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 your system. If the person record was created from a [template](#), some or all of these fields might be pre-filled.

See also: [Configuring the Display of the Person Record](#)

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.

NOTE: 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.

NOTE: If you configure an [LDAP server](#) for password authentication, you will not need to enter passwords here.

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 this group.
6. Select a default [Widget Desktop layout](#) for this person from the **Default Widget Desktop** drop-down list. This is the layout that will appear automatically when the person opens the Widget Desktop after logging into the system.
7. Assign a [custom menu](#) to this person by selecting it from the **Custom Menu** drop-down list. The list shows all available custom menus in the active partition.

This assignment will take precedence over any partition-based or role-based custom menu assignment that would otherwise apply to this person.

NOTE: A predefined custom menu named *User Tasks* includes the same set of options that in earlier releases appeared in the User Tasks widget on the Home page.

The default user roles for security management system users are listed below, from lowest to highest:

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

In addition to the roles above, you can assign custom user roles created using the **Configuration : Site Settings : User Roles** page. For more information, see [Creating User Roles](#).

NOTE: The [page bar](#) is built dynamically for each user who logs in. It shows only controls for accessing pages the user has permission to view or use based on his or her user role.

See also: [Setting Up Directory Services](#)

[Setting Up Partitions](#)

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 (via the **Share all people with every partition** option on the [Network Controller page](#)), the tab displays a note to that effect.

The level of access that administrators in these partitions will have to the person record depends on whether the **Allow edit of persons made visible** option is also selected on the Network Controller page. If that option is selected, the administrators will have full access to the person record, including full editing rights. If it is not selected, the administrators will have **limited access** to the person record. 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. On the **Personal Information** page, click the **Partitions** tab.

The **Partition** drop-down list includes all other partitions in which you have at least administrator privilege, or that have been made visible by their administrators.

3. Select the partition whose administrators should be granted limited access to this person record.
4. Enter the date and time the limited access should expire.
NOTE: Clicking the calendar icon displays a calendar you can use 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.

If you have a NetVR system, you can use this tab to access video related to recent activity. For more information, see [Accessing Recorded Video from a Person Record](#).

See also: [Access History Reports](#)

Changing a Person's Access

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

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

- Issue, revoke, and disable credentials. See [Managing a person's credentials](#).
- [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 individual users from credential non-use rules](#).
- [Trace a person's activity](#).
- [Assign an email distribution group for notification of credential, access level, and person record expirations](#).
- [Assign a PIN](#).
- [Assign an extended unlock period](#).

NOTES: In a person record that was created 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. [Perform a search](#) to display the person record you want to change.
2. Under Access Levels on the Access Control tab, select each access level you want to assign from the Available list and click the right arrow button to move it to the Selected list.
Use SHIFT-click to select multiple access levels at once.
2. (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.
3. 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.
4. Click **Save**.

NOTE: Access levels 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 set or remove an activation date or expiration date for an access level:

1. In the list of access levels, double-click anywhere in the row for the access level you want to edit.
2. 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.
3. 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.
4. 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.
5. To have the system automatically remove the access level once it expires, select **Yes** from the **Auto-remove** drop-down list.
During the daily system check, the controller will check for and delete expired access levels.
6. Click **Save**.

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

To assign regional anti-passback privileges:

1. 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.

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 Passback violations and Tailgate violations behaviors selected on the [Regions](#) page.

2. 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 (on the [Network Controller](#) page), you can exempt individuals from this rule.

1. Select the **Exempt from credential non-use rules** check box.
2. Click **Save**.

To trace a person's activity:

1. To trace this person's activity in the active partition, select the **Trace this person** check box.
2. Click **Save**.

Whenever this person makes a valid or invalid access request in the active 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 activated whenever this person makes a valid or invalid access request in the active 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. If the **Notify on expirations** drop-down list appears at the bottom of the Access Control tab, 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.

2. Click **Save**.

You will see the **Notify on expirations** drop-down list only when the **Enable expiration notification** option is selected on the [Network Controller](#) page. The number of days before an

expiration the notification will be sent is determined by the **Notification period** set for that Network Controller option.

To assign a PIN:

1. In the **PIN** text box in the lower right corner of the **Access Control** tab, enter a four- to six-digit PIN.
NOTE: Most Wiegand keypads support four-digit PINs. Bit-burst keypads support PINs of any length.
2. Alternatively, click this 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](#).
3. To exempt this person from the need to enter a PIN at portals with keypads (card-only access), select the **Exempt from PIN** check box.
Users can select the Exempt from PIN attribute when creating Custom People report definitions and defining person search criteria.
4. Click **Save**.

To assign an extended unlock period:

1. 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 setting in the portal definition.
2. Click **Save**.

See also: [Setting Up Access Levels](#)

[Adding People to the System](#)

[Editing and Deleting Person Records](#)

[Managing a Person's Credentials](#)

[Managing Email Distribution Groups](#)

[Handling Missing Credentials](#)

Managing a Person's Credentials

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

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

- Issue a 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](#).

For information on assigning access levels and setting other options on the Access Control tab, see [Changing a Person's Access](#). For information on the automatic expiration of active credentials, see [About Automatic Credential Expiration](#).

To issue a new credential using a reader:

1. [Perform a search](#) to display the person record you want to change.
2. On the Access Control tab, 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 on the list. To enable a credential format, a user with setup privileges must select its Enabled check box 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. Once this date is reached in the controller's time zone, the system will change the credential's status from *Active* to *Expired*.
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, and then click **Go**.
10. Present the credential to the reader. The encoded credential number appears in the **Encoded #** box.

NOTES: If auto-incrementing of encoded credential numbers is enabled for your system (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 (on the [Network Controller page](#)), 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 **Add New Credential** button.
2. 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 (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.

NOTE: If the person already has the maximum number of active access credentials set for your system (on the [Network Controller](#) page), 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.

3. Select a format from the **Credential Format** drop-down list.
4. (optional) Select a different status for the credential from the **Status** drop-down list. See "To disable a credential" below for more information.
5. (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.
6. (optional) To set an expiration date for the credential, click the **Expiration Date** calendar icon and select a date from the calendar that appears. Once this date is reached in the controller's time zone, the system will change the credential's status from *Active* to *Expired*.
To remove an expiration date from a credential, click the date and then press **DELETE**.
7. Click **Save**.

To issue a new credential for use with remote locksets:

1. Click the **Add New Credential** button.
2. Enter the hot stamp number printed on the credential into the **Hot stamp #** box, and enter the encoded credential number into the **Encoded #** box.
- or --

For a PIN-only credential, enter the six-digit PIN into both the **Hot stamp #** box and the **Encoded #** box.

NOTES: If auto-incrementing of encoded credential numbers is enabled for your system (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 access credentials set for your system (on the [Network Controller](#) page), 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.

3. Select a format from the **Credential Format** drop-down list. For a PIN-only credential, select **Remote Lockset PIN Only**.
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.
4. (optional) Select a different status for the credential from the **Status** drop-down list. See "To disable a credential" below for more information.
5. (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.

- (optional) To set an expiration date for the credential, click the **Expiration Date** calendar icon and select a date from the calendar that appears. Once this date is reached, the system will change the credential's status from *Active* to *Expired*.


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

- (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 a credential. For more information, see [About Remote Lockset User Types](#).

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 other confirmation that the credential was not read, and no information about the access attempt is recorded.

- Click **Save**.

To revoke a credential:

- In the list of credentials, select the credential you want to revoke.
- Click this icon  to revoke the credential.
- Click **Yes** in the **Revoke Credential** confirmation dialog box.

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

NOTE: 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 one of the procedures above for issuing a new credential.

To disable a credential:

- In the list of credentials, select the credential you want to disable. A disabled credential cannot be used for access.
- On the **Status** drop-down list, change the **Active** setting to any of the following:
 - **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 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*.

You can run a [Credential Audit report](#) to view existing credentials by their current status settings. You can assign a [credential profile](#) to individual credentials to have the system automatically disable them after a specific number of days of non-use.

See also: [Changing a Person's Access](#)

[Handling Temporary Credentials](#)

[About Automatic Credential Expiration](#)

[Adding People to the System](#)

[Editing and Deleting Person Records](#)

[Customizing Credential Attributes](#)

Handling Temporary Credentials

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 whenever 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](#).
- [Return temporary credential\(s\) and optionally reactivate the missing credential\(s\) immediately](#).
- [Reactivate missing credentials\(s\)](#).

To issue a temporary credential:

1. Click the [Access Control tab](#) in the person record you want to change.
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. Scan the temporary credential.

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]."

6. Click **Save**.

NOTE: A person can have only one active temporary credential at a time. Each time an additional temporary credential is issued to a person, the previously issued temporary credential is disabled and its status changes from *Temporary* to *Temporary Expired*.

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. Scan the temporary credential.
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](#) 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.

2. If a read is required to reactivate missing credentials, a reactivation dialog 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**.
 - Scan a missing credential. The credential's status changes from *Missing* to *Active*.
 - Scan 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 credentials at a later time, using the procedure below.

3. 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 the 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. Scan a missing credential. The credential's status changes from *Missing* to *Active*.
5. Scan 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**.

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.

See also: [Managing Credentials](#)

[Creating a Temporary Credential Policy](#)

[Changing a Person's Access](#)

[Adding People to the System](#)

[Editing and Deleting Person Records](#)

[Customizing Credential Attributes](#)

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 been reached in the controller's time zone. 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 been reached in the controller's time zone. 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*.

See also: [Managing a Person's Credentials](#)

[Handling Temporary Credentials](#)

[Customizing Credential Attributes](#)

[Adding People to the System](#)

[Searching for Person Records](#)

[Editing and Deleting Person Records](#)

Credential Formats

26-Bit Wiegand

	Start Bit	Number of Bits
Facility Code	2	8
Card ID Number	10	16

Casi Rusco 40 Bit

	Start Bit	Number of Bits
Facility Code	1	19
Card ID Number	20	19

Corporate 1000 35 Bit

	Start Bit	Number of Bits
Facility Code	2	12
Card ID Number	14	20

Corporate 1000 48 Bit

	Start Bit	Number of Bits
Facility Code	3	22
Card ID Number	25	23

FIPS 201 128 Bit

	Start Nibble	Number of Nibbles
Agency Number	1	4
System Number	5	4
Credential Number	9	6
Credential Series Number	15	1
Credential Issue Number	16	1
Person Identifier	17	10
Organization Category	27	1
Organization Identifier	28	4
Person Organization Category	32	1

NOTE: The 32 characters are encoded as binary-coded decimal (BCD) digits. The FIPS 201 128-bit credential format can be enabled and disabled, but it cannot be modified or used to create a new format.

FIPS 201 75 Bit

	Start Bit	Number of Bits
Agency Number	2	14
System Number	16	14
Credential Number	30	20

NOTE: The 48 characters are concatenated to form a single, 14-digit credential number and are displayed in the person record. The FIPS 201 75-bit format can be enabled and disabled, but it cannot be modified or used to create a new format.

Honeywell 40 Bit

	Start Bit	Number of Bits
Facility Code	2	12
Card ID Number	14	18

Lenel 36 Bit

	Start Bit	Number of Bits
Facility Code	1	16
Card ID Number	17	18

S2 36 Bit

	Start Bit	Number of Bits
Facility Code	33	3
Card ID Number	2	31

Software House 37 Bit

	Start Bit	Number of Bits
Facility Code	5	10
Site Code	15	6
Card ID Number	21	16

NOTE: The Network Controller supports Facility Code only or Site Code only, but not both. One can be ignored, or both groups of bits can be used for the facility code with a start bit of 5 and a bit length of 16.

STRAC 128 Bit

	Start Bit	Number of Bits
--	-----------	----------------

GUID	1	128
Card ID Number	1	128

NOTE: The GUID of the card in hex format (for example, 5d569f218bfc42c39cdeb98caac41ce0) is displayed and used as the encoded card number in the security management system.

See also: [Decoding Cards](#)

[Specifying Card/Keypad Formats](#)

About ASSA ABLOY Remote Lockset User Types

When you are [issuing a new credential](#) to be used with ASSA ABLOY remote locksets, you can assign any of the remote lockset user types listed below. Your assignment will affect the user's access and abilities at portals currently accessible to the user based on his or her access levels.

Once a card has been assigned a remote lockset user type, it is no longer usable as an access card. The exception is **Regular Access Card**, which allows a card to function with both remote locksets and regular locks. This is the user type you will select for the majority of the users in your system.

NOTE: Users whose cards have been assigned any of the user types listed below, except **Emergency Open**, may be constrained by time specs. That is, the users may be denied access or functionality at a portal for which a time spec is in effect.

- **Regular Access Card:** By presenting this card, a user can momentarily unlock the remote lockset (or regular lock). The card gives the user no special abilities. For example, the user's credentials will not be accepted during lockout and panic modes (described below).
- **Trigger Comm Update:** By presenting this card, a user can start a communications session between the remote lockset and the controller.
- **Toggle Passage Mode:** By presenting this card, a user can toggle the remote lockset between passage mode (described below) and the locked state.
- **Relock Passage:** By presenting this card, a user can relock the lockset if it is in an unlocked state for any reason, but cannot unlock it. When passage mode ends (at the end of the scheduled unlock period for the portal), the relock request is discarded and the lock returns to normal operation. This user type is useful, for example, when a lockset must be re-locked before its scheduled lock time.
- **Panic Lockdown:** By presenting this card, a user can place the lockset into panic mode.
- **Lockout Users:** By presenting this card, a user can toggle the remote lockset between lockout mode and normal operation. Note that the door does not unlock when it goes into lockout mode; the card cannot be used to gain access. This user type is especially useful for preventing people from entering an area where a dangerous situation has been identified.
- **Master Clear Lockouts:** By presenting this card, a user is never granted access but is able to clear panic, lockout, and relock modes for the remote lockset.
- **Emergency Open:** By presenting this card, a user can unlock the remote lockset for emergencies, regardless of panic, lockout, or relock modes—and in spite of low battery situations for battery powered locksets. If passage mode is in effect when the user presents the card, the lockset returns to passage mode. Otherwise, the lockset remains unlocked for the duration of the [Extended Unlock Time](#) specified in the portal definition.

- **Supervisor Open:** By presenting this card, a user can unlock the remote lockset regardless of lockout mode, but cannot override panic mode.

NOTES: Sx locksets support all user types listed above. Px locksets support only the Regular Access Card, Trigger Comm Update, and Supervisor Open user types.

The Panic Lockdown user type observes time specs, but the Emergency Open user type ignores them.

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

About Remote Lockset Modes

- **Passage mode:** Activated either at the start of the scheduled unlock period for the portal, or when a user presents a **Toggle Passage Mode** card. Although the lockset is in passage mode, it is not actually unlocked until a valid card is presented.
- **Lockout mode:** Activated when a user presents a **Lockout Users** card. If the lockset is in passage mode, it is re-locked. Access is granted only to users who present **Master Clear Lockouts**, **Emergency Open**, or **Supervisor Open** cards. Lockout mode can be cleared by any user with a **Lockout Users** or **Master Clear Lockouts** card.
- **Panic mode:** Activated when a user presents a **Panic Lockdown** card or when a remote command is issued. It immediately cancels passage mode and locks out all users except those with **Master Clear Lockouts** and **Emergency Open** cards for the duration of the panic. Panic mode can be cleared by a user with a **Master Clear Lockouts** card or via a command from the server.

See also: [Overview: Integrating Remote Locksets](#)

[Enabling and Configuring Remote Locksets](#)

[Configuring Remote Lockset Advanced Options](#)

[About the Remote Lockset Advanced Options](#)

[Creating Remote Lockset Profiles](#)

[Creating Time Specs](#)

[Viewing Remote Lockset Status](#)

[Monitoring Remote Locksets](#)

[Remote Locksets Report](#)

[Integrating Remote Locksets \(PDF\)](#)

Managing Email Distribution Groups

Select **Administration : People : Manage Email Distribution Groups**.

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

For example, if expiration notification is enabled for your system (on the [Network Controller page](#)), you can have the system notify certain people when an individual's person record, credential, or access level is about to expire. To do this, you add the people to an email distribution group and then assign the group to the individual's person record.

You can also select an email distribution group when defining a Send Email or Send SMS Message action for an event. When the event is activated, an email or SMS message will be sent to everyone in the group.

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 [Searching for Person Records](#).

3. Click **Search**.

The names of people matching your search criteria appear in the Results list.

4. For each person you want to include in the distribution group, select the name in the Results list and click the "Move to list" 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.
6. Click **Save** when the Selected list includes the set of people you want in the distribution group.

NOTE: Because email distribution groups refer to their members' person records, a member whose email address changes will continue to receive email distributed by the group.

See also: [Email Server Settings](#)

[Defining Event Actions](#)

[Creating Custom People Reports](#)

[Creating Custom History Reports](#)

[How Groups are Used in the System](#)

Creating and Printing Photo ID Badges

Capturing and Saving ID Photos

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

Select **Administration : People Add** or **People Search**.

Multiple hardware and software products have been integrated to provide image capture and photo ID printing features from within the security management system. Refer to the [Photo ID Badging Installation, Setup, and Operations Guide \(PDF\)](#) for details.

The first step in creating a person's photo ID badge is capturing an ID photo and saving it to the person record.

NOTE: The maximum image size is 80 KB, unless the [Photo ID Size Limit](#) has been increased on the Network Controller page.

To capture and save an ID photo:

1. [Add a new person](#) to the system or [search for an existing person record](#).
2. Click the Photo ID tab in the person record.
3. Select the badge design you want to use from the **Badge** drop-down list.
4. Select the **Request Photo ID** check box.
5. Click **Photo ID** to display the Photo IDs pop-up window.

NOTE: To use the imaging software needed for batch printing, you will need to add your controller's IP address to your browser's list of trusted sites. For example, in the Internet Explorer Tools menu, select Internet options, click the Security tab, select the Trusted sites zone, click the Sites button, and add the controller's IP address to the zone.

6. In the Photo IDs window, click **Capture Image** to display the Select Image Source window.
7. Select the appropriate image source for your camera.
For example, select **Microsoft WDM Image Capture (Win32)** if you are using a Logitech camera, or select **Canon Live Capture** if you are using a Canon camera.
8. Click **OK** to display the Capture window for your camera.

NOTE: The value shown in the read-only **Badge Print Count** text box indicates the number of times the specific badge has been printed.

9. Ensure that the person is properly within the picture frame and is at least six feet away from the camera, then click the capture button.
10. Click **OK** to close the Capture window and redisplay the Photo IDs window with the image placed in the badge design.
11. Confirm that the person's image is correctly captured and then click **Save Image**.
The captured image appears in the person record.
12. Click **Close** in the Photo IDs window.
13. Scroll to the bottom of the person record and click **Save**.

NOTE: To save this image separately as a JPEG or bitmap file, right-click it in the person record and select **Save Picture As**.

See also: [Photo ID Badging Installation, Setup, and Operations Guide \(PDF\)](#)

[Printing Photo IDs](#)

[Batch Printing Photo IDs](#)

[Configuring the Topaz Signature Pad to Create Signed Photo IDs \(PDF\)](#)

[Uploading Photo ID Layouts](#)

[Photo ID Requests Report](#)

[System Data for Photo ID Layouts](#)

[Deleting Photo ID Layouts](#)

Printing Photo IDs

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

Select **Administration : People Add** or **People Search**.

Multiple hardware and software products have been integrated to provide image capture and photo ID printing features from within the security management system. Install the software and drivers from the CD provided, and refer to the [Photo ID Badging Installation, Setup, and Operations Guide \(PDF\)](#).

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

After [capturing an ID photo](#) and saving it to a person record, you can use the Photo ID tab to:

- [Print a photo ID badge at your workstation](#).
- [Request printing of a photo ID badge](#).
- [Print photo ID badges from the request queue](#).
- [Capture and save digital signatures](#).
- [View the number of times a badge has been printed using the Badge Print Count field](#).

To print a photo ID badge at your workstation:

1. Make sure the photo ID printer is connected to your workstation with a USB cable. See the manufacturer documentation for guidance on hardware setup.
2. Make sure the printer's Windows driver listed above is installed on your workstation. See the manufacturer documentation for guidance on software and driver installation.
3. [Add a new person](#) to the system or [search for an existing person record](#).
4. Click the Photo ID tab in the person record.
5. Select the badge design you want to use from the **Badge** drop-down list.
6. Click **Photo ID** to display the Photo IDs pop-up window.

NOTE: If the window does not appear, turn off the pop-up blocker or add the Network Controller site to the allowed site list.

7. If you are printing a magnetic stripe card, select the card id number from the **Access Cards** drop-down list, and clear the **Use Default Printer** check box.
8. Click **Print Photo ID**.
The Print dialog box (or the Card Printer Encoder Setup dialog box if you are printing a magnetic stripe card) appears.
9. From the **Name** drop-down list select the photo ID printer.

10. If you are printing a magnetic stripe card, click the Magstripe tab, select the name of the printer you want to use, and then select the printer manufacturer from the **Current Magstripe Encoder** list.
11. Click **OK** and retrieve the badge from the printer tray.
12. If you captured an image in the photo ID window, be sure to click **Save** in the person record. This saves the captured image and selected badge design with the 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. Select **Administration : People : Change/delete** and search for an existing person record.
2. Click the Photo ID tab.
3. Under Badge, select the **Request Photo ID** checkbox.
4. Click **Save**.
5. Select **Administration : Reports : People : Photo ID Requests** and verify that this report lists the request you just made.

To print photo ID badges from the request queue:

1. The photo ID printer must be connected to your workstation with a USB cable. See the manufacturer documentation for guidance on hardware setup.
2. The printer's Windows driver listed above must be installed on your workstation. See the manufacturer documentation for guidance on software and driver installation.
3. Select **Administration : Reports : People : Photo ID Requests**. This report lists all currently outstanding photo ID print requests.
4. Click the printer icon in the Action column (the rightmost column) for the badge you wish to print.
A small photo ID window appears.
5. In the photo ID window, click **Print Photo ID**.
The Print dialog box (or the Card Printer Encoder Setup dialog box if you are printing a magnetic stripe card) appears.
6. From the **Name** drop-down list, select the photo ID printer.
7. If you are printing a magnetic stripe card, click the Magstripe tab and select the name of the magnetic stripe encoder.
8. Click **OK** and retrieve the badge from the printer tray.
9. Close the photo ID window.

See also: [Photo ID Badging Installation, Setup, and Operations Guide \(PDF\)](#)

[Capturing and Saving ID Photos](#)

[Batch Printing Photo IDs](#)

[Configuring the Topaz Signature Pad to Create Signed Photo IDs \(PDF\)](#)

[Uploading Photo ID Layouts](#)

[Photo ID Requests Report](#)

[System Data for Photo ID Layouts](#)

[Deleting Photo ID Layouts](#)

Batch Printing Photo IDs

Select **Administration : People Add** or **People Search**.

After [searching for person records](#), you can click a link that appears above the search results to open the Badge Print Workflow dialog box. This dialog box displays a list of the people found in the search. You can use it to:

- [Batch print multiple photo ID badges](#). You can batch print badges for some or all of the people found in the search, or you can print badges individually.
- [Create a new credential](#) for any person found in the search.
- [Batch print magnetic stripe photo IDs](#). Although batch printing is not designed for use with magnetic stripe access credentials, magnetic stripe information can be encoded for secondary uses such as point of sale, library checkout, or membership IDs.

In addition to the procedures below, refer to the [Photo ID Badging Installation, Setup, and Operations Guide \(PDF\)](#).

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

To batch print multiple photo IDs:

NOTE: Be sure to add your controller IP address to the Internet Explorer Trusted Sites list in order to use the imaging software needed for batch printing. In the Internet Explorer Tools menu, select Internet options, the Security tab, Trusted sites, Sites, and add your IP address to the zone.

1. On the search page, set search criteria to find the people whose badges you want to print.

Example: Search for cardholders whose **Badge Print Count** equals 0. A list of people whose badges have not been printed is returned.

Note that Badge Print Count is a read-only field on the Photo ID tab of a person record, It displays the number of times that person's badge has been printed.

Important: Ensure that information to be printed on these individuals' badges (such as last name, first name, photo image, and any user-defined fields) is already present in their person records before proceeding to use batch printing.

2. Click **Search** to display the search results.
3. Click the **Badge Print Workflow** link in the alphabetical menu bar of the search results screen.

The Badge Print Workflow dialog box displays up to 100 results, allowing up to 100 badges to be printed at a time. After printing the first 100 badges, run the search again to find additional people whose badges have not been printed.

4. Select a layout from the **Badge Layout** drop-down list.
5. Select the badges to be printed.
All results are selected by default, but individual badges may be deselected or reselected from the list. The check box to the left of **Last Name** in the header acts as a toggle to select all or deselect all.
6. Click **Print Selected** to print the checked badges using the default printer for that workstation.
For printing, the Status column changes from "Ready," to "Printing," to "COMPLETED". The Badge Print Count number is incremented each time a badge is printed.

NOTE: You can use the **Print** button that appears on each badge to print individual badges.

To create a new credential for a person:

1. In the Badge Print Workflow dialog box, select a format from the **Credential Format** drop-down list after printing.
2. Enroll the card numbers manually by entering them into the **Encoded Number** box, or enroll them by presentation.

To enroll the numbers by presentation, select a reader from the **Enrollment Reader** drop-down list. Click **Read** and present a printed badge to the reader to add credentials to the badge.

The Status column displays "PRESENT CARD" when **Read** is clicked. Once the badge is read, the column changes to "READ COMPLETE," and the badge's encoded number appears in the **Encoded Number** box.

3. Click **Save** to issue a new credential for the user. The Status column displays "SAVED".
The new credential uses the enrolled number for both the **Hot Stamp #** and the **Encoded #**. It uses the selected **Credential Format**, its Status is set to Active, and no Expiration Date is set.

To batch print magnetic stripe photo IDs:

NOTE: To batch print magnetic stripe cards, you cannot be using the Google Toolbar. The EPI Builder magnetic stripe encoder dialog box does not function properly if the Google Toolbar is installed.

1. Select **Configuration : Site Settings : Network Controller** and click the Access Control tab.
2. Under **Credentials**, select the **Use Magnetic Stripe Encoding** check box.
3. Click **Save**.
4. Verify that the Badge Print Workflow dialog box displays Magnetic Stripe Encoding: ON.
5. Follow the steps in the preceding procedure, *To batch print multiple photo IDs*.
When you click **Print Selected**, the **Card Printer Encoder Setup** dialog box appears.
6. Select the name of your printer from the **Printer Name** drop-down list.
7. Verify the printer manufacturer from the **Current Magstripe Encoder** list.
8. Click **OK**.

9. After printing the badges, continue to the previous procedure, *To create a new credential for a person*, to complete the credentials.

See also: [Photo ID Badging Installation, Setup, and Operations Guide \(PDF\)](#)

[Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Configuring the Topaz Signature Pad to Create Signed Photo IDs \(PDF\)](#)

[Uploading Photo ID Layouts](#)

[Photo ID Requests Report](#)

[System Data for Photo ID Layouts](#)

[Deleting Photo ID Layouts](#)

Capturing and Saving Digital Signatures

The system supports the use of SignatureGem™ signature pads from Topaz Systems, Inc. This feature has been tested with Model T-L462-HSB.

To install the Topaz Signature Pad software:

1. From the Topaz Systems SigPlus eSignature Installation window select **Install SigPlus eSignatures**. Follow the instructions and complete this installation.
NOTE: When the installation program asks you to Select Connection Type, ensure that your selection is correct by first checking the model name on the back of the signature pad. If the model number ends in "HSB" then select the HSB connection type.
2. Plug the signature tablet into a USB port on the computer.
3. Use the DemoOCX application supplied in the installation to verify that the signature pad is correctly installed and working.
4. Create a C:\temp directory on the signature station computer. This is the directory into which the signatures are saved when they are captured.

To create a badge layout that includes a "Signature" image type:

1. Create a "PhotoID" image type, and then create a "Signature" image type. See **View : Image Setup** in EPI Designer.
NOTE: You must create the PhotoID image type first and then the Signature image type. This is because the image type index numbers are hard-coded in this feature.
3. Add a dynamic image for the photo ID to the badge design and set its image type to PhotoID.
4. Add a dynamic image for the signature to the badge design and set its image type to Signature.
5. Confirm that the badge layout shows "PhotoID" and "Signature" in the middle of the image locations in the badge design.
6. Complete your badge design and save it.

To upload your badge design:

1. In the security management system, select **Administration : Utility : Photo ID Layout Upload**.
2. Click **Browse** and browse to the location of your badge design file.
3. Select the badge design file and click **Open**. The path and filename will appear in the **Select file** text box.
4. Click **Save**.

To add a signature by capturing it to a signature pad:

1. Select **Administration : People : Change/delete** and search for the individual's person record.
2. Click the Photo ID tab in the person record.
3. Click **Capture signature**.
The Capture signature dialog box appears.
4. Have the person sign his or her name on the signature pad.
5. Click **Capture signature**, and then click **OK** to confirm that you want to use this signature.

To add a signature by uploading an image file:

1. Select **Administration : People : Change/delete** and search for the individual's person record.
2. Click the Photo ID tab in the person record.
3. Click **Attach Signature**.
4. In the Upload Signature dialog box, click **Choose File**.
5. Browse to the C:\temp directory, and select the signature file. The filename must end with the extension .jpeg or .jpg.
NOTE: Be sure that you browse to the C:\temp directory, and not to the My Documents\temp directory.
6. Click **OK**.
7. Use the **Change** and **Delete** buttons to modify or delete the signature.

To verify that the signature image appears in the badge design:

1. On the Photo ID tab of the person record, click **Photo ID** to open the Photo IDs pop-up window.
2. Select from the drop-down list the badge design containing the dynamic signature image field.
The signature should appear on the badge.

See also: [Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Batch Printing Photo IDs](#)

[System Data for Photo ID Layouts](#)

[Configuring the Topaz Signature Pad to Create Signed Photo IDs \(PDF\)](#)

Report Administration

Select **Administration : Reports** to display the following options.

Choose this	To see information on
Configuration	Reports on the current configuration of system resources.
History	Reports on system activity history.
People	Reports on access information pertaining to people.

See also: [Monitoring the Activity Log](#)

Configuration Reports

Select **Administration : Reports : Configuration** and select the report you want.

As Built Report

To run an **As Built** report, select a Node from the **Network Node** drop-down list and click **Run report**. A new browser window opens and displays an image of each application blade associated with the node and the specific resources configured for that blade. You can print this report.

See also: [Resources Report](#)

Cameras Report

Displays all camera configuration information.

See also: [Creating Camera Definitions](#)

[Setting Up Camera Types](#)

Camera Presets Report

Displays configured presets for each camera in the system.

See also: [Creating Camera Preset Positions](#)

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 emergency call button, and the inputs and outputs corresponding to its floor-select buttons.

See also: [Overview of Elevator Access Control](#)

[Defining Elevators](#)

Floor Groups Report

Displays all configured floor groups for use in elevator control.

See also: [Creating Floor Groups](#)

[Naming Floors to Be Managed By Elevator Access Control](#)

Holidays Report

Displays information on holidays, which act as exclusions to any time spec that does not include them.

See also: [Creating Holidays](#)

[Creating Time Specs](#)

Portals Report

Displays portal definition information.

See also: [Setting Up Portals](#)

[Setting Up Portal Groups](#)

Portal Groups Report

Displays all portal groups, the portals included in each, and the assigned threat level group.

See also: [Setting Up Portals](#)

[Setting Up Portal Groups](#)

[Setting Up Threat Level Groups](#)

Reader Groups Report

Displays defined groups of readers.

See also: [Setting Up Reader Groups](#)

Remote Locksets Report

This report is available if the Remote Locksets feature is licensed for your system. The 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 opens the [Remote Node Cache Contents page](#), where you can view the associated pending/transferred data summary report.

See also: [Overview: Integrating Remote Locksets](#)

[Enabling and Configuring Remote Locksets](#)

Resources Report

Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points. The name of any resource that has been disabled appears in bold italics.

See also: [Setting Up Readers and Keypads](#)

[Setting Up Alarm Inputs](#)

[Setting Up Outputs](#)

[Slot and Position Numbers](#)

Threat Levels Report

Displays all configured threat levels, including their descriptions and color assignments.

See also: [Using Threat Levels to Change System Behavior](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Setting up Threat Level Groups](#)

[Threat Level Settings](#)

[Setting Threat Levels](#)

Threat Level Groups Report

Displays all configured threat level groups and the threat levels assigned to them.

See also: [Using Threat Levels to Change System Behavior](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Setting Up Threat Level Groups](#)

[Threat Level Settings](#)

[Setting Threat Levels](#)

Time Specs Report

Displays all defined time specs currently in the system. Time specs 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. For example, 900 is 9:00 AM and 1700 is 5:00 PM. Holidays are listed in groups as they were entered.

See also: [Creating Time Specs](#)

[Creating Holidays](#)

History Reports

Select **Administration : Reports : History**.

History reports can retrieve data from archives when the requested report data is no longer active on the controller. 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.

Choose this	To see information on
Access History Report	Reports that trace access attempts.
Alarm Resolution Report	Reports tracking alarm resolution—the period between the activation of an alarm and its resolution,
Audit Trail Report	Reports showing changes made to the security database over a specified period of time.
Custom Report	Custom reports created and saved for re-use.
Duty Log Report	Reports showing duty log comments that have been appended to Activity Log entries.
General Event History	Reports showing specific events from the Activity Log.
Portal Access Count	Reports showing the number of portal accesses for an individual.

See also: [FTP Backup Settings](#)

[About Archive Files](#)

[Setting Up the Network Storage Location](#)

Access History Reports

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:

1. To return only requests from anyone with a particular last name, enter that name in the **Person** field.
2. To return only valid, invalid, or uncompleted requests, select **Valid accesses**, **Rejected accesses**, or **Access not completed**, respectively.
3. 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.
4. To return only requests received at a particular portal or elevator, select the portal or elevator name from the **At (portal name)** drop-down list.
5. To return no more than a certain number of requests, enter that number in the **Maximum Records** field.
6. 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)".

7. 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.
8. 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.

See also: [FTP Backup Settings](#)

[About Archive Files](#)

[Setting Up the Network Storage Location](#)

Alarm Resolution Reports

Select **Administration : Reports : History : Alarm Resolution**.

On this page you can create a report that tracks alarm duration. This is the period between the activation of an alarm and its resolution.

Alarms are individual activations of [events](#) defined in the system. For an alarm to be resolved, it must be acknowledged (if acknowledgement is required according to the associated event definition) and its underlying cause must be cleared.

The default Alarm Resolution report searches the security database and archive files and returns records for alarms activated in the active partition that have since been resolved, up to a maximum of 100,000 records. For an alarm to be included in the report results, its associated event must be configured to display alarms when activated.

Before running the report, you can set search parameters to limit the results to a particular period of time and to particular events. You can also limit the number of records the report will return.

To create an Alarm Resolution report:

1. To specify the reporting period, enter a **From** date and time and a **Through** date and time. Enter the times in 24-hour format; for example, enter 13:00 for 1 p.m.
Any alarm that was activated in the active partition within the reporting period and has since been resolved will be included in the report results. It is not necessary for the alarm resolution to have occurred during the reporting period.
2. To limit the results to alarms associated with specific events, select those events in the Available list and click the right-arrow button to move it to the Selected list.
To move multiple events at once, **SHIFT**-click to select contiguous events or **CTRL**-click to select non-contiguous events.
3. To change the number of records the report will return, enter a different number in the **Maximum Records** field. The default is 10,000 records.
4. Click **Run report**.
The results are displayed in HTML format in a separate window. The entry for each alarm includes the name of the associated event, the activation and deactivation times, and the duration in days and minutes.
5. To sort the data alphabetically by event name, click the Event column header. Click it multiple times to switch between an ascending and descending sort order.
6. 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.

See also: [Setting Up Events](#)

[Monitoring and Resolving Alarms in the Alarm Workflow Widget](#)

[Creating Alarm Workflow Policies](#)

Audit Trail Reports

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 generate an Audit Trail report:

1. Click the **From (date)** calendar icon and select a start date for the report.
2. 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.
3. (optional) On the **Changed by** drop-down list, select the name of the user whose changes you want to retrieve.
4. (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.
5. 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.
6. 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.
7. 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. For information on viewing the results, see [Viewing Audit Trail Report Results](#).
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 print the report results, click **Print** to display the Print dialog.

See also: [History Reports](#)

Viewing Audit Trail Report Results

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

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.
- **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.

The following example shows the row for a transaction in which a person record was updated.

DATE / TIME	USER	DATA	FIELD	ACTION	ORIGINAL VALUE	NEW VALUE
▶ 11/17/10 15:06:24	admin	person	firstname		Janet	<n/c>

Once you expand the row, you can see that there was an update to the **lastname** field: the person's last name was changed from Federer to Makris. The last line for the transaction tells you that the change was made in the Master partition.

DATE / TIME	USER	DATA	FIELD	ACTION	ORIGINAL VALUE	NEW VALUE
▼ 11/17/10 15:06:24	admin	person	firstname		Janet	<n/c>
11/17/10 15:06:24	admin	person	lastname	UPDATE	Federer	Makris
11/17/10 15:06:24	admin	person	partitionid		Master	<n/c>

See also: [History Reports](#)

Creating Custom History Reports

Select **Administration : Reports : History : Custom Report**.


On this page you can create, edit, and delete Custom History report definitions. After creating a report definition, you can run the report and view the results in HTML format. From the HTML viewer you will also have access to the results in PDF or CSV format.

Beginning with software Release 4.8, you can use a new Totals tab to configure totals for a report, as described at step 9 below.

To create a Custom History report definition:

1. If one or more Custom History reports are already defined in the system, click **New Report** at the top of the report list.
2. On the page that appears, enter a **Name** for the report.
3. (optional) Enter a **Title** to be displayed with the report results and a **Description** that explains the report's use.
4. (optional) In the **Limit** text box, specify the maximum number of records to be returned; or, if you plan to configure totals at step 9, specify the number of records to be used when computing the totals.

If you have configured totals for a report, the results will generally contain far fewer rows than the specified Limit. This is because each row will be a summary of some number of the records used to compute the totals.

5. On the **Columns** tab, set up the report output:
 - For 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 inches.
 - 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 you want to display as a column, then click the right-arrow button  to move it to the Selected list. Be sure to include the **Total** field if you plan to configure totals at step 9.

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 in 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 first day and last day for which activity should be reported. 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. By default, activity will be reported between 00:00 on the first day and 23:59 on the last day of the reporting period.

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.

- For **Days of the Week**, select the check box for each day of the week for which activity should be reported. If you want activity to be reported only during a specific period of time on these days, enter the starting time and ending time in the **Only between the hours (HH:MM)** text boxes, using the format HH:MM.

NOTE: If you enter an ending time that is earlier in the day than the starting time, activity will be reported between the starting time on each selected day and the ending time on the following day. For example, if you select the days Wednesday, Thursday, and Friday and specify an intra-day reporting period of 18:00 to 08:00, activity will be reported for the period between 6 p.m on Wednesday and 8 a.m. on Saturday.

7. On the **People Filter**, **Location**, and **Events** tabs, specify criteria to be used to narrow down the report results. For more information, see [Entering Filter Criteria](#) below.
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 or all 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.

NOTE: Run-time prompts are not applicable to scheduled reports.

9. To include totals in the report, make sure the **Total** field is selected on the **Columns** tab, and do the following on the **Totals** tab:

For **Totals**, specify the type of totals to be computed:

- Select **Compute totals for the set of columns selected**. The report will compute totals for the set of columns selected on the Columns tab.
- Select **Compute totals of unique <field> for the set of columns selected**, and replace <field> with one of the available data fields. The report will compute totals of unique instances of this field for the selected columns.

For **Period**, specify the time period for which totals will be computed:

- **Compute totals for the selected time period (start through end)**. The report will compute totals for the entire reporting period. Make sure the **Date/Time** field is NOT selected on the Columns tab to ensure meaningful results.

- **Compute daily totals for the selected time period (start through end).** The report will compute totals for each day of the reporting period. Make sure the **Date/Time** field is selected on the Columns tab.
- **Compute hourly totals for the selected time period (start through end)** The report will compute totals for each hour of the reporting period. Make sure the **Date/Time** field is selected on the Columns tab.

For more information, see [Tech Note 33: Configuring Totals for Custom History Reports](#).

10. To schedule the report, do the following on the **Schedule** tab:
 - Select the check box for each day of the week you want the report to run.
 - On the **Email Output Format** drop-down list that appears, select the output format (CSV or PDF) for report results that are sent via email.
 - 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. Click **Run report**.

The results are displayed in HTML format in a separate window. You can click any column header to sort the data on that column, and you click the header multiple times to switch between an ascending and descending sort order.

13. (optional) To display the results in a different format, click the PDF or CSV link at the top of the page. If you click the CSV link, you are prompted to either open or save the comma-separated values file.
14. To delete the report, click **Delete** on the Custom Report page and click **OK** to confirm the deletion.
15. 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 for each data field the operator the system will use to compare the value you specify with database values for that field. The choices are: **contains**, **is**, **is blank**, **is not blank**, **is greater than**, **is less than**, **is not**, **is one of**, **not in**, and **starts with**.
 - In the **Value** column, enter for each data field the value 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**.

2. Click **Save**.



The report results will be limited to activity related to 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, portal 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.

See also: [Creating Custom People Reports](#)

[About Archive Files](#)

[Managing Email Distribution Groups](#)

Duty Log Reports

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

With this page you can request a report showing duty log comments residing in the current security database, including archives. For each duty log comment included in the report results, you can view details about the comment itself and about the Activity Log entry to which it is appended. For more information, see [Viewing Duty Log Report Results](#).

To generate a Duty Log report:

1. Click the **From (date)** calendar icon and select a start date for the report.
2. 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.
3. (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.
4. 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 report results.
 5. 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.
 6. To print the report results, click **Print** to display the Print dialog.
 7. 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](#).
 8. To expand all rows, click **Expand all**.

See also: [History Reports](#)

Viewing Duty Log Report Results

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

When you define and run a [Duty Log report](#), the results are displayed in a table. The table includes a row for each Activity Log entry that has at least one duty log message matching your report criteria. The rows are sorted in descending order by date, with the most recent log entry appearing at the top of the report.

You can expand a row to view all of the duty log messages appended to a log entry:

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

For each duty log message listed in the report results, you can view the following information:

- **COMMENT DATE/TIME**: The date and time the message was entered.
- **OPERATOR**: The person who entered the message.
- **EVENT DATE/TIME**: The date and time of the logged event associated with the message.
- **EVENT/COMMENT**: The text of the Activity Log entry followed by the specific text of the duty log message. If a log entry has multiple duty log messages, the text of the Activity Log entry is displayed only for the first message.

See also: [Monitoring the Activity Log](#)

General Event History Reports

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. To return only activity logged during a specific period of time, enter 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.
2. To return only activity at a particular portal or elevator, select it from the **At (portal name)** or **At (elevator name)** drop-down list.
3. To return no more than a certain number of entries, enter that number in the **Limit to** text box.
4. 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.
5. 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.
6. In the **Columns** list, select the set 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 link you can click to view the video.
7. Click **Run report**. If you selected CSV output, you are prompted to open or save the CSV file.
If you selected HTML output, the report is displayed directly on this page. 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. 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.

See also: [FTP Backup Settings](#)

[About Archive Files](#)

[Setting the Network Storage Location](#)

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" then 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**.

See also: [Monitoring the Activity Log](#)

[Using the Monitoring Desktop](#)

People Reports

Select **Administration : Reports : People** and select the report you want.

Access Levels Report

Displays all access levels currently defined in the system. For each access level, the report includes its specified description, time spec, reader or reader group, floor group, and threat level group.

See also: [Creating Time Specs](#)

[Setting Up Access Levels](#)

[Assigning Access Levels](#)

[Creating Floor Groups](#)

[Setting Up Threat Level Groups](#)

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, the card number and card format, the location and date and time of the credential's last use, and the partition to which the cardholder's person record (and thus the credential) is assigned.

Before running the report, you can apply filters to limit the report results to:

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

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 active partition only.

See also: [Managing a Person's Credentials](#)

Current Users Report

Displays a list of logged-in users who are either from the active partition or who have been [granted user roles](#) in the active partition.

See also: [Creating a Security Management System User Account](#)

Custom Report

[Click here for information on creating Custom People reports.](#)

Occupancy Report

Displays a list of defined regions in the active partition. For each region, the report includes the number of people currently occupying the region, the maximum number of occupants allowed (if a maximum has been specified), the time of the last entry into the region, the name of the person who last entered, the time of the last exit from the region, and the name of the last person to exit. People outside a partition are counted as occupants of uncontrolled space.

See also: [Configuring Regional Anti-Passback](#)

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 active partition](#).

Click a 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

Displays all outstanding photo ID print requests and lists the following information for each request:

- ID
- Name
- Selected photo ID layout
- Person's activation date in the system
- 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. In the print photo ID window that appears, click **Print Photo ID**.

See also: [Printing Photo IDs](#)

[Uploading Photo ID Layouts](#)

Portal Access Report

Displays the names and access levels of people who have access to the portal you have selected from the **Portal** drop-down list. To filter the list, you can specify a user-defined field and a value for that field. For example, if field 1 is defined as **Department**, you can include only employees from the Finance department in the report by selecting **field 1** from the **Where** drop-down and then selecting **Finance** as the field's value.

Roll Call Report

Allows you to select a defined region from the **Region** drop-down list to display a list of people currently occupying that region. To refine the report results, you can select check boxes that appear below the drop-down list:

- When **<all>** is selected, you can select **Ignore Uncontrolled Space** to exclude anyone who is not in a defined region.
- When **Uncontrolled Space** is selected, you can select **Show people not in the above region** to include only people who are not in the Uncontrolled Space.
- When a defined region is selected, you can select **Show people not in the above region** to include only people who are not in that region, and/or **Ignore Uncontrolled Space** to exclude anyone who is not in a defined region.

Once an [evacuation plan](#) has been started, you can use the Roll Call report to review the progress of the evacuation. For **Region**, select any of the evacuation regions defined in the plan, then run the report. By periodically refreshing the report results, you can get an up-to-date view of the individuals remaining to be evacuated from that region.

See also: [Configuring Regional Anti-Passback](#)

Roster Report

If there are fewer than 1,000 people in the active partition, the report lists them all. If there are 1,000 or more people in the active partition, the report lists every person whose name begins with the first letter of the alphabet. For example, in English, the report shows every person whose last name begins with the letter A.

If the check box "Show persons from other partitions visible to this partition" is selected, the report also includes people who have been made [visible in the active partition](#).

The report provides the following information for each person:

- Name
- ID Photo (thumbnail)
- Expiration date
- Date the person's record was last modified
- The region the person is currently in, and a **Grace** button (see below)
- Access levels

- Card number and Format

Select a letter from the alphabet at the top of the page to limit the report results to people whose last names begin with the selected letter.

For system users holding at least an Administration user role, the **Region** column shows the region each individual is currently in, and provides **Grace** buttons that allow the system user to grace individuals against passback violations.

NOTE: A system user with only a Monitor user role can also grace users if both of the following settings are selected in the Web Site section of the [Network Controller page](#): **Show Passback Grace as Menu Option** and **Show Region and Passback Grace info in the Roster and People reports**.

See also: [Adding People to the System](#)

[Changing a Person's Access](#)

[Setting Up the Network Controller](#)

[Creating Custom User Roles](#)

[Configuring Regional Anti-Passback](#)

Creating Custom People Reports

Select **Administration : Reports : People : Custom Report**.

On this page you can create, edit, and delete Custom People report definitions. After creating a report definition, you can run the report and view the results in HTML format. From the HTML viewer you will also have access to the results in PDF or CSV format.

To create a Custom People report definition:

1. If one or more Custom People reports are already defined in the system, click **New Report** at the top of the report list.
2. On the page that appears, enter a **Name** for the report.
3. (optional) Enter a **Title** to be displayed with the report results and a **Description** that explains the report's use.
4. (optional) In the **Limit** text box, specify the maximum number of records to be returned.
5. On the **Columns** tab, set up the report output:
 - For 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). At either orientation, the left and right page margins will be 0.5 inches each.
 - 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 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 in 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.

NOTE: If the "Picture," data field is selected for a report, the HTML and PDF outputs will include each person's ID photo, scaled appropriately for display on the screen. The CSV output will include the image file name for each person's ID photo rather than the image itself.

6. On the **People Filter** and **Access Level** tabs, specify criteria to be used to narrow down the report results. For more information, see [Entering Filter Criteria](#) below.
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 or all 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.

NOTE: Run-time prompts are not applicable to scheduled reports.

9. On the **Schedule** tab:
 - Select the check box for each day of the week you want the report to run.
 - On the **Email Output Format** drop-down list that appears, select the output format (CSV or PDF) for report results that are sent via email.
 - 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.
10. Click **Save**.
11. Click **Run report**.

The results are displayed in HTML format in a separate window. You can click any column header to sort the data on that column, and you click the header multiple times to switch between an ascending and descending sort order.

12. (optional) To display the results in a different format, click the PDF or CSV link at the top of the page. If you click the CSV link, you are prompted to either open or save the comma-separated values file.
13. To delete the report, click **Delete** on the Custom Report page and click **OK** to confirm the deletion.

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 for each data field the operator the system will use to compare the value you specify with database values for that field. The choices are: **contains**, **is**, **is blank**, **is not blank**, **is greater than**, **is less than**, **is not**, **is one of**, **not in**, and **starts with**.
 - In the **Value** column, enter for each data field the value 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 and 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 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  to move it to the Selected list.
3. Click **Save**.

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

See also: [People Reports](#)

[Creating Custom History Reports](#)

[About Archive Files](#)

[Managing Email Distribution Groups](#)

Setting Up Automatic Email Distribution of Custom Reports

For any custom report definition that is scheduled to run automatically, you can select an email distribution list to which the reports will be sent.

To set up automatic email distribution of custom reports:

1. Set up an [email distribution group](#) to which you want the reports sent (*Administration : People : Manage Email Distribution Groups*).
2. Check the Contact tab in each recipients's [person record](#) (*Administration : People : Change/delete*) to make sure everyone in the email distribution group has a valid email address.
3. Create or edit a [Custom History](#) or [Custom People](#) report definition (*Administration : Reports : History/People : Custom Report*). On the Schedule tab, schedule automatic report runs and select your email distribution group.
4. Check to make sure an [email relay server](#) has been set up (*Setup : Network Resources : Email Settings*). This will allow the relay of messages sent from the controller.

Enabling Copy to Clipboard in the Mozilla Firefox Browser

The **Copy to clipboard** button allows you to copy report results to the Windows Clipboard. For you to use the button in the Mozilla Firefox browser, you must first enable it by manually editing an application setting, known as a preference.

CAUTION: Modifying preferences can, in rare instances, break Mozilla Firefox or cause strange behavior. Do so only if you are confident in your abilities.

To enable the Copy to clipboard button in the Mozilla Firefox browser:

1. Enter the following line into the browser address bar:

about:config

The list of preferences should open in the browser window.

2. Click within the active part of the preference list window and select **New > Boolean** from the context menu.
3. Paste the following preference name into the **New boolean value** window input box:
signed.applets.codebase_principal_support
4. Set the boolean value to **true**.

Keep in mind that preference names are case sensitive.

See also: [Audit Trail Reports](#)

Scheduling Actions

Select **Administration : Schedule Action**.

On this page you can create a scheduled action to:

- Lock or unlock a portal or portal group.
- Arm or disarm an input or input group.
- Activate or deactivate an output or output group.
- Enable free access or controlled access for an elevator floor or floor group.

NOTES: The portal group scheduled actions are not supported for Mercury portals. If a portal group contains Mercury portals, a scheduled a lock or unlock action on the group will have no effect on the Mercury portals.

The free access and controlled access actions are available only for elevators on standard nodes that are configured for Floor tracking or No floor tracking. They are not supported for elevators on Mercury panels.

The Schedule Action page presents a resource view and a calendar view:

The screenshot shows the 'Schedule Action' page. On the left is a resource view with a list of categories: Elevator Floor, Floor Group, Input, Input Group, Output, Output Group, Portal, and Portal Group. On the right is a calendar view for the week of Jan 24 - 30, 2016. The calendar has columns for each day and rows for times from 12am to 5am. The interface includes navigation buttons for 'Today', previous/next week, and view options for 'Month', 'Week', and 'Day'.

After selecting a resource or group in the resource view, you can schedule one or more actions.

NOTE: By default, the resource view and calendar view display the time zone of the controller. If your site is deployed across multiple time zones, see [Scheduling Actions Across Time Zones](#) for considerations when scheduling actions for resources in different time zones.

To select a resource or group:

1. In the resource view, click the right arrow next to a resource or group type.
2. Click **+**.
3. Select the resource or group you want from the menu that appears.

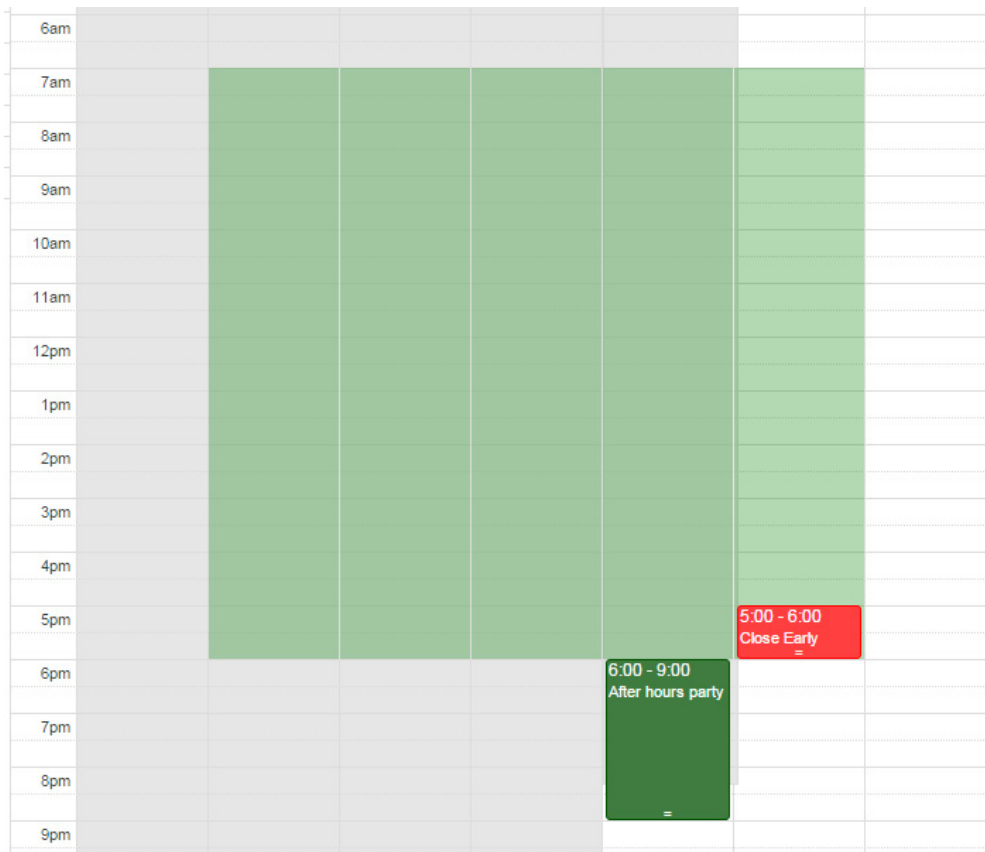
Your selection appears in the list of resources or groups of that type.

The calendar view changes to reflect periods when the resource or group is affected by:

- Group time specs. The active periods appear in light green and show the regular schedule for the resource or group based on the configured time specs. The inactive time appears in white.
- Scheduled actions. These periods appear in dark green, or in red to show overrides.


If an override is defined by a related resource or group, it will have a cross-hatched background, indicating that it cannot be edited. For example, when viewing a portal belonging to a group that has an override, you will see the override but will not be able to edit it.


Because you cannot schedule in the past, dates and times earlier than the current date and time are grayed out.



To schedule an action from the resource view:

1. Select the resource or group.

Click this button  for a resource to see which groups it belongs to, or for a group to see its members.

2. Click the **Add action to begin now** button: 

The current date and time is selected as the action's start time in the dialog box that appears.
3. Select the action you want to schedule.
4. Optionally, enter a **Description** for the action that explains its use.
5. Change the start date and time and/or end date and time as needed.
6. Click **OK**.

The new scheduled action appears in the calendar and is listed under the resource or group name in the resource view.

To schedule an action from the calendar view:

1. Select the resource or group in the resource view.
2. In the calendar view, click the position for the date and time you want the action to start.


That date and time is selected as the action's start time in the dialog box that appears.
2. Select the action you want to schedule.
3. Optionally, enter a **Description** for the action that explains its use.
4. Change the start date and time and/or end date and time as needed.
5. Click **OK**.

The new scheduled action appears in the calendar and is listed under the resource or group name in the resource view.

NOTES: 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 credential read.

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 edit a scheduled action:


1. Select the resource or group in the resource view.
2. Click the **Edit this action** button: 

- or -

Click the scheduled action in the calendar.

2. Make the desired changes in the dialog that appears and click **OK**.

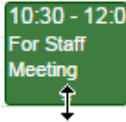
To show a scheduled action in the calendar:

1. Select the resource or group in the resource view.
2. Click the **Show this action in calendar** button: 

The calendar view changes to show the week for which the event is scheduled.

To move a scheduled action or extend its end date and time:

1. To move the scheduled action, drag it to a new position in the current month, week, or day.
2. To extend the scheduled action's end time, hover over its lower edge until a double-sided arrow appears:



2. Drag up to an earlier time or down to a later time in the current day or week.

In the Week calendar view, you can also drag right to extend the scheduled actions' end date.

See also: [Scheduling Actions for Resources in Multiple Time Zones](#)

[Setting Up Portals](#)

[Unlocking Portals](#)

[The Portal Status and Portal Unlock Widgets](#)

[Enabling and Configuring Remote Locksets](#)

[Managing Floor Access Using the Elevator Access Widget](#)

Scheduling Actions Across Time Zones

By default, the resource and calendar views on the [Schedule Action page](#) display dates and times in the controller's time zone. If any of the resources defined in your system are in different time zones than the controller, the user interface assists you in scheduling actions by:

- Displaying the time zone currently in use (on each resource and on the calendar).
- Switching to a resource's time zone and notifying you.
- Providing an option for switching between a resource's time zone and the controller's time zone.

NOTE: Groups containing resources with a combination of time zones are not supported and are not presented in the user interface.

To switch to a different time zone:

If one or more of the resources defined in your system is in a different time zone than the controller, a drop-down menu at the top of the calendar shows the time zone currently in use. To switch to a different time zone, select it from the menu.

When the controller's time zone is selected:


- The resource view shows dates and times in the controller's time zone.

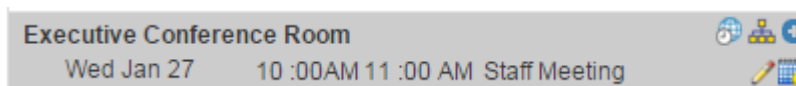
- The calendar view shows dates and times for the selected resource (including overrides) in the controller's time zone.

When a resource's time zone is selected:

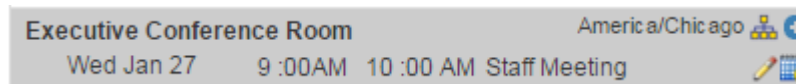
- The resource view shows the dates and times for each resource in its actual time zone.
- The calendar view shows dates and times for the selected resource in its actual time zone.

To identify a resource that is in a different time zone than the controller:


- When the controller's time zone is selected, this icon is shown to the right of the resource name , as in the following example:



- When the resource's time zone is selected, the resource's actual time zone is shown to the right of its name, as in the following example:



To identify a group whose members are in varying time zones:

- Regardless of which time zone is selected, this icon appears to the right of the group's name: 

In this case, the group can be viewed and edited only in the controller's time zone.

See also: [Scheduling Actions for Portals, Inputs, and Outputs](#)

[Setting Up Portals](#)

[Unlocking Portals](#)

[The Portal Status and Portal Unlock Widgets](#)

[Enabling and Configuring Remote Locksets](#)

[Managing Floor Access Using the Elevator Access Widget](#)

Setting Threat Levels

Select **Threat Level** from the [command palette](#).

If you have administrator access, you can use the Threat Levels dialog box that appears to set the threat level for all [locations](#) or selected locations in the active partition. Depending on your system's [threat level settings](#), 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 active partition
- The default location and all of its sub-locations
- An individual sub-location
- An individual sub-location and all of its sub-locations

NOTE: Whenever the default location for the active 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.



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

To set or change the threat level:

1. If a password is required for making threat level changes, enter it in the **Password** box.
2. Select the threat level you want to apply.
3. 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 active partition or to any of its sub-locations.
4. 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.

NOTE: Threat level changes might change the behavior of [access levels](#), [portals](#), [portal groups](#), and [events](#).

5. Click **OK**.

The threat level change is written into the [Activity Log](#).

NOTE: It is also possible to change threat levels using an [event action](#) or an API command.

See also: [Using Threat Levels to Change System Behavior](#)

[Creating Custom User Roles](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Setting Up Threat Level Groups](#)

[Threat Level Settings](#)

[The Threat Level Widget](#)

[Monitoring the Activity Log](#)

Utility Administration

Select **Administration : Utility** to display the following options.

Choose this	To see information on
Back Up System	Creating a copy of the security database.
Duty Log	Configuring preset duty log comments.
Photo ID Layout Upload	Uploading photo ID badge layouts for printing.
Photo ID Layout Delete	Deleting photo ID badge layouts from the controller.

See also: [Setting the Network Storage Location](#)

[FTP Backup Settings](#)

[About Archive Files](#)

Backing Up the System Data

Select **Configuration : System Maintenance : Backup System**.

- or -

Select **Administration : Utility : Backup System**.

With this page you can:

- Back up the security database to the network controller.
- Back up the security database to a network attached storage (NAS) if one is configured using [Setting Up the Network Storage Location](#) or [FTP Backup Settings](#).
- Download a backup of the security database to off-controller storage.

The system data is regularly backed up to the network controller each night at 00:15 hours. The Sunday backup is a full backup. The Monday through Saturday backups 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 off-controller system backups. Backups delivered to a configured FTP server or NAS drive will not be overwritten.

You can perform additional backups whenever you want.

NOTE: The system will also automatically create [archive files](#) of all data required for [General Event History reports](#), [Custom History reports](#), [Custom People reports](#) and [Audit Trail Reports](#). Each Sunday, after the full backup at 00:15 hours, the system checks the number of Activity Log records. If this number exceeds 150,000 then all records in excess of 100,000 are zipped into an archive file. This file is stored on the controller and on any configured NAS or FTP servers.

NOTE

To back up system data:

1. Enter a **Comment** to explain the purpose of this backup.
2. Click **Full Backup**.

3. Once 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.

To download a backup to off-controller storage:

1. In the **Existing Backups** table, click **get** for the backup you wish to save to off-controller storage.
2. In the **File Download** dialog, click **Save**.
3. In the **Save As** dialog, browse to the location where you wish to save this backup.
4. Click **Save**.

See also: [Restoring the System Data](#)

[Setting Up the Network Storage Location](#)

[FTP Backup Settings](#)

[About Archive Files](#)

[Setting Up the Network Controller](#)

[System Maintenance Utilities](#)

About Archive Files

The system automatically creates archive files of all data required for [General Event History Reports](#), [Custom History Reports](#), and [Custom People Reports](#).

Each Sunday, after the full backup at 00:15 hours, the system checks the number of Activity Log records. If this number exceeds 150,000 then all records in excess of 100,000 are zipped into an archive file. Only full days of data are included.

This file is stored on the controller and on any configured NAS or FTP servers.

The archive files are named:

arch_YYYYMMDD_YYYYMMDD.zip

where the first date is the oldest day of records, and the second date is the most recent day of records contained within the archive.

If the inclusive dates of your custom reports are weeks or months in the past, it is likely that some of the relevant data is in archive files. The report will still run correctly. The appropriate data will be retrieved from the archive files. This will take a few moments.

See also: [Backing Up the System Data](#)

Configuring Duty Log Messages

Select **Administration : Utility : Duty Log**.

On this page you can configure preset duty log messages, which administrators and monitors can select for inclusion in the [Activity Log](#).

To configure a preset duty log message:

1. In the **Name** text field, enter a short name for this message.
NOTE: If preset duty log messages already exist, click the **add** link under the **Name** field.
2. In the **Default duty log text** box, enter the text you want to appear in the Activity Log when an administrator or monitor selects this preset message from the [Duty Log Entry](#) page.
3. Click **Save**.

See also: [Adding Duty Log Messages to the Activity Log](#)

[Monitoring the Activity Log](#)

Deleting Photo ID Layouts

Select **Administration : Utility : Photo ID Layout Delete**.

- or -

Select **Configuration : Access Control : Utilities** and then click **Photo ID Layout Delete**.

On this page you can delete photo ID layouts that have been uploaded to the controller.

NOTE: This utility can also be reached by selecting **Setup : Access Control : Utilities**.

To delete a photo ID layout:

1. Select the **Delete?** check box next to each photo ID layout you want to delete.
2. Click **Delete File(s)**.

See also: [Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Batch Printing Photo ID](#)

[Photo ID Requests Report](#)

[System Data for Photo ID Layouts](#)

[Uploading Photo ID Layouts](#)

Uploading Photo ID Layouts

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

- or -

Select **Configuration : Access Control : Utilities : Photo ID Layout Upload**.

On 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](#).

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**.
NOTE: Photo ID layout files must end with the .dgn extension and can be no larger than 15 MB.
3. Click **Save**.

See also: [Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Batch Printing Photo IDs](#)

[Photo ID Requests Report](#)

[System Data for Photo ID Layouts](#)

System Data for Photo ID Layouts

Using EPI Designer, you can create your own custom photo ID badge layouts.

Selected data fields from the [basic personal Information section](#) of a person record can be used in the photo ID badge layout. The contents of those data fields will print on the badge when it is printed.

Data field names that may be used in the photo ID badge layout you create using EPI Designer are:

- First_Name
- Middle_Name
- Last_Name
- U_Field1 through U_Field20 (User-defined sections)
- Company_ID (ID#)
- User_Note
- Badge_Name (photo ID layout name)
- Start_Date
- End_Date
- cardid
- facilitycode

NOTE: User-defined fields 6 through 20 are supported only in V4.0 build 370 and above.

See also: [Uploading Photo ID Layouts](#)

[Photo ID Requests Report](#)

[Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Batch Printing Photo IDs](#)

[Configuring the Topaz Signature Pad to Create Signed Photo IDs \(PDF\)](#)

[Photo ID Badging Installation, Setup, and Operations Guide \(PDF\)](#)

Configuring the System

This section provides information on the following topics.

Access Control	Configuring resources that control building access.
Alarms	Configuring resources that identify and manage system alarms.
Cameras	Entering configuration information for cameras.
Evacuation Plans	Creating evacuation plans.
Floorplans	Composing and grouping floorplans.
Network Resources	Entering information about network resources that provide services for this system.
Site Settings	Identifying system hardware and user roles and permissions.
System Maintenance	Backing up system data and restoring backups, updating the software, managing storage, and using security database and security management system software utilities.
Threat Levels	Creating, setting, and editing threat levels and threat level groups.
Time	Specifying time-related settings.
Widget Desktops	Composing Widget Desktop layouts and configuring Camera View widgets.

See also: [Initial System Setup Checklist](#)

System Setup Checklist

When setting up your system, complete the steps below in the order given below. The list is ordered to ensure that prerequisite steps are completed first. Use the **Back** button to return here after each step is completed.

IMPORTANT: The first time you log into the system after configuring initial settings for the controller, as described in the [Initial Software Setup Guide \(PDF\)](#), be sure to change the default password for the administrator account (admin). Select Support/Utilities : [Change Password](#). Give the new password for the admin account to the network administrator or security director.

(1) Entering Site Settings:

- [Network Controller](#)
- Network Nodes

(2) Setting up Time Specs:

- [Holidays](#)
- [Time Specs](#)

(3) Setting up Alarms:

- [Outputs](#)
- [Output Groups](#)
- [Events](#)
- [Inputs](#)
- [Input Groups](#)
- [Alarm Panels](#)

(4) Setting up Access Control:

- [Card Formats](#)
- [Person Sections](#)
- [Readers](#)
- [Reader Groups](#)
- [Portals](#)
- [Portal Groups](#)
- [Elevators](#) and [Floors](#)
- [Floor Groups](#)
- [Access Levels](#)

(5) Setting up Cameras:

- [Types](#)
- [Definitions](#)
- [Menu Order](#)
- [Presets](#)
- [Views](#)
- [Video Management Systems](#)

(6) Setting up Floorplans:

- [Upload](#)
- [Compose](#)

(7) Setting up Network Resources:

- [Domain Name Server](#)
- [Email Settings](#)
- [Network Storage](#)
- [Time Server](#)

(8) System Maintenance:

- [Back Up Database](#)
- [Manage Storage](#)

See also: [Setup Page](#)

[Initial Software Setup Guide \(PDF\)](#)

[Network Node Hardware Installation Guide \(PDF\)](#)

The hardware installation guide for your system.

Access Control

Select **Configuration : Access Control** to display the following options.

Choose this	To see information on
Access Levels	Creating access levels that specify permitted readers and valid access times for the cardholders to whom they are assigned.
Card/Keypad Formats	Defining card/keypad formats for cardholder credentials.
Credential Attributes	Customizing attributes that can be defined for credentials, such as their Status settings.
Credential Profiles	Creating profiles that define the maximum number of days of non-use for each credential to which they are assigned.
Elevators	Configuring elevator access control by naming floors and then creating <i>elevator definitions</i> to secure floors, <i>floor groups</i> to define free-access periods and normal threat levels for secure floors, and <i>elevator groups</i> to allow users with custom user roles to monitor elevators and enable free access to their floor-select buttons.
Keypad Commands	Defining sets of keypad commands that can be entered at keypads to activate specific events.
Locations	Creating locations and assigning portals to them.
Person Records	Configuring the display of person records, including the tabs and user-defined fields (UDFs) that will appear in each record. Creating person record templates that provide a quick way to add people to the system.
Portals	Creating portal definitions that specify their readers, alarm outputs, locking mechanisms, door switch monitors (DSMs), and Request-to-Exit (REX) functions.
Portal Groups	Creating portal groups and assigning unlock time specs to their portals.
Readers/Keypads	Creating reader/keypad definitions that specify their nodes, expansion slots, and positions.
Reader Groups	Creating groups of reader/keypad devices that can be associated with access levels.
Regions	Setting up regions and configuring regional anti-passback.
Temporary Credential Policies	Creating a policy that will determine how the system handles temporary credentials.
Utilities	Decoding access cards, and uploading and deleting photo ID layouts.

See also: [Creating Time Specs](#)

[Setting Up Alarm Inputs](#)

[Setting Up Outputs](#)

[Configuring Keypads \(PDF\)](#)

[HID Dorado Magnetic Reader Setup \(PDF\)](#)

Setting Up Access Levels

Select **Configuration : Access Control : Access Levels**.

With this page you can set up access levels, which can then be [assigned to people](#). Up to 32 access levels can be assigned to each person in the system. Note that before you can complete the definition of access levels, you must create appropriate [time specs](#).

NOTE: Each S2 node is restricted to 512 access levels. Each Mercury panel is restricted to 32 access levels.

For each access level you can specify:

- Permitted [readers](#) and valid time specs.
- An [event](#) to be activated when the access level is used to gain access.
- Support for [Double Card Presentation mode](#).
- An [alarm panel](#) to be disarmed for cardholders holding the access level.
- [Elevator floor groups](#) to determine the floors to which cardholders holding the access level will be permitted access.
- [Threat level groups](#) to determine the threat levels under which the access level will be considered valid.
- An [escort type](#) that either requires holders of the access level to have an escort at permitted readers or allows them to serve as an escort at these readers. This feature is for use with Mercury panels only.

NOTE: The **Master Access Level** is a static, system-owned access level that uses the **All Readers** reader group and the **Always** time spec.

To create an access level:

1. Enter a descriptive **Name** for the access level, or click the **add** link and then enter the name.
2. Select the **Enabled** check box to the right of the **Name** field to enable the access level.
3. Optionally, enter a **Description** for the access level that explains its use.
4. For **Reader(s)**, select either the **Group** of readers or the **Individual** reader to which cardholders holding this access level will be permitted access.
5. For **Time Spec**, select the time spec or time spec group that will determine valid access times for cardholders with this access level.
6. From the **Disarm alarm panel** drop-down list, select any alarm panel that should be disarmed for cardholders holding this access level.

NOTE: The alarm panel will disarm only if the reader belongs to a [reader group specified for disarming](#) the alarm panel, and [the alarm panel is enabled for auto-arming](#).

7. Under Events, select the event to be activated when this access level is used to gain access.
8. Under Keypad Command Codes, select the **Enable Keypad Commands** check box to permit cardholders holding this access level to enter [keypad commands](#) to activate events.
9. Click **Save**.

(optional) To associate a floor group with an access level:

1. From the **Floor Group** drop-down list, select a floor group for access control of specific named floors. Be sure that the reader or reader group selected for the access level contains an elevator reader.
2. Click **Save**.

(optional) To associate a threat level group with an access level:

1. From the **Threat Level Group** drop-down list, select a threat level group to associate with this access level.

The access level will be considered valid only at readers whose locations are under threat levels included in the selected group. If a location's threat level is not a member of the selected threat level group, its readers will deny access to users with this access level.

2. Select **<not applicable>** if threat level changes should NOT affect the validity of this access level.

NOTE: The selected threat level group is applicable to standard-lock portals only. It is ignored at remote lockset portals.

3. Click **Save**.

CAUTION: If a person is assigned multiple access levels, the most permissive access level will determine whether access is granted or denied. For this reason, it might be necessary to either eliminate additional access levels in the person's record, or assign the threat level group to all of the person's access levels.

(optional, for use with Mercury panels only) To assign an escort type to an access level:

1. From the **Escort type** drop-down list, select one of the following:
 - **<not applicable>**: (default) A cardholder holding this access level will be granted access according to the rules defined by this access level. He will not require an escort and cannot serve as an escort for someone who requires one.
 - **Escort**: A cardholder holding this access level can enable access for one or more people requiring an escort. Once these people have presented their credentials at a permitted reader (within 15 seconds of each other), the cardholder must present his own credentials within 15 seconds.

For a cardholder to be able to escort multiple people at a time through a portal, the turnstile portal type must be enabled in the [portal definition](#).

- **Requires Escort**: A cardholder holding this access level will be granted access at a permitted reader ONLY if the next access request at the reader comes within 15 seconds, from a cardholder holding an Escort access level. Otherwise, access will be denied and the Activity Log will display a message with the reason code [NO ESCORT].

If you select Requires Escort, a cardholder holding this access level will require an escort for access at any of its permitted readers—even if the cardholder holds other access levels that do not require an escort at those readers.

2. Click **Save**.

IMPORTANT: Be sure that the permitted readers for this access level are not assigned to regions used for regional access control. Such a region's anti-passback features will conflict with the Escort type feature.

To change an access level:

1. From the **Name** drop-down list, select an existing access level.
The remaining fields on this page will fill in with the details of this access level.
2. Edit the fields that require changes.
3. Click **Save**.

See also: [Changing a Person's Access](#)

[Creating Time Specs](#)

[Setting Up Portal Groups](#)

[Setting Up Alarm Panels](#)

[Setting Up Events](#)

[Setting Up Reader Groups](#)

[Defining Elevators](#)

[Creating Floor Groups](#)

[Using Threat Levels to Change System Behavior](#)

Specifying Card/Keypad Formats

Select **Configuration : Access Control : Card/Keypad Formats**.

A set of [credential formats](#) is pre-loaded on every new system. Beginning with software release 4.6.01, each of these formats, and any format added to the system subsequently, is disabled by default.

NOTE: If the system data is restored from a database containing at least one user, all existing card formats will be enabled by default.

Before a user can select a card format when issuing a credential, the format must be enabled. This requires simply selecting the Enabled check box on this page when the card format is selected.

A card format that is not in use can be disabled by clearing the Enabled check box. A card format that is assigned to one or more credentials cannot be disabled.

Access control blades support card readers and keypads that use either Wiegand or Magnetic Stripe ABA Track 2 data formats. Instructions for creating both types of formats follow.

NOTE: Unlike standard nodes, which can have up to 32 card formats, each Mercury panel is restricted to 8 card formats.

Wiegand Formats

Several of the most common Wiegand formats are pre-loaded in the system and are available from the **Name** drop-down list. If you are using cards or keypads of a different format, you will need to know the values to use. Refer to the card manufacturer's documentation.

You may be able to decode the format using the [Card Decoder Utility](#).

[For help creating a Wiegand format click here.](#)

Magnetic Stripe ABA Track 2 Formats

Magnetic stripe cards are easily re-programmed and there are no standard magnetic stripe formats for access control. Therefore, you will need to create magnetic stripe Track 2 formats. You will have to know the specific track 2 format programmed onto your cards.

NOTE: The magnetic stripe readers must use the Wiegand signal level protocol in order for the data stream to be understood by the system. This Wiegand output is passed to the node and formatted according to the ABA Track 2 protocol.

[For help creating a magnetic stripe ABA Track 2 format click here.](#)

Binary-Coded Decimal (BCD) Formats

Binary-Coded Decimal (BCD) formats are user-defined credential formats that can be enabled, disabled, and modified. To define a format that works with the local system, you can include the fields that reflect your organization's use of facility code and encoded numbers.

When a BCD format is selected on the Card/Keypad Formats page, the fields that make up the facility code and encoded card number are displayed in units of BCD characters.

[For help creating a custom BCD format click here.](#)

To create a new Wiegand card/keypad format:

1. Click the **add** link under the **Name** drop-down list.

NOTE: If you are adding a card format that is substantially similar to an existing format, you can save time by selecting that format from the drop-down list, clicking the **clone** link, entering a new **Name**, and making any needed changes to the new format.
2. Enter a **Name** for the new card format. This is a required entry.
3. To enable the card format, select the **Enabled** check box.
4. Enter a **Description** for the card format.
5. From the **Data Format** drop-down list, select **Wiegand**.
6. In the **Length** text box, enter the number of bits in this card format. This is a required entry. The number entered here determines the number of bit definition drop-down lists provided below.
7. Check the card manufacturer's documentation for the facility code of the card batch you are using. Enter this number in the **Facility Code** text box.

NOTE: Make sure the facility code for keypads differs from the facility codes used in the card population. It is important that the system recognize keypad input as separate from card reads.

For instructions on setting keypad facility codes, refer to the keypad manufacturer's documentation.

8. Enter in the following four fields the correct start-bit and bit-length values for the format you are creating:
 - **Facility Code Start:** The first bit of the facility code number.
 - **Facility Code Length:** The number of bits used to indicate the facility code. For special applications, select the **Reverse bit order** check box to reverse the read order of the bits in the facility code portion of the card format.
 - **Encoded # Start:** The first bit of the card ID number.
 - **Encoded # Length:** The number of bits used to indicate the card ID number. For special applications, select the **Reverse bit order** check box to reverse the read order of the bits in the card ID portion of the card format.

NOTE: If you want your system to ignore the facility code when validating card reads, enter a zero (0) in each of the following fields: **Facility Code**, **Facility Code Start**, and **Facility Code Length**.
9. Select the **Hot Stamp and encoded numbers default identical** check box if the number printed on the card is the same as the encoded number. If this box is checked, whenever you enroll a card using a reader or manually enter a number in the **Hot Stamp #** field, the system populates both **Hot Stamp #** and **Encoded #** fields with the same value.
10. **Bit definitions in card format:** These drop-down lists will fill in automatically when you complete step 7 above. The number of bit drop-down lists will match the number you entered in the **Length** box at step 5.

P is for a parity bit. **F** is for a facility code bit. **N** is for a card number bit.
11. **Parity bit definitions:** These drop-down lists are filled in with the default parity bit definitions for the Wiegand format. The first bit (bit 1) is used for even parity error checking and covers bits 2 through 13. The last significant bit (bit 26) is used for odd parity error checking and covers bits 14 through 25.
12. To ensure that the new card format will be recognized by Mercury panels, select the **Mercury-supported** check box.
13. If the card format will be used with Mercury Casi F2F readers, select the **Casi F2F** check box. For more information, see [Special Requirements for Configuring Mercury M5 Bridge Panels](#).
14. Click **Save**.

To create a magnetic stripe ABA Track 2 format:

1. Click the **add** link under the **Name** drop-down list.

NOTE: If you are adding a card format that is substantially similar to an existing format, you can save time by selecting that format from the drop-down list, clicking the **clone** link, entering a new **Name**, and making any needed changes to the new format.
2. Enter a **Name** for the new card format. This is a required entry.
3. To enable the card format, select the **Enabled** check box.
4. Enter a **Description** for the card format.
5. From the **Data Format** drop-down list, select **Magstripe Track 2**.
6. In the **Length** text box, enter the number of **bytes** in this card format. This is a required entry. The number entered here determines the number of byte definition drop-down lists provided below.

7. Check the card manufacturer's documentation for the facility code of the card batch you are using. Enter this number in the **Facility Code** field.

NOTE: Make sure the facility code for keypads differs from the facility codes used in the card population. It is important that the system recognize keypad input as separate from card reads. For instructions on setting keypad facility codes, refer to the keypad manufacturer's documentation.
8. Enter in the following four fields the correct start byte and byte length values for the format you are creating:
 - **Facility Code Start:** The first byte of the facility code number.
 - **Facility Code Length:** The number of bytes used to indicate the facility code.
 - **Encoded # Start:** The first byte of the card ID number.
 - **Encoded # Length:** The number of bytes used to indicate the card ID number.

NOTE: If you want your system to ignore the facility code when validating card reads, enter a zero (0) in each of the following fields: **Facility Code**, **Facility Code Start**, and **Facility Code Length**.
9. Select the **Hot Stamp and encoded numbers default identical** check box if the number printed on the card is the same as the encoded number. If this box is checked, whenever you enroll a card using a reader or manually enter a number in the **Hot Stamp #** field, the system populates both **Hot Stamp #** and **Encoded #** fields with the same value.
10. To ensure that the new card format will be recognized by ASSA ABLOY remote locksets with magnetic stripe card readers, select the **Magnetic Stripe Remote Lockset supported** check box.
11. **Byte definitions in card format:** These drop-down lists will fill in automatically when you complete step 7 above. The number of byte drop-down lists will match the number you entered in the **Length** box at step 5.
 - **F** is for a facility code byte.
 - **N** is for a card number byte.
 - **?** is for an unmatched number.
 - **SS** is a Start Sentinel byte with the ASCII value ";".
 - **ES** is an End Sentinel byte with the ASCII value "?".
 - **LRC** is a checksum character.
12. Click **Save**.

To define a custom Binary-Coded Decimal (BCD) format:

1. Click the **add** link under the Name drop-down list.
2. Enter a **Name** for the new card format. This is a required entry.
3. To enable the card format, select the **Enabled** check box.
4. Enter a **Description** for the card format.
5. From the **Data Format** drop-down list, select **BCD**.
6. For special applications, select the **Reverse bit order** check box to reverse the order of the bits in each nibble. The bits read will be reversed on a nibble by nibble basis for the full length of the credential. For example, bits in the natural MSB (most-significant bit first) bit order will be reversed to the LSB (least significant bit first) bit order.

A **nibble** is a group of four binary digits (bits), or half a byte, which can be represented by a single digit.

7. In the **Length** text box, enter the number of nibbles in this card format.
8. Check the card manufacturer's documentation for the facility code of the card batch you are using. Enter this number in the **Facility Code** text box.
9. Enter in the following four fields the correct start-nibble and nibble-length values for the format you are creating:
 - **Facility Code Start**: The first nibble of the facility code number.
 - **Facility Code Length**: The number of nibbles used to indicate the facility code.
 - **Encoded # Start**: The first nibble of the card ID number.
 - **Encoded # Length**: The number of nibbles used to indicate the card ID number.
9. Select the **Hot Stamp and encoded numbers default identical** check box if the number printed on the card is the same as the encoded number. If this box is checked, whenever you enroll a card using a reader or manually enter a number in the Hot Stamp # field, the system populates both Hot Stamp # and Encoded # fields with the same value.
10. Click **Save**.

See also: [Handling Lost Cards](#)

[Changing a Person's Access](#)

[Decoding Cards](#)

[Credential Formats](#)

[Setting Up Readers and Keypads](#)

[Configuring Mercury Panels](#)

[About Remote Lockset User Types](#)

Customizing Credential Attributes

Select **Configuration : Access Control : Credential Attributes**.

One of the attributes that can be defined for a credential on the Access Control tab of a person record is the credential's status. On this page you can customize nine of the available credential status settings: Clear, Damaged, Forgotten, Lost, Not Returned, Not Validated, Returned, Stolen, and Suspended.

To customize a credential status setting, you can:

- Change its name and/or description.
- Enable or disable it.
- Specify that any credential to which it is applied will have the ability to grant access.

By default, none of the customizable status settings are set to grant access. For the system-defined status settings, only **Active** and **Temporary** are set to grant access.

To customize a credential status setting:

1. Select the name of the status setting from the **Name** drop-down list.
2. Select the **Enabled** check box if you want this status setting to be displayed as a choice when a user is setting a credential's status in a person record.
In a new system, all of these status settings are disabled by default.
3. To change the name of the status setting, click the **rename** link and enter the new name in the **Name** text box.
4. To change the description of the status setting, enter a new description in the **Description** text box.
5. (optional) Select the **Enables Credential** check box if you want credentials with this status setting to be able to grant access. This includes credentials to which the status setting is currently applied and those to which it is subsequently applied.
6. Click **Save**.

See also: [Managing a Person's Credentials](#)

[Credential Audit Report](#)

[Handling Lost Cards](#)

Creating Credential Profiles

Select **Configuration : Access Control : Credential Profiles**.

If **Enable credential profiles** is selected on the [Network Controller page](#), you can use this page to create, edit, and delete credential profiles. These profiles let you set expiration dates for individual credentials in the active partition.

Each credential profile defines a maximum number of days of non-use for each credential to which it is assigned. If the credential is not used within the specified number of days after the date it was issued, it is disabled and its status is set to "Not Used."

If **Disable credentials after failed accesses** is enabled, the credential profile can be configured so that the credential is disabled after a user-defined number of failed requests (**Failure limit**) to use the credential have been made within a user-defined **Time interval** and **Time unit**.

For example, if the **Failure limit**, **Time interval** and **Time unit** are set to the default values, the credential profile is disabled after three failed requests at using the credential within a 24-hour period.

If **Reset failed accesses counter on a valid access** is enabled, a threshold counter is reset to zero when a valid credential request occurs. The Threshold Counter begins to be incremented by one when the first credential failure occurs.

If **Reset failed accesses counter on a valid access** is not enabled, the credential profile remains disabled even when a valid credential access occurs.

A user-defined [event](#) may be configured to occur when a credential is disabled by the **Disable credentials after failed accesses** feature.

Once a credential profile has been assigned to credentials, subsequent changes made to the profile are applied to those credentials automatically.

To create a credential profile:

1. Enter a descriptive **Name** for the profile, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the profile that explains its use.
3. In the **Days until unused card expires** field, enter a maximum number of days of non-use.
Any credential to which this profile is assigned will be disabled if it is not used within the specified number of days after the date it was issued.
4. Select the **Disable credentials after failed accesses** check box to enable the feature. Select one or more of the following options:
 - Select a number between 1 and 10 (or accept the default of 3) from the **Failure limit** drop-down list to specify the number of failed credential requests before the credential is disabled.
 - Select a **Time interval** from the drop-down list or accept the default of 24 hours.
 - Select a **Time unit** (minutes, hours, or days) from the drop-down list or accept the default (hours).
 - Select the **Reset failed accesses counter on a valid access** check box to reset the threshold counter to zero when a valid credential access is completed.
 - Select an **Event** from the drop-down list (or accept the default of <none>) that will be activated when the failed credential thresholds have been met and the credential is disabled.
5. Click **Save**.

To edit or delete a credential profile:

1. Select an existing credential profile from the **Name** drop-down list.
2. To edit the profile, change the entries in the **Description** and/or **Days until unused card expires** fields.
3. To rename the profile, click the **rename** link and enter a new name.
4. Click **Save**.
5. To remove the profile from the system, click **Delete**.

See also: [Managing a Person's Credentials](#)

[Customizing Credential Attributes](#)

[Credential Audit Report](#)

[Handling Lost Cards](#)

Elevator Access Control

Overview of Elevator Access Control

By configuring elevator access control for a facility, you can:

- Secure a building's floors, making them accessible only upon valid credential reads.
- Define time periods when secure floors will be freely accessible under normal threat levels, and define threat levels under which access to the floors will always require a valid credential read.
- Give users roles that will allow them to use the [Elevator Status widget](#) to enable free-access and controlled-access for secure floors.

The procedures required to accomplish these tasks are outlined in the following table:

Task	Procedures
Securing a building's floors.	<ul style="list-style-type: none"> • Name the floors you want to secure. • Create elevator definitions. • Add each elevator's reader to an access level. • Assign the access level to cardholders.
Defining free-access periods and normal threat levels for secure floors.	<ul style="list-style-type: none"> • Add secure floors to a floor group. • Assign the floor group to the same access level as the elevator readers.
Giving users roles that will allow them to enable free-access and controlled-access for secure floors.	<ul style="list-style-type: none"> • Add elevators to an elevator group. • Include the elevator group in a user role. • Assign the user role to users.

See also: [Tech Note 34: Wiring Elevator Control](#)

Naming Floors to Be Managed By Elevator Access Control

Select **Configuration : Access Control : Elevators : Floors**.

Before you can use [elevator access control](#), you will need to create names for the floors in the security management system. Use this page to give floors descriptive names and to specify the way they will be ordered in drop-down lists.

To name a floor:

1. Click **New** and enter a descriptive name for a floor requiring access control.
2. Click **Apply** to add the floor to the list of named floors.
3. To re-order the list, select individual floors and click the **Move up** and **Move down** buttons to move them to different positions in the list.
4. Click **Save**.
5. To delete a floor, select it in the list and click **Delete**.

The named floors can now be included in elevator definitions and floor groups.

See also: [Overview of Elevator Access Control](#)

[Defining Elevators](#)

[Creating Floor Groups](#)

[Managing Floor Access Using the Elevator Status Widget](#)

Defining Elevators

Select **Configuration : Access Control : Elevators : Definitions**.

Elevator definitions are the key component of [elevator access control](#). They allow you to specify the readers, inputs, and outputs the system will use to control and monitor each elevator's floor-select buttons.

An elevator definition specifies:

- The node to which the elevator's reader, inputs, and outputs are wired.
- The reader that will control access to floors by enabling the corresponding floor-select buttons upon valid credential reads.
You will need to associate this reader (or a reader group containing it) with one or more access levels. The access levels can then be assigned to cardholders' person records to give them access to secure floors.
- Outputs that will enable or disable the corresponding floor-select buttons when activated by valid card reads, scheduled events, and Momentary Free Access actions.
- (optional) Inputs that will change state when the corresponding floor-select buttons are pushed, allowing the system to track floor selection.
- (optional) An input that will change state (and an event that will be activated) when the elevator's emergency call button is pushed.

Before creating an elevator definition, you will need to [name the building's floors](#). You will also need to set up the elevator's [reader](#), [inputs](#), [outputs](#), and emergency call [event](#) if they are not already configured in the system.

To create an elevator definition:

1. Enter a descriptive **Name** for the elevator, or click the **add** link and then enter the name.
2. For **Network Node**, select the node to which the elevator's reader, inputs, and outputs are wired.
3. For **Reader**, select the reader that will be used to control access to floors.
NOTE: A reader cannot be assigned to more than one function. Only readers that are not currently assigned elsewhere will appear in this list.
4. For **Integration Type**, select one of the following:
 - **No floor tracking**, if floor-selection tracking is not required. Mappings between named floors and the outputs corresponding to floor-select buttons are used to control access to those floors.

- **Floor tracking** or **Floor tracking (Intercept Style)**, if floor-selection tracking is required. Mappings between named floors and the outputs and inputs corresponding to floor-select buttons are used to control access to those floors and to track their selection.

NOTE: For floor tracking, Mercury panels support only *Intercept Style*. See [Tech Note 34: Wiring Elevator Control](#), for elevator integration details and wiring.

On standard nodes, access to elevators configured for *No floor tracking* or *Floor tracking* can be managed using the [Elevator Status widget](#).

5. For **Button Activation Time**, enter the number of seconds floor-select buttons will remain enabled once a valid credential is presented to the reader.

Valid values are from 1 to 60 seconds. For the *No floor tracking* integration type, the floor-select buttons will be disabled after this number of seconds. For either of the *Floor tracking* integration types, the floor-select buttons will be disabled after this number of seconds or after one of the buttons is pushed.

6. For **Button Pulse Time** (available only for the *Intercept Style* integration type), enter the duration, in seconds, of the pulse to the elevator control room to complete a floor selection. The default is one second.

Note that for elevators on Mercury panels, the button pulse time is limited to 14 seconds.

7. (optional) From the **Emergency Call** drop-down list, select the input corresponding to the elevator's emergency call button. From the **Event** drop-down list, select an event to be activated when this button is pushed and select the **Enabled** check box to enable it.
8. Map each floor to be managed by access control to the output (and optionally, to the input) corresponding to its floor-select button:

- From the **Floor** drop-down list, select each floor in turn.
- From the **Floor Enable (Output)** drop-down list, select the output corresponding to the floor-select button for that floor. This output will be activated by valid card reads, causing the button to become enabled.
- (optional) From the **Floor Selection (Input)** drop-down list, select the input corresponding to the floor-select button for that floor. This input will change state when the button is pushed, allowing the system to detect its status.
- Click **Apply** to add the floor to the Current Mappings list with its mapped output and optional mapped input.
- To create a new mapping, click **New**. To remove a mapping, click **Remove**.

Because all inputs and outputs for an elevator must reside on the same node, the number of floors you can map will depend on your node capacity. For standard nodes with one access control blade and six output blades, you can map up to 52 floors with the *No floor tracking* integration type (outputs only). With either of the *Floor tracking* integration types (outputs and inputs), you can map up to 28 floors (27 if you also configure an input for the emergency call button).

For Mercury panels, you can map up to 128 floors, regardless of the integration type.

NOTE: A particular input or output can be assigned to only one of the elevator's floors. Only inputs and outputs that are not currently assigned elsewhere will appear in the drop-down lists.

9. Click **Save**.

To edit or delete an elevator definition:

1. Select the elevator definition you want to edit from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this elevator definition.
2. You can change the settings for **Network Node**, **Reader**, **Emergency Call**, **Button Activation Time**, and **Button Pulse Time** settings.
3. If you change the **Integration Type**, any inputs from the floor-to-input mappings will be removed when you save your changes.
4. To remove a floor-input/output mapping, select it in the **Current Mappings** list and click **Remove**.
5. To change a floor-input/output mapping, select it in the **Current Mappings** list, select a different floor, input, or output and then click **Apply**.
6. To create a new floor-output mapping click **New** under the **Current Mappings** list, select a floor, output, and input and then click **Apply**.
7. Click **Save**.
8. To delete the elevator definition, click **Delete**.

NOTE: You can use [elevator floor groups](#) to define free access periods and normal threat levels for floors that are managed by access control.

See also: [Overview of Elevator Access Control](#)

[Naming Floors to Be Managed By Access Control](#)

[Creating Elevator Groups](#)

[Creating Floor Groups](#)

[Managing Floor Access Using the Elevator Status Widget](#)

[Setting Up Inputs](#)

[Setting Up Outputs](#)

Creating Elevator Floor Groups

Select **Configuration : Access Control : Elevators : Floor Groups**.

Floor groups let you define free-access periods for floors that are managed by [elevator access control](#). During a free-access period, and under normal threat levels, the floors will be freely accessible without valid credential reads. Once the free-access period ends, or the threat level changes to one defined as abnormal, the floors will return to their controlled-access state.

For example, a company might want to make the floor housing its cafeteria freely accessible to employees only at lunchtime. For the rest of the day, and at any time of the day during emergencies and other abnormal conditions, access to the floor would require a valid credential read.

Once you have created a floor group, you can create an [access level](#) for it and include the elevator's reader. Cardholders holding that access level will have access to the elevator's secure floors at all times, regardless of the current threat level.

To add a floor group to the system:

1. Enter a descriptive **Name** for the floor group, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the floor group that explains its use.
3. From the **Free-access Timespec** drop-down list, select a [time spec](#) or time spec group.
The floors in this floor group will be freely accessible during the times defined by the selected time spec or time spec group. For example, if you select a time spec covering the period between 8 AM and 5 PM Monday through Friday, the floors will be freely accessible during normal working hours on weekdays.
5. From the **Threat Level Group** drop-down list, select a threat level group.
The floors in this floor group will be freely accessible only when its Free-access Timespec is valid AND the current threat level is a member of the selected threat level group. At all other times, access to the floors will require a valid credential read.
6. For each floor you want to add to this group, select it in the Available list and click the right-arrow button to move it to the Selected list.
7. Click **Save**.
You can now associate the floor group with the same access level as an elevator's reader, ensuring that cardholders holding that access level will have access to the elevator's secure floors at all times.

To edit or delete a floor group:

1. Select an existing floor group from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this floor group.
2. Edit any part of the floor group definition.
3. Click **Save**.
4. To delete the floor group, click **Delete**.

See also: [Overview of Elevator Access Control](#)

[Naming Floors to Be Managed By Access Control](#)

[Defining Elevators](#)

[Managing Floor Access Using the Elevator Status Widget](#)

[Setting Up Access Levels](#)

[Setting Up Threat Level Groups](#)

[How Groups are Used in the System](#)

Creating Elevator Groups

Select **Configuration : Access Control : Elevators : Elevator Groups**.

Elevator groups have a single purpose: adding elevator permissions to [user roles](#). They are not required for the operation of [elevator access control](#).

When an elevator group is included in a user role, users with that role will be able to monitor the elevators in the group. They may also be able to use the [Elevator Status widget](#) to enable free access for the elevators' floor-select buttons.

To create an elevator group:

1. Enter a descriptive **Name** for the elevator group, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the elevator group that explains its use.
3. For each elevator you want to add to this group, select it in the Available list and click the right-arrow button to move it to the Selected list.
4. Click **Save**.

To edit or delete an elevator group:

1. Select an existing elevator group from the **Name** drop-down list.

The remaining fields on the page fill with the settings for this elevator group.

2. Edit any part of the elevator group definition.
3. Click **Save**.
4. To delete the elevator group, click **Delete**.

See also: [Overview of Elevator Access Control](#)

[Defining Elevators](#)

[Creating User Roles](#)

[Naming Floors to Be Managed By Access Control](#)

[Creating Floor Groups](#)

[Managing Floor Access Using the Elevator Status Widget](#)

[How Groups are Used in the System](#)

Configuring an Otis Elevator Compass Integration

Select **Configuration : Access Control : Elevators : Otis Compass Configuration**.

On this page you can do the following to configure an integration with the Otis Elevator Compass Destination Entry System:

- [View communication status information in the Compass system](#).
- [Enable, suspend, or end communication between the security management system and the Compass system](#).

- [Map named floors in the security management system to landings in the Compass system.](#)
- [Configure nodes in the Compass system.](#) These are Destination Entry Server (DES) nodes, Destination Entry Redirector (DER) nodes, and Destination Entry Computer (DEC) nodes.
- [Optionally, associate offline events with Compass nodes.](#) An offline event is activated when the associated node moves from an active/online state to a failed state, and is deactivated when the node returns to an operational state.

For more information, see the tech note [Otis Elevator Compass™ Integration Overview \(PDF\)](#).

NOTE: Floors and floor groups associated with the Compass system are configured using the standard [Floors](#) and [Floor groups](#) configuration pages. Status events associated with the Compass system are configured using the standard [Events](#) configuration page. Reader groups and access levels associated with the Compass system are configured using the standard [Reader Groups](#) and [Access Levels](#) configuration pages.

To view communication status information in the Compass system:

1. Select **Configuration : Access Control : Elevators : Otis Compass Configuration**.
2. In the Service Statistics table, review the status of the Network Controller.
3. In the Status Updates table, review status and other information for all DEC nodes.
4. In the Setup and Authorizations table, review all setup and authorizations sent to DEC nodes.

To enable, suspend, or end communication between the security management system and the Compass system:


1. Select **Configuration : Access Control : Elevators : Otis Compass Configuration**.
2. Select the **S2NC/Otis Compass Communication** check box at the top of the page.
3. Click **Save**.
4. To suspend or end communication, clear the check box and then click **Save**.

While the communication is suspended, the Compass system goes into a default mode determined by the configuration of the Compass system.

To map named floors to landings in the Compass system:

1. Select **Configuration : Access Control : Elevators : Otis Compass Configuration**.
2. Click the **Floor Map** tab.

In the table, floors are sorted in decreasing order by the value of the landing numbers. Floor names without landing numbers appear at the bottom of the list.





3. To associate a named floor to an elevator landing number for use in the Compass system, click this icon  in the right column, enter the landing number in the dialog box that appears, and then click **OK**.

A landing number can be any number from -127 to 127. It is the number the security management system sends to the Compass system to call and direct an elevator to the associated floor.

NOTE: Any floor with an assigned landing number can be selected as a user's default floor on the **Access Control** tab of the person detail page. Floors with no assigned landing numbers cannot be selected for this, or any other purpose, within the Compass system.


4. When you have finished, click **Save**.

To configure DES, DER, and DEC nodes of the Compass system:

1. Select **Configuration : Access Control : Elevators : Otis Compass Configuration**.
2. Click the **Configuration** tab.
3. In the first table, add a DES or DER node by clicking this button  and then entering its IP address, name, and type.
4. In the second table, add a DEC nodes by clicking this button  and then entering its IP address, name, and type.
5. To delete a node in either table, select it and click this button .
6. To modify a node in either table, select it and click this button , modify any of the information in the dialog box that appears, and then click **OK**.
7. When you have finished, click **Save**.

(optional) To associate offline events with nodes in the Compass system:

1. Select **Configuration : Access Control : Elevators : Otis Compass Configuration**.
2. Click the **Events** tab.

You can associate an offline event with any of the Compass nodes listed in the table. The event will be activated when the node moves from the active/online state to a failed state, and is deactivated when the node returns to an operational state.
3. Select a node and then click this icon  in the right column
4. In the dialog box that appears, select the offline event you want to associate with the selected node, and then click **OK**.
5. Repeat steps 2-4 for each node you want to configure.

You can configure as many or as few events as you like, depending on your site's monitoring and reporting needs.
6. Click **Save** when you have finished.

See also: [Changing a Person's Access](#)

[Setting Up Access Levels](#)

[Setting Up Reader Groups](#)

[Setting Up Events](#)

[Naming Secure Floors](#)

[Creating Floor Groups](#)

Defining Keypad Commands

Select **Configuration : Access Control : Keypad Commands**.

On this page you can define a set of keypad commands by associating one or more numeric codes with events defined in the system. The set can subsequently be assigned to a bit-burst keypad (or combination reader/bit-burst keypad device) to put it into command mode.

Once a keypad is in command mode, qualified cardholders can enter commands from the assigned set of keypad commands to activate the associated events. A qualified cardholder is someone holding an access level permitting both access to the keypad and the use of keypad commands.

To define a set of keypad commands:

1. For each keypad command you want to add to the set, do the following:
 - In the **Command Name** column, enter a descriptive name for the command.
 - In the **Code** column, enter a two-digit code number.

NOTE: The code numbers you enter need not be unique to this set of keypad commands. For example, you can use the code number "01" for an "Arm Area" command in this set and for an "Unlock Portal" command in another set.

 - In the **Event** column, select the event to be activated when the code number is entered at a keypad.
2. Click **Save**.

NOTES:

Keypad commands are supported only by bit-burst keypads that are connected to S2 nodes. They are not available for Mercury panels.

When a keypad that is in command mode is added to a portal definition, the portal's Keypad Timed Unlock feature will be disabled, but its Two Man Rule and Double Card Presentation features will remain enabled.

For a keypad in command mode, whether cardholders will be required to enter PINs before entering keypad commands depends on how the keypad is configured:

- If the keypad is configured as a stand-alone device that will not be used for access, PINs will not be required for entering keypad commands.
- If the keypad is configured as an access device for a portal, PINs will be required for entering keypad commands ONLY if they are required for entry and exit at the portal. This is because the PIN requirement for entering keypad commands is managed in the same way as the PIN requirement for portal access—that is, via the time spec assigned to the keypad in the portal definition.

See also: [Setting Up Readers and Keypads](#)

[Setting Up Access Levels](#)

[Setting Up Portals](#)

Setting Up Locations

Select **Configuration : Access Control : Locations**.

A location is an area whose threat level can be set independently and to which you can assign portals and online remote locksets. Each system starts with a single, default location.

Unless you create additional locations, all portals and locksets are assigned to this default location, and only system-wide threat level changes can affect their behavior. For information on assigning threat level groups to affect portal and lockset behavior, see [Using Threat Levels to Change System Behavior](#).

If you need greater flexibility when assigning threat level groups, you can create one or more locations. By creating locations within the default location, then additional locations within these locations, and so on, you can subdivide the system into a location hierarchy with the appropriate level of granularity.

Within this hierarchy, the threat level can be set independently for individual locations, or for individual locations and their sub-locations. Depending on how threat level groups are applied in such a system, a change in the threat level for a particular location can affect the behavior of all portals and locksets in that location, or in that location and all of its sub-locations.

NOTE: The threat level can be set manually using the [Set Threat Level](#) page or the [Threat Level widget](#), or automatically via the [Set Threat Level event action](#).

To add a location to the system:

1. Click the **add** link under the **Name** text box and enter a name for the new location.
2. Optionally, enter a **Description** for the location that explains its use.
3. Select the **Parent** location for the new location. The new location will be a sub-location of the parent location you select.
4. For each portal or lockset you want to assign to the new location, select it in the **Available** list and click the right-arrow icon to move it to the **Selected** list.

NOTE: A portal or lockset can be assigned to only one location at a time.

5. Click **Save**.

NOTE: For Mercury panels, portals can be assigned to the default location only, not to sub-locations. Support for sub-locations will be added in the future.

See also: [Setting Up Portals](#)

[Overview: Integrating Remote Locksets](#)

[Setting Threat Levels](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Setting Up Threat Level Groups](#)

[Using Threat Levels to Change System Behavior](#)

Person Record Setup

Configuring the Display of Person Records

Select **Configuration : Access Control : Person Records : Configuration**.

With this page you can configure the display of [person records](#) by:

- Hiding the Contact, Other Contact, and Vehicles tabs.
- Hiding or configuring the User-defined tab.

After changing options on this page, you will need to log out and then log in again to see the effects of your changes on new and existing person records.

NOTE: For information on defining lists of values that can be displayed as drop-down lists for fields on the User-defined tab, see [Defining UDF Value Lists](#).

To hide or show tabs in person records:

1. Clear any of the following check boxes: **Contact**, **Other Contact**, and **Vehicles** to hide the corresponding tab on person records—or select any of these check boxes to show the corresponding tab.
2. Click **Save**.

To hide or configure the User-defined tab in person records:

1. Clear the **Show?** check box to hide the User-defined tab on person records, or select the check box to show the tab.
2. To re-label the tab, enter a new label in the **Tab Label** text box.
3. To customize any of the 20 data fields that appear on the User-defined tab by default, do any or all of the following:
 - To re-label the field, enter a new label in the **Label** text box.
 - Select the **Enabled** check box to show the field, or clear the check box to hide the field.
 - Select the **Required** check box to require that data is entered in the field. A red asterisk (*) will appear next to the name of each field requiring an entry before the person record can be saved.

NOTE: If the Required check box is dimmed, click **Save** to save your current changes and enable the check box.

- Select the **Unique** check box to require that any data entered into the field is unique across all users for that field. A red dagger (†) will appear next to the name of each field requiring unique data.
- To adjust the horizontal size of the field, enter a new size in the **Field Size** text box. At the default size of 20, approximately 20 of the characters a user enters in the field will be visible in the field at one time. The actual number will vary depending on your browser settings.

NOTE: The Field Size setting has no effect on the number of characters users will be able to enter into the field.

- To require a specific type of entry in the field, select one of the following from the **Field Type** drop-down list: **Text**, **Numeric**, **Boolean**, or **List**.

An entry in a text field must be an alphanumeric value. An entry in a numeric field must be a positive integer. An entry in a boolean field must be a selected (true) or clear (false) check box. An entry in a list field must be a selected value on a drop-down list.

- If this is a list field, select the UDF value list you want to display as the drop-down list for this field. The available lists in the **List** column are defined on the [UDF Value Lists page](#).

4. Click **Save**.

See also: [Defining UDF Value Lists](#)

[Editing Person Records](#)

[Searching for Person Records](#)

Defining UDF Value Lists

Select **Configuration : Access Control : Person Records : UDF Value Lists**.

With this page you can define lists of values that can be displayed as drop-down lists for user-defined fields in person records.

To define a UDF value list:

1. Enter a descriptive **Name** for the list, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the list that explains its use.
3. In the **Items** text box, enter each of the values you want in the list. After each entry, press **ENTER** or click the right-arrow button to move the value into the new list.
4. To re-order the list, select individual list items and click the up-arrow and down-arrow buttons to move them to different positions in the list.
5. Click **Save**.

When configuring the display of person records, users will be able to specify the new list as the drop-down list for a user-defined field.

See also: [Configuring the Display of Person Records](#)

[Editing Person Records](#)

[Searching for Person Records](#)

Creating Person Record Templates

Select **Configuration : Access Control : Person Records : Templates**.

To provide users with a quick way to add people to the system, you can create person record templates. Each template defines values, such as a default set of access levels, that will be filled in automatically in any person record created from the template.

Once you create a person record template, it appears in a drop-down list of available templates at the top of the person record form. When adding a person to the system, a user can either select a template from the list or add the person without a template.

NOTES: Edits made to a person record template affect only person records created from that template subsequently. Person records created from the previous version of the template are not affected.

In a person record created from a template, the template name appears in the read-only Template field. Users can include this name in Custom People report definitions and in person search criteria.

To create a person record template:

1. Enter a descriptive **Name** for the template or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the template that explains its use.
3. On the Basic Info tab do either or both of the following:
 - Add one or more **Notes** that you want to appear in person records created from the template.
 - For **Expiration**, select the number of days or months after which person records created from the template should expire. Select **Never** if you don't want the person records to expire automatically.
4. On the Access Control tab, do any of the following:
 - Select one or more available **Access Levels** to be assigned to person records created from the template, and click the right arrow button to move them to the Selected list.
 - Select **Regional anti-passback privileges** (Exempt, Soft Always, or Hard Always) to be assigned to person records created from the template.
 - Select the **Exempt from credential non-use rules** check box to exempt anyone whose person record is created from the template from the system's "Disable credentials after "n" days of non-use" rule.
 - Select the **Trace this person** check box to trace the activity of anyone whose person record is created from the template.
 - For **Notify on expirations**, select an email distribution group to be notified if a person record created from the template (or any credential or access level included in the person record) is about to expire.
 - Select the **Use Extended Unlock** check box to give anyone whose person record is created from the template extra time (as defined by the system's "Use Extended Unlock" setting) to get through a portal.
5. On the User-defined tab, add values to any of the 20 user-defined fields to capture that data in person records created from the template.
6. Click **Save**.

The template is added to the list of available templates in the active partition.

To edit or delete a person record template:

1. Select an existing template from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this template.
2. Edit any part of the template definition.
3. Click **Save**.
4. To delete the template select it from the **Name** drop-down list and click **Delete**.
You cannot delete a template that is in use—that is, one that is associated with one or more person records.

See also: [Adding People to the System](#)

[Editing Person Records](#)

[Changing a Person's Access](#)

[Searching for Person Records](#)

[Configuring the Display of Person Records](#)

[Defining UDF Value Lists](#)

[Creating Custom People Reports](#)

Portal Setup

Setting Up Portals

Select **Configuration : Access Control : Portals**.

A portal is a door or any other access point. You can use this page to create, change, and delete portal definitions. A portal definition can include:

- [The unlock/request-to-exit \(REX\) behavior of the portal](#).
NOTE: To set an unlock time for a portal, include the portal in a [portal group](#) and select an Unlock Timespec for that portal group.
- [Card readers and keypads](#) at the portal.
- [A two-man access restriction](#), which ensures the portal can be unlocked only with valid card reads by two different cardholders within a specified period of time.
- [Support for Double Card Presentation mode](#). When this mode is enabled for a portal, a qualified cardholder can switch the portal to an unlocked or locked state and put it under manual control. This temporarily removes the portal from the automatic control of the portal group currently determining its automatic unlocking and relocking behavior.
- [Support for the keypad timed unlock feature](#). This feature allows cardholders to unlock a portal with a reader/keypad device and have the portal remain unlocked for a specified period of time.

NOTE: The keypad timed unlock feature requires the use of bit burst keypads. Buffered output keypads will not work with this feature.

- [Portal policies](#). This feature allows you to specify one or more policies defining threat level changes that will affect the portal's state.
- [The events behavior of the portal](#).

NOTE: Only one of the following features can be enabled for a portal at a time: Two Man Rule, Double Card Presentation, or Keypad Timed Unlock.

To create a portal:

1. Enter a descriptive **Name** for the portal, or click the **add** link and then enter the name.
NOTE: The **Name** drop-down list includes all portals currently defined in the system. When you select a portal, the page fills with the data that define that portal.
2. From the **Network Node** drop-down list, select the node to which the portal's inputs and outputs are wired.
3. From the **Location** drop-down list, select the [location](#) to which you want to assign the new portal.
4. Follow the procedures below to define the portal's access and alarm behavior.
5. Click **Save**.

To define the unlock/request-to-exit (REX) behavior of the portal:

1. From the **Lock** drop-down, select the output that controls the door lock, and enter the **Unlock** time in seconds.
NOTE: An output for a door lock cannot be assigned both to a portal and to another function. Only outputs that are not currently assigned elsewhere are listed in the **Lock** drop-down.
2. (optional) Under **Extended Time**, enter an **Unlock** time (in seconds) for the lock. You can also select a **Secondary Output** (such as an output for driving a door motor to automatically open the door), and you can specify a **Secondary Active Time** for the activation of the secondary output. The extended time and secondary output are for individuals requiring more time or assistance to enter a door.
NOTE: On the **Access Control** tab of the [person record](#), there is a **Use Extended Unlock** check box. When this check box selected on a person record, the Extended Time and Secondary Output will function whenever that cardholder's card is read.
3. From the **DSM** drop-down, select the input that monitors the door switch and will communicate to the node when the door is open. Enter a **Shunt** time (in seconds) for the DSM. The shunt timer begins when the DSM indicates the door is open. Alarm outputs are suppressed for the duration of the shunt time.
4. (optional) Under **Extended Time**, enter an extended **Shunt** time (in seconds) for the DSM. The extended time is for individuals requiring more time or assistance to enter a door.
NOTE: A DSM input cannot be assigned both to a portal and to another function. Only inputs that are not currently assigned elsewhere are listed in the **DSM** drop-down.
5. Select the **Relock on Open?** check box if you want the door to re-lock once it is open, rather than wait for the unlock timer to expire.
6. Select from the **REX** drop-down the input that notifies the node of a request-to-exit. For **REX mode**, select **Motion** if the REX is a motion sensor or **Push** if the REX is a manual switch such as a push button or a crash bar. When the REX is active, alarm outputs are suppressed until the shunt timer expires.

NOTE: A REX input cannot be assigned both to a portal and to another function. Only inputs that are not currently assigned elsewhere are listed in the **REX** drop-down.

7. Select the **Unlock on REX?** check box if the door is normally locked from the inside and must be unlocked to allow exit.
8. Select the **Unlock on REX when portal open?** check box if you want to door to unlock even if the door switch reports that it is currently open.

NOTE: For a portal associated with a Mercury panel, the **Unlock on REX when portal open?** option is selected by default and cannot be changed.

9. Click **Save**.

To specify the card readers and keypads at the portal:

1. From the **Reader 1** and **Reader 2** drop-down lists, select the entry and exit readers for this portal.

NOTES:

A reader cannot be assigned to more than one function. Only readers that are not currently assigned elsewhere are listed on the **Reader 1** and **Reader 2** drop-down lists.

Accept Read While Open: By selecting this check box, you can specify that readers must accept card reads even while the door is open or when an interior REX has fired. If this box is not selected, the reader will not accept any card reads until the DSM indicates that the door is closed or the REX shunt timer has expired.

For a portal associated with a Mercury panel, the **Accept Read While Open** option is selected by default and cannot be changed.

Allows access to Region: If you are using regional anti-passback, select from this drop-down the region to which this reader allows access.

2. From the **Keypad 1** and **Keypad 2** drop-down lists, select the keypad required for entry and exit at this portal. You can set the allowable time for PIN entry on the [Network Controller](#) page.

NOTES:

A keypad cannot be assigned to more than one function. Only keypads that are not currently assigned elsewhere are listed on the **Keypad 1** and **Keypad 2** drop-down lists.

PIN numbers for keypads must be either 4 or 6 digits and must be entered into the [person record](#) for each card holder. Therefore, when both a reader and keypad are required, the valid card read and the PIN must match.

For both keypads and the exit reader you can specify a **Time Spec** and a **Threat Level Group** by selecting them from the appropriate drop-down lists. Once a [time spec](#) and [threat level group](#) are selected, use of the keypad and/or outgoing reader will be required only during the hours of the selected time spec **and** when the system threat level is included in the selected threat level group.

WARNING: When an outgoing reader or outgoing keypad is enabled, the REX for that portal will not function. Such a portal may require an emergency manual REX to enable egress under dangerous conditions, such as a fire.

3. Click **Save**.

(optional, for use with Mercury panels only) To set the portal type:

1. To configure the portal as a turnstile, select the **Turnstile enabled** check box in the Portal Type section.
This will allow a user holding an [Escort access level](#) to escort multiple people at a time through the portal.
2. Click **Save**.

To specify a two-man access restriction for a portal:

This feature cannot be enabled if either Double Card Presentation or Keypad Timed Unlock is currently enabled for the portal, or if the portal definition includes a keypad that is in [command mode](#). It is not available for Mercury panels.

1. Under Two Man Rule, select the **Require two man access** button to require two valid credential reads for entry to the portal.
2. Select a **Time Spec** or time spec group (or keep the default, **Always**) and a **Threat Level Group** (or keep the default, **<not applicable>**).

The two-man access restriction will be in effect only during the period defined by the selected time spec or time spec group **and** when the current system threat level is included in the selected [threat level group](#). The number of seconds that can elapse between the two valid credential reads is determined by the *Two man entry timeout* setting on the [Network Controller page](#).

3. Click **Save**.

Whenever the two-man entry restriction is in effect for the portal, messages written to the Activity Log to record successful access attempts will look similar to the following:

14:43:29 Access granted for Ken Boswell [FIRST] at Suite Entrance

14:43:35 Access granted for Melissa Ziegler [SECOND] at Suite Entrance

If a second valid card read does not occur within the specified number of seconds, the access attempt is terminated and a message similar to the following is written to the Activity Log:

14:43:35 Access denied for Ken Boswell [No 2nd ACCESS] at Suite Entrance

To enable Double Card Presentation mode for a portal:

See [Enabling Double Card Presentation Mode for Portals](#).

To enable timed unlocks for a portal with one or more reader/keypad devices:

This feature cannot be enabled if either Two Man Rule or Double Card Presentation is currently enabled for the portal, or if the portal definition includes a keypad that is in [command mode](#).

1. Configure one or more reader/keypad devices for a portal, as described above.

NOTE: The keypad timed unlock feature requires the use of bit burst keypads. Buffered output keypads will not work with this feature.

2. Under Keypad Timed Unlock, select the **Enable keypad timed unlock** check box to allow cardholders to unlock the portal and specify the number of minutes it will remain unlocked.

When this check box is selected, any cardholder with valid access to the portal can present his or her card to any of the portal's reader/keypad devices when the portal is in a closed state. After entering the associated PIN, the cardholder can enter an unlock time in minutes (1-99). Single-digit numbers must either be preceded by a zero or followed by a number sign (#). For example, entering either **08** or **8#** after the PIN will unlock the portal for eight minutes.

Once the unlock time has been entered, the reader/keypad device issues a confirmation in the form of a long beep followed by a short beep, and the timer starts. The cardholder can now open the door and leave it open for the duration of the unlock time without activating a Portal Held alarm. A [TIMED UNLOCK] message appears in the Activity Log, indicating who initiated the timed unlock. If the portal is closed before the time limit has been exceeded, the timer ends and the portal relocks immediately.

If the portal remains open after the time limit has been exceeded, a Portal Held alarm is activated and a [TIMED UNLOCK EXCEEDED] message appears in the Activity Log. The reader/keypad device issues a warning in the form of a 30-second sequence of beeps. At the end of this sequence, the portal re-locks. If the portal is closed before this sequence is completed, the beep sequence stops and the portal relocks immediately.

3. Click **Save**.

To specify portal policies:

1. Under Portal Policies, select a threat level group for any of the following:

- **Scheduled actions apply only during these threat levels.**

Any [scheduled lock or unlock](#) defined for the portal will apply only when the system threat level is in the selected group.

- **UI lock/unlock override removed if threat level change is not in threat level group.**

If the portal has been switched to a locked or unlocked state via the [Lock Portal or Unlock Portal button](#), the override will end if the system threat level changes to one that is not in the selected group.

2. Click **Save**.

To define the events behavior of a portal:

1. (optional) For the first four alarm conditions described below, assign both a **Local to Node** system resource (an output) and a **System-wide event**. For the Duress or Double Card Presentation alarm conditions, assign a system-wide event.

Local to Node responses will not be logged in the security database. System-wide events will be logged in the security database.

The **Local to Node** output selected from the **Output** drop-down will activate for the duration indicated in the **Time** box. Valid values are 0 to 255 seconds. Note that if you enter a 0 (zero) here for either the **Forced** or **Held** condition, the alarm output will remain active until the alarm condition is cleared. If you enter a 0 (zero) for either the **Invalid** or **Valid** condition, the output will pulse for one second only, because the valid and invalid conditions clear immediately.

The **System-wide** event selected from the **Event** drop-down will execute and log an entry in the security database.

The five portal alarm conditions are:

- **Forced:** A portal has been forced open and there has been neither a card read nor a request-to-exit.
- **Held:** A portal has been held open past the expiration of the shunt timer.
- **Invalid:** A card has been presented to the reader and no valid entry for that card has been found in the database.
- **Valid:** A card with a valid status has been presented at a reader by a cardholder with a valid access level for that reader.
- **Duress:** A card has been presented to the reader, followed by an entry of the cardholder's [duress PIN](#) into the keypad.
- **Double Card Presentation:** For a portal with Double Card Presentation enabled, a [qualified user](#) has performed a double read to unlock the portal.

2. Click **Save**.

NOTE: The **In group(s)** list includes any portal groups that include this portal. You cannot delete a portal while it is part of a portal group.

See also: [Changing Portal Definitions](#)

[Configuring Regional Anti-Passback](#)

[Anti-Passback Applications \(PDF\)](#)

[Deleting Portals](#)

[Setting Up Portal Groups](#)

[Setting Up Readers and Keypads](#)

[Setting Up Reader Groups](#)

[Setting Up Events](#)

[Using Threat Levels to Change System Behavior](#)

Setting Up Portal Groups

Select **Configuration : Access Control : Portal Groups**.

To make one or more portals accessible during specific time periods, you can add them to a portal group. The way you set up the portal group will determine the automatic unlocking and re-locking behavior of all portals in the group.

NOTE: The default portal group, **All Portals**, is a system-owned group containing all portals currently configured in the system. When you add a portal to the system, it is added to the **All Portals** group automatically.

With this page you can:

- Create, edit, and delete portal groups.
- Assign an *unlock time spec* to a portal group to define its allowed access times. All portals in the group will be unlocked at the start of the period defined by the unlock time spec and re-locked at the end of that period.
- Optionally, assign a *First-in Unlock rule* to a portal group to specify that its portals should unlock for the time spec period only if a cardholder with a particular access level is present. If the group includes portals that have remote locksets, you will also need to assign an **unlock restriction** to the group.

To add a portal group to the system:

1. Enter a descriptive **Name** for the portal group, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the portal group that explains its use.
3. For **Unlock Timespec**, select a time spec or time spec group. The portals in this portal group will be locked at all times except during the period defined by this time spec or time spec group. If no appropriate time spec exists, create one on the [Time Specs](#) page.
For example, to ensure that employees can freely enter the workplace during business hours, you might assign an unlock time spec of 6 AM (06:00) to 8 PM (20:00) to a portal group containing the building's main entrances.
4. (optional) Select the **First-in Unlock rule** that should apply to all regular-lock portals in the group. (If the portal group includes remote-lockset portals, you must also complete step 5 below.)
5. If the group includes remote-lockset portals, select **on any valid access** from the **Remote locksets ignore Unlock Rule and will unlock** drop-down list. All remote-lockset portals in the group will unlock on the first valid card read occurring during the unlock time spec period and will relock at the end of that period.
6. (optional) Select the **Threat Level Group** you want to assign to all portals in the group. For any portal in the group, the unlock rule will have an effect only if the portal's location is under a threat level included in the assigned threat level group. If there are offline remote-lockset portals in the group, they will be unaffected by the **Threat Level Group** setting.
7. Select **<not applicable>** if threat level changes should NOT affect the portals' unlock and relock behavior.
8. For each portal you want to add to this group, select it in the **Available** list and click the right-arrow button to move it to the **Selected** list.
9. Click **Save**.

To edit a portal group:

1. Select an existing portal group from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this portal group.
2. Edit any part of the portal group definition.
3. Click **Save**.

To delete a portal group from the system:

1. Select an existing portal group from the **Name** drop-down list.
2. Click **Delete**.

See also: [Setting Up Portals](#)

[Using the First-in Unlock System Rule \(PDF\)](#)

[Creating Time Specs](#)

[Configuration Reports](#)

[Creating Custom User Roles](#)

[Setting Up Threat Level Groups](#)

[Threat Level Settings](#)

[Setting Threat Levels](#)

[Using Threat Levels to Change System Behavior](#)

[Enabling and Configuring Remote Locksets](#)

[How Groups are Used in the System](#)

Changing Portal Definitions

Select **Configuration : Access Control : Portals**.

To edit a portal definition:

1. Select the portal you want to edit from the **Name** drop-down list.
2. You can change the alarm output, shunt, and unlock time durations.
3. If you want to change input, output, or reader designations, be sure that the newly selected items are connected to appropriate devices for the selected portal.
4. Click the **Save** button at the bottom of the page. If you want to cancel this action, either select another portal or leave this page without clicking Save.

NOTE: After creating or modifying a portal definition, you should test the portal's behavior.

See also: [Setting Up Portals](#)

Deleting Portals

Select **Configuration : Access Control : Portals**.

To delete a portal:

1. Select an existing portal from the **Name** drop-down list.
NOTE: If the portal is part of one or more portal groups, these groups are listed next to **In group(s)** at the bottom of the page. Before you can delete the portal, you will need to remove it from these groups.
2. Click the **Delete** button at the bottom of the page.

See also: [Setting Up Portals](#)

[Setting Up Portal Groups](#)

Ways to Unlock Portals

In addition to presenting valid credentials at a portal, there are multiple ways to unlock it. You can:

- Add it to a [portal group](#) and assign an unlock time spec to the group.
Note: If you also apply a [First-in unlock rule](#) to the portal group, the portal will unlock only when the rule is satisfied AND the portal group's unlock time spec is valid.
- Momentarily unlock it via an [event action](#), or from the [Portal Status page](#), the [Widget Desktop](#), the [Monitoring Desktop](#), or [a floorplan](#).
- Schedule an extended unlock from [the Schedule Action page](#), the [Portal Status page](#), the [Widget Desktop](#), or the [Monitoring Desktop](#), or [a floorplan](#).
- [Switch it to a persistent unlocked state](#). This will remove it from the control of any [scheduled Lock action](#), [double card read](#), or portal group [time spec](#) currently in effect for the portal—and will suspend any [Lock Portal event action](#) defined for the portal.

Note: When setting portal group permissions for a [user role](#), you can grant holders of that role the following privileges individually: Momentary unlock, Extended lock/unlock, UI (persistent) lock/unlock, and Disable.

See also: [Setting Up Portals](#)

[Setting Up Portal Groups](#)

[Creating Time Specs](#)

[Using the Widget Desktop](#)

[Monitoring Floorplans](#)

Setting Up Double Card Presentation Mode

About Double Card Presentation Mode

Select **Configuration : Access Control : Portals**.

As you create or edit a portal definition, you can choose to enable *Double Card Presentation mode* for the portal. This will allow a qualified cardholder (someone with a valid access level for which this mode is also enabled) to switch the portal to an unlocked or locked state and put it under manual control. This temporarily removes the portal from the automatic control of the portal group currently determining its automatic unlocking and re-locking behavior.

For information on enabling Double Card Presentation mode, refer to:

- [Enabling Double Card Presentation Mode for Access Levels](#)
- [Enabling Double Card Presentation Mode for Portals](#)

About Double Reads

To put a portal under manual control, a qualified cardholder presents his or her credentials twice within a five second period. This is called a *double read*. If a keypad PIN entry is required at the portal, the PIN must be entered both times; however, the system will allow 15 seconds between the two reader/keypad entries.

A double read has the following effects:

If the portal is currently locked, the double read unlocks it and puts it into manual mode. The portal will remain in this state until:

- Another double read by a qualified user switches it to the locked state.
- The **Maximum Unlock Time** specified for the cardholder's access level expires, or the **Time Spec** selected for Double Card Presentation in the portal definition ends—whichever comes first.
- The portal's [location](#) changes to a threat level that is not a member of the threat level group selected for Double Card Presentation mode in the portal definition.
- The portal is locked manually from a monitoring station.

If the portal is currently unlocked, the double read locks it and puts it into manual mode. Cardholders (including the cardholder who performed the double read) can still present valid credentials to obtain entry. The portal remains in this state until:

- Another double read by a qualified cardholder switches it to the unlocked state.
- The **Time Spec** selected for Double Card Presentation mode in the portal definition ends.
- The portal's [location](#) changes to a threat level that is not a member of the threat level group selected for Double Card Presentation mode in the portal definition.
- The portal is unlocked manually from a monitoring station.

NOTE: If the reader beeper is connected, it will sound a long beep followed by a short beep when a double read has unlocked the portal. It will sound a short beep followed by a long beep when a double read has locked the portal.

See also: [Setting Up Portals](#)

[Setting Up Portal Groups](#)

[Creating Time Specs](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Using Threat Levels to Change System Behavior](#)

[Setting Up Events](#)

Enabling Double Card Presentation Mode for Access Levels

Select **Configuration : Access Control : Access Levels**.

As you set up or edit an access level, you can choose to enable *Double Card Presentation mode*. When this mode is enabled for an access level, cardholders with that access level can change a qualified portal to the unlocked or locked state and put it under manual control. This temporarily removes the portal from the automatic control of the portal group currently determining its automatic unlocking and re-locking behavior.

NOTE: A qualified portal is one for which Double Card Presentation mode is also enabled, and for which the time spec and threat level set for this mode are valid. For a double read to work at such a portal, the user must have access rights to the portal. For more information, see [Enabling Double Card Presentation Mode for Portals](#).

For a summary of how Double Card Presentation mode works, see [About Double Card Presentation Mode](#).

To enable Double Card Presentation mode for an access level:

1. Select an existing access level or [add a new one](#).
2. Under Double Card Presentation, select the **Enable Double Presentation Mode** check box.
3. For **Maximum Unlock Time**, enter the maximum number of hours and minutes a portal will remain unlocked after a double read. The maximum unlock timer will be reset at each unlock.

You can set any maximum unlock time between zero (0) minutes and 24 hours. If you set it to zero, the unlock time is unlimited.

4. Click **Save**.

Any user with this access level will now be able to use double reads to change a qualified portal to the unlocked or locked state and put it under manual control.

NOTE: Each double-read unlock or relock action is logged in the Activity Log and can be included in reports.

See also: [Setting Up Access Levels](#)

[Enabling Double Card Presentation Mode for Portals](#)

[Setting Up Portals](#)

[Setting Up Portal Groups](#)

[Changing a Person's Access](#)

Enabling Double Card Presentation Mode for Portals

Select **Configuration : Access Control : Portals**.

As you create or edit a portal definition, you can choose to enable *Double Card Presentation mode*. When this mode is enabled, and its time spec and threat level are valid, a qualified cardholder can change the portal to the unlocked or locked state and put it under manual control. This temporarily removes the portal from the automatic control of the portal group currently determining its automatic unlocking and relocking behavior.

For a summary of how Double Card Presentation mode works, see [About Double Card Presentation](#).

NOTE: A qualified cardholder is someone with a valid access level for which Double Card Presentation mode is enabled and who has access rights to the portal. For more information, see [Enabling Double Card Presentation Mode for Access Levels](#).

To enable Double Card Presentation Mode for a portal:

This feature cannot be enabled if either Two Man Rule or Keypad Timed Unlock is currently enabled for the portal, or if the portal definition includes a keypad that is in [command mode](#).

1. Select an existing portal or [add a new one](#).
2. Under Double Card Presentation, select the **Enable Double Card Presentation mode** button.
3. From the **Time Spec** drop-down list, select the time spec (or time spec group) that will govern when Double Card Presentation mode is valid for the portal. If a double read has put the portal into an unlocked state, it will be relocked immediately when this time spec expires.
Note that if the cardholder's access level expires while the portal is in an unlocked state, the portal will remain in that state until the time spec expires.
5. (optional) On the **Threat Level Group** drop-down list, select the threat level group that will govern the availability of this feature.

If a double read by a qualified user puts the portal into an unlocked state, it will be relocked immediately if the threat level for the portal's [location](#) changes to one that is not a member of this threat level group. For more information, see [Using Threat Levels to Change System Behavior](#).

Once you click **Save**, any user who has a valid access level for which Double Card Presentation mode is enabled, and who has access rights to the portal, will be able to use double reads to change it to the unlocked or locked state and put it into manual mode.

6. **NOTE:** Each double-read unlock or relock action is logged in the Activity Log and can be included in reports.

See also: [Setting Up Portals](#)

[Enabling Double Card Presentation Mode for Access Levels](#)

[Setting Up Portal Groups](#)

[Creating Time Specs](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Using Threat Levels to Change System Behavior](#)

[Setting Up Events](#)

Reader/Keypad Setup

Setting Up Readers and Keypads

Select **Configuration : Access Control : Readers/Keypads**.

On this page you can:

- Add readers and keypads to the system.
- Associate a camera with a reader or keypad.
- Assign a reader to a region for anti-passback control.
- Set the Facility Code Mode for a Mercury reader/keypad.
- Set an Allegion AD-400 Lockset Mode for a Schlage AD-400 wireless lockset.
- Put a keypad into [command mode](#).
- Edit and delete readers and keypads.

NOTE: You cannot delete a reader or keypad that is in use anywhere in the system. The **Used By** list that appears on this page will indicate all of the resources that currently use a reader or keypad. Readers and keypads can be used by reader groups, portals, access levels, and elevators.

Before you can complete the definitions of [reader groups](#), [access levels](#), or [portals](#) you must configure the individual readers and keypads.

Special Notes on Keypads: The system can support any keypad, or combination reader/keypad device that outputs Wiegand formatted data. A keypad entry is converted into a 16 bit number, which is placed into Wiegand formatted data with a facility code and parity bits.

Bit-burst keypads are also supported.

Keypad facility codes must differ from facility codes used in the card population. Nodes use the facility code to recognize the difference between card reads and keypad PIN entries. (Facility codes on most keypad devices can be set.) Be sure to enter the keypad format and facility code using the [Card/Keypad Formats page](#).

PIN numbers for keypads may be 4 or 6 digits long and must be entered into the [person record](#) for each cardholder. When both a reader and keypad are required, the valid card read and the PIN must match both the card number and PIN entered in the person record.

To add a reader/keypad to the system:

1. Enter a descriptive **Name** for the reader/keypad, or click the **add** link and then enter the name.
2. Select the **Enabled** checkbox to the right of the **Name** field.

3. Optionally, enter a **Description** for the reader/keypad that explains its use.
4. From the **Network Node** drop-down list, select the node to which the reader/keypad is wired.
5. From the **Expansion Slot** drop-down list, select the [slot number](#) of the board to which the reader/keypad is connected.
6. From the **Position** drop-down list, select the connector [position number](#) to which the reader/keypad is connected.
7. From the **Reader/Keypad Type** drop-down list, select the reader, keypad, or combination reader/keypad device type. If you select a keypad or combination reader/keypad device type, select the card/keypad format or bit-burst keypad model from the drop-down list that appears.

NOTE: If you select a Casi F2F "Supervised (Inputs)" type, be sure that the inputs are configured on the portal. Otherwise, the presentation of a valid Casi F2F card at the reader/keypad will always result in an "Access not completed" message in the Activity Log.
8. (optional) If you are configuring the reader for a Schlage PIM400-1501, select and enable a **Tamper Event** to be activated when tampering is detected at the PIM or at a connected wireless device; and/or a **Low Battery Event** to be activated when a low battery condition is detected at a connected wireless device.
9. (optional) To associate a camera with the reader/keypad, select the camera name from the **Camera** drop-down list. This setting is for use with NetVR. Once a camera is associated with a reader/keypad, users will be able to click access events in the Forensic Desktop Activity Log to see video associated with these events.
10. If you are using [regional anti-passback](#), select the region where this reader/keypad resides from the **Reader is in region** drop-down list.
11. If you are configuring the reader/keypad for a Mercury panel, select a **Facility Code Mode**. The mode you select will determine the conditions under which the reader/keypad will grant access based solely on a match of a credential's facility code (rather than on a match of both the facility code and the encoded credential numbers):
 - **None** (the default): The facility code is treated as part of the overall encoded credential number. A card matching only the facility code will not be granted access.
 - **Configuration:** Facility-code only checking is turned on only while the complete set of credentials is being downloaded to the Mercury panel. Once the credential download is complete, the behavior is the same as for the None setting.
 - **Offline:** Facility-code only checking is turned on only when the SIO is disconnected from its Mercury panel (via the RS-485 link). When the SIO is connected to the panel, the behavior is the same as for the None setting.
 - **Configuration and Offline:** Facility-code only checking is turned on both during the credential download and when the SIO is disconnected from its Mercury panel. At all other times, the behavior is the same as for the None setting.
 - **Permanent:** Facility-code only checking is turned on at all times.

NOTE: For information on applying a Facility Code Mode to multiple readers/keypads at once, see [Bulk Changing the Facility Code Mode for Mercury Readers/Keypads](#).
12. (optional) If you are configuring a Schlage AD-400 wireless lockset, select an **AD-400 Lockset Mode**. The available modes are None, Office, Privacy, and Apartment.

You cannot set an Allegion AD-400 Lockset Mode other than None for a lockset whose associated portal: (1) has an unlock time spec other than Never, (2) is in [Double Card](#)

[Presentation Mode](#), (3) has been switched to an [unlocked or locked state](#), or (4) has a [scheduled unlock/lock action](#) or an [unlock/lock event action](#) defined.

12. (optional) From the **Keypad Commands** drop-down list, select the set of [keypad commands](#) you want to assign to this keypad or reader/keypad device to put it into [command mode](#).
13. Click **Save**.

To edit or delete a reader or keypad:

1. Select an existing reader or keypad from the **Name** drop-down list.
2. Edit any part of the reader or keypad definition.
3. Click **Save**.
4. To delete the reader or keypad, click **Delete**.

If the reader or keypad is not currently used by any reader group, portal, access level, or elevator, it will be removed from the system.

See also: [Specifying Card/Keypad Formats](#)

[About Keypad Command Mode](#)

[Defining Keypad Commands](#)

[Bulk Changing the Facility Code Mode for Mercury Readers/Keypads](#)

[Bulk Changing the Allegion AD-400 Lockset Mode](#)

[Special Considerations for Configuring Schlage Wireless Devices](#)

[Setting Up Portals](#)

[Setting Up Reader Groups](#)

[Slot and Position Numbers](#)

[Configuring Regional Anti-Passback](#)

[Creating Anti-Passback Applications \(PDF\)](#)

[HID Dorado Magnetic Reader Setup \(PDF\)](#)

[Configuring Keypads \(PDF\)](#)

About Keypad Command Mode

Keypad command mode is a state into which you can put a bit-burst keypad by assigning it a set of [keypad commands](#). When a keypad is in command mode, any cardholder whose access level permits the use of keypad commands at that keypad can enter commands from the assigned set (after presenting valid credentials) to activate [events](#) defined in the system.

If the bit-burst keypad is part of a combination reader/keypad device and the reader is attached to a portal, the keypad must also be included in the portal definition for keypad commands to work. If the keypad is assigned the time spec **Never**, PINs will not be required for entering keypad commands (or for

accessing the portal). However, cardholders will need to present their credentials at the reader before entering keypad commands.

When a keypad that is in command mode is added to a portal definition, the portal's Keypad Timed Unlock feature will be disabled, but its Two Man Rule and Double Card Presentation features will remain enabled.

See also: [Setting Up Readers and Keypads](#)

[Setting Up Portals](#)

[Defining Keypad Command Codes](#)

Setting Up Reader Groups

Select **Configuration : Access Control : Reader Groups**.

On this page you can create, edit, and delete reader groups. These groups can be assigned to:

- [Access levels](#) to specify cardholders' permitted readers.
- [Alarm panels](#) to automatically disarm them upon valid credential reads.

NOTE: The default reader group, **All Readers**, is a system-owned group containing all readers currently configured in the system. When you add a reader to the system, it is added to the **All Readers** group automatically.

To add a reader group to the system:

1. Enter a descriptive **Name** for the reader group, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the group that explains its use.
3. For each reader you want to add to this group, select it in the **Available** list and click the right-arrow button to move it to the **Selected** list.
4. Click **Save**.

To edit or delete a reader group:

1. Select an existing reader group from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this reader group.
2. Edit any part of the reader group definition.
3. Click **Save**.
4. To delete the reader group, select it from the **Name** drop-down list and click **Delete**.

See also: [Setting Up Readers and Keypads](#)

[Setting Up Access Levels](#)

[Setting Up Alarm Panel Auto-arm Behavior](#)

[Arming and Disarming Alarm Panels](#)

[Bulk Changing the Facility Code Mode for Mercury Readers/Keypads](#)

[How Groups are Used in the System](#)

Configuring Regional Anti-Passback

Select **Configuration : Access Control : Regions**.

With this page you can:

- Create, change and delete regions used for regional access control.
- Specify system responses to passback, tailgate, and occupancy violations.
- Specify a region to be used only for mustering.

NOTE: Before you can complete the **Regions** page, you must [set up the events](#) you want the system to use in response to passback, tailgate, and occupancy violations.

To set up a region:

1. Click the **add** link under **Name** and enter the name of the new region.
2. If the region is to be used only for mustering, select the check box to the right of the **Name** drop-down.
3. Select a region from the **Parent region** drop-down list.
4. In the **Passback Violations** and **Tailgate Violations** sections, select the default actions the system will take when passback and tailgate violations occur.

Select **Ignore** to have the system ignore violations. Select **Hard** to have the system deny access in the case of a violation. Select **Soft** to have the system log the event but allow access in the case of a violation.

A *tailgate violation* occurs when a cardholder's credentials are read in a region where that person is known NOT to be. For example, once a cardholder has presented an access card to exit a protected region, he or she is known to be outside that region. A subsequent read of the same card at any reader within the protected region will be considered a tailgate violation, if it occurs within the number of seconds specified in the **Misc. Information** section.

A *passback violation* occurs when a cardholder's credentials are read for entry into a region where that person is known to be. For example, once a cardholder has presented an access card to enter a protected region, he or she is known to be inside that region. A subsequent read of the same card to enter the protected region will be considered a passback violation, if it occurs within the number of seconds specified in the **Misc. Information** section.

5. In the **Passback violations**, **Tailgate violations**, and **Occupancy limit enforcement** sections, specify the events you want the system to execute in case of violations.

When a violation occurs, the violation behaviors specified for the region to which access is being attempted will be executed. In a case where the reader is not part of a portal, and therefore may not allow access to a region, the violation behaviors specified for the region where the reader is located will be executed.

NOTE: Because Mercury panels do not distinguish between passback violations and tailgate violations, the behaviors specified in the **Passback violations** section are executed for both

passback violations and tailgate violations. The settings in the **Tailgate violations** section are ignored.

6. In the **Occupancy limit enforcement** section, you can enter a **Maximum occupancy**, and then select from the drop-downs the events you want the system to execute when the occupancy limit is reached and when the region is empty.
7. In the **Misc. Information** section, you can enter the number of seconds within which multiple reads of the same card will be considered a tailgate or passback violation.
8. Click **Save**.

Additional anti-passback setup:

1. Select **Configuration : Access Control : Readers/Keypads** and assign readers to regions.
2. For any two-reader portal, select **Configuration : Access Control : Portals**, select the portal, and for each reader, select the region to which the reader allows access.
3. You can specify a person's regional anti-passback privileges in the **Access Control** tab of the **Personal Information** page. Select **Administration : People : Change/delete**, and then search for a specific person.

NOTE: These anti-passback privileges will take precedence over the tailgate violation and passback violation behaviors specified on the **Regions** page.

4. (optional) To give system monitors the ability to grant passback grace, select both of the following options on the [Network Controller page](#): **Show Passback Grace as Menu Option** and **Show Region and Passback Grace info in the Roster and People reports**.

NOTE: When an individual is "graced" that person's next card read will be allowed, no violations will be triggered, and the person will be moved to the region specified by the **Auto-passback Grace to Region** setting on the Network Controller page. Thereafter, all anti-passback rules will be in effect, as before.

5. (optional) To specify that **Roster Reports** will include region information, select **Show Region and Passback Grace info in the Roster and People Reports** on the [Network Controller page](#).

See also: [Setting Up Readers and Keypads](#)

[Creating Anti-Passback Applications \(PDF\)](#)

[Setting Up Portals](#)

[Setting Up Events](#)

[Changing a Person's Access](#)

[Setting up the Network Controller](#)

[System Monitors and Passback Grace](#)

[Roster Reports](#)

Creating a Temporary Credential Policy

Select **Configuration : Access Control : Temporary Credential Policies**.

You can use this page to define a policy that determines how the system handles temporary credentials. Such a policy specifies:

- The expiration period for temporary credentials.
- Whether administrators can extend the expiration period for individual temporary credentials.
- An event to be activated when a temporary credential is used to request access.
- Whether a person's missing credentials will become disabled automatically when he or she is issued a temporary credential.
- Whether a read is required to reactivate a missing credential.

To create a temporary credential policy:

1. Optionally, enter a **Description** for the policy that explains its use.
2. For **Days until temporary credentials expire**, enter the number of days temporary credentials should remain active once they are issued.
3. Select the **Allow expiration extension** check box to allow administrators to extend the expiration period for individual credentials.
4. If you want a specific event to be activated each time a temporary credential is used to request access, select it from the **Temporary credential usage event** drop-down list. Select the **Temporary credential usage event enabled** check box to enable the event.
5. Select the **Disable missing credentials** check box to have the system automatically disable a person's missing credentials when he or she is issued a temporary credential.
6. Select the **Missing credentials must be read for reactivation** check box to specify that a read is required to reactivate missing credentials when they become available.
7. Click **Save**.

See also: [Managing a Person's Credentials](#)

[Handling Missing Credentials](#)

[Customizing Credential Attributes](#)

[Credential Audit Report](#)

[Handling Lost Cards](#)

Access Control Utilities

Select **Configuration : Access Control : Utilities** to display the following options:

Choose this

To see information on

[Card Decoder](#)

Obtaining raw card information to help identify an unknown card.

Photo ID Layout Delete	Reviewing and selecting photo ID layouts for deleting.
Photo ID Layout Upload	Uploading photo ID layouts for creating and printing badges.
Facility Code Mode	Performing a bulk change of the Facility Code Mode setting for Mercury reader/keypads
Allegion AD-400 Lockset Mode	Performing a bulk change of the Allegion AD-400 Lockset Mode setting for Schlage AD-400 wireless locks.

See also: [Specifying Card/Keypad Formats](#)

[Changing a Person's Access](#)

[Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Batch Printing Photo IDs](#)

Decoding Cards

Select **Configuration : Access Control : Utilities : Card Decoder**.

You can use this page to:

- Decode the bits on Wiegand formatted cards.
- Decode the bytes on Track 2 of Magnetic stripe cards.

Wiegand access cards typically contain a stream of bits that encode the facility code and the encoded card number. The card format specifies the total number of bits, and which of these are the parity bits, the facility code, and the encoded number.

Magnetic stripe cards typically contain a stream of bytes on Track 2 that encode the facility code and the encoded card number. The card format specifies the total number of bytes, the Start Sentinel (indicated with the ASCII value ";"), the End Sentinel (indicated with the ASCII value "?"), a field separator (indicated with the ASCII value "="), and a checksum character.

If you do not know the format of the existing card population, you can discover it using this utility.

NOTE: The more you can learn about the card format before you try this process, the easier this process will be. Any information you can obtain, such as facility code value, will facilitate the decoding process.

To decode a population of Wiegand cards:

1. Obtain five to ten sample cards from the existing card population.
2. Select a card format from the **Card Format** drop-down list. To include disabled card formats in the list, select the **Include disabled card formats** check box.

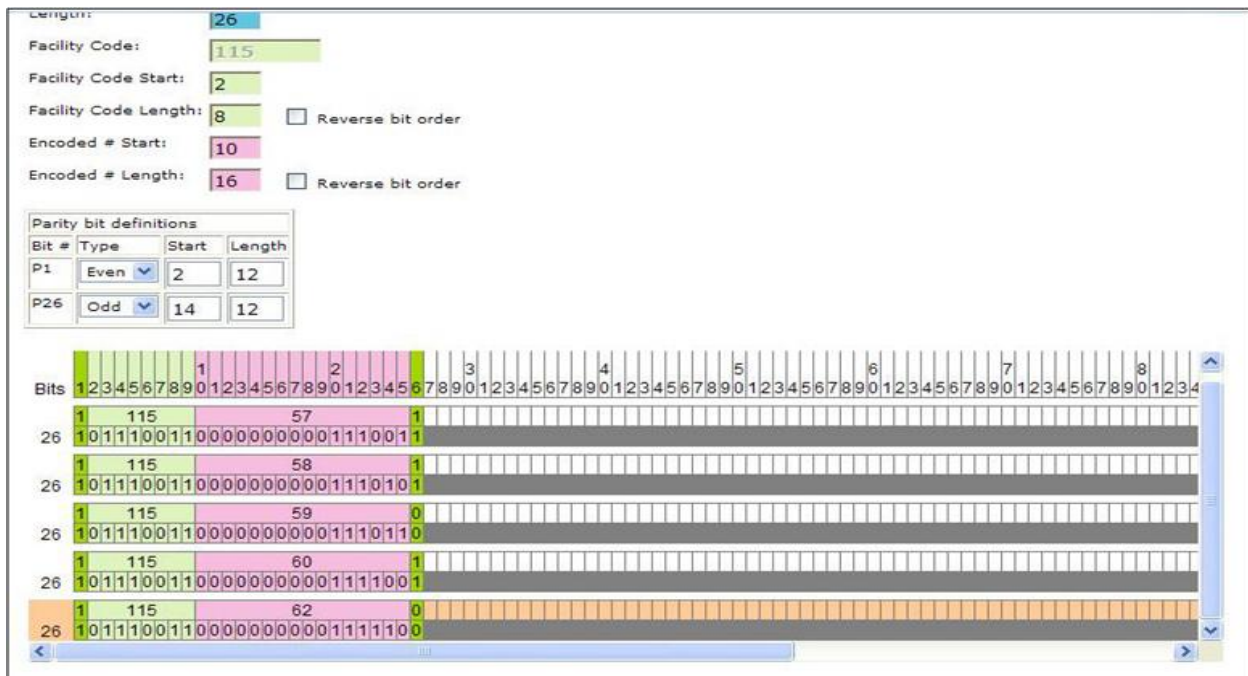
Wiegand 26 bit format is the most popular, so try that first. The numbered bit positions displayed across the bottom of the page become color coded based upon the card format selection. Facility code bit positions are shaded green. Card ID bit positions are shaded purple.

The **Facility Code**, **Facility Code Start**, and **Facility Code Length** boxes (green background), and the **Encoded # Start** and **Encoded # Length** boxes (purple background) automatically display the correct values for the selected card format.

- (optional) If your facility reverses the bits in the Facility Code and/or Card ID portions of its card format, select the **Reverse bit order** check box for **Facility Code Length** and/or **Encoded # Length**.
- Select a reader for reading sample cards from the **Use Reader** drop-down list.
- Read several of the sample cards. The bit streams from these cards appear at the bottom of the page under the bit position numbers. The **Length** box displays the total number of bits on the card.
- Now comes the hard part. You must examine the bits from each card to discover patterns that will tell you the format of the card. See the example below.
- Depending on the patterns you see, you may need to alter the **Facility Code Start** or the **Facility Code Length**. You may also need to alter the **Encoded # Start** or the **Encoded # Length**.
- Once you have correctly set the facility code and encoded number start bits and lengths, you can create a card format to match the card population by clicking the **Create Card Format** button.
- This will take you to the [Card/Keypad Formats](#) page. Enter a **Name** for your format and click **Save**.

Example

Assume that five cards are read. The bit position numbers are color-coded according to the Wiegand 26 bit format, which was selected in step 2 above. The bit streams shown in the following figure are displayed.



Note the following:

- All the cards have a total bit length of 26.

- These cards differ most between bit positions 10 to 26. It is likely that this is where the card ID number is located since each card ID number is unique.
- All the cards have a repeating pattern in the first 9 bit positions. It is likely that this is where the facility code is located since facility codes are typically the same on an entire batch of cards. Facility code values typically range from 0 to 255 and therefore do not require more than 8 bits.
- All the cards have an even number of ones (1). It is likely that these cards are coded with even parity and therefore either the first bit, or the last significant bit (the 26th bit), or both, are used for parity error checking.

Based on these observations we can assume that:

- These are Wiegand 26 bit cards.
- The 1st and 26th bits are parity bits.
- The facility code is one byte (8 bits) from bit 2 to bit 9.
- The facility code value is 115.
- The card ID number is two bytes (16 bits) from bit 10 to bit 25.
- The card ID numbers for these cards are, in order: 57, 58, 59, 60, and 62.

See also: [Specifying Card/Keypad Formats](#)

[Changing a Person's Access](#)

[Access Card Formats](#)

Deleting Photo ID Layouts

Select **Administration : Utility : Photo ID Layout Delete**.

- or -

Select **Configuration : Access Control : Utilities** and then click **Photo ID Layout Delete**.

On this page you can delete photo ID layouts that have been uploaded to the controller.

NOTE: This utility can also be reached by selecting **Setup : Access Control : Utilities**.

To delete a photo ID layout:

1. Select the **Delete?** check box next to each photo ID layout you want to delete.
2. Click **Delete File(s)**.

See also: [Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Batch Printing Photo ID](#)

[Photo ID Requests Report](#)

[System Data for Photo ID Layouts](#)

[Uploading Photo ID Layouts](#)

Uploading Photo ID Layouts

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

- or -

Select **Configuration : Access Control : Utilities : Photo ID Layout Upload**.

On 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](#).

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**.
NOTE: Photo ID layout files must end with the .dgn extension and can be no larger than 15 MB.
3. Click **Save**.

See also: [Capturing and Saving ID Photos](#)

[Printing Photo IDs](#)

[Batch Printing Photo IDs](#)

[Photo ID Requests Report](#)

[System Data for Photo ID Layouts](#)

Bulk Changing the Facility Code Mode for Mercury Readers/Keypads

Select **Configuration : Access Control : Utilities : Facility Code Mode**.

When configuring a reader/keypad for a Mercury panel, you can select a Facility Code Mode. The Facility Code Mode will determine the conditions under which the reader/keypad will grant access based solely on a match of a credential's facility code (rather than on a match of both the facility code and the encoded credential numbers).

To change the Facility Code Mode for multiple readers/keypads at once, you can apply it to one or more reader groups.

To bulk change the Facility Code Mode for Mercury readers/keypads:

1. In the list of reader groups, select one or more groups, or click **Select All** to select all available groups.
2. On the **Facility Code Mode** drop-down list, select one of the available modes:

- **None** (the default): The facility code is treated as part of the overall encoded credential number. A card matching only the facility code will not be granted access.
 - **Configuration**: Facility-code only checking is turned on only while the complete set of credentials is being downloaded to the Mercury panel. Once the credential download is complete, the behavior is the same as for the None setting.
 - **Offline**: Facility-code only checking is turned on only when the SIO is disconnected from its Mercury panel (via the RS-485 link). When the SIO is connected to the panel, the behavior is the same as for the None setting.
 - **Configuration and Offline**: Facility-code only checking is turned on both during the credential download and when the SIO is disconnected from its Mercury panel. At all other times, the behavior is the same as for the None setting.
 - **Permanent**: Facility-code only checking is turned on at all times.
3. Click **Apply** to apply the selected mode to all Mercury readers/keypads in the selected groups.

See also: [Setting Up Readers/Keypads](#)

[Setting Up Reader Groups](#)

[Specifying Card/Keypad Formats](#)

[Configuring Mercury Panels](#)

Bulk Changing the Allegion AD-400 Lockset Mode

Select **Configuration : Access Control : Utilities**.

You can change an Allegion AD-400 Lockset Mode for multiple Schlage AD-400 locksets at once by assigning it to one or more reader groups.

NOTE: An Allegion AD-400 Lockset Mode other than None cannot be assigned to a reader group containing a lockset whose associated portal: (1) has an unlock time spec other than Never, (2) is in [Double Card Presentation Mode](#), (3) has been switched to an [unlocked or locked state](#), or (4) has a [scheduled unlock/lock action](#) or an [unlock/lock event action](#) defined.

To bulk change the Allegion AD-400 Lockset Mode:

1. Click the **Allegion AD-400 Lockset Mode** link.
2. On the page that appears, select the reader groups containing the locksets you want to configure.
Click **Select All** to select all of the available reader groups.
3. Select a mode from the **AD-400 Lockset Mode** drop-down list.
The available modes are None, Office, Privacy, and Apartment.
4. Click **Apply**.
The mode you selected will be applied to all AD-400 locksets in the selected groups.

See also: [Setting Up Readers and Keypads](#)

[Special Considerations for Configuring Schlage Wireless Devices](#)

Alarms

Select **Configuration : Alarms** to display the following options.

Choose this	To see information on
Alarm Filters	Creating alarm filters. Each filter defines criteria that alarms must match in order to be displayed in the Offered Alarms view of the Alarm Workflow widget.
Alarm Filter Groups	Creating groups of alarm filters. An alarm filter can be assigned to users to restrict the number of alarms they can view in the Alarm Workflow widget.
Alarm Panels	Configuring alarm panels and specifying auto-arming behavior.
Alarm Workflow Policies	Creating alarm workflow policies. Each policy defines a set of rules that dictate whether or when an event's active alarms will be moved to the Escalated or Urgent state.
Events	Specifying events and system behavior in response to the events.
Event Groups	Specifying groups of events for use in user roles.
Inputs	Naming inputs and specifying node, slot, and position. Entering an output name as a following resource ID.
Input Groups	Creating and editing groups of inputs. Selecting a time spec for arming inputs in an input group.
Outputs	Naming outputs and specifying node, slot, and position. Entering a default state of Energized or Not Energized.
Output Groups	Creating and editing groups of outputs. Selecting a time spec for activating outputs in the group.
Temperature Inputs	Naming temperature inputs and specifying node, slot, and position. Selecting temperature-related events.
Virtual Inputs	Connecting virtual inputs to events when motion is detected or a camera goes down.

See also: [Integrating Alarm Panels with the System \(PDF\)](#)

[DMP Intrusion Panel Integration \(PDF\)](#)

[Setting Up Portals](#)

[Creating Custom User Roles](#)

[Monitoring and Resolving Alarms in the Alarm Workflow Widget](#)

Alarm Filter Setup

Setting Up Alarm Filters

Select **Configuration : Alarms : Alarm Filters**.

Alarm filters let you restrict the alarms to which individual users have access. For example, if your organization uses a central command center to oversee locally monitored locations, you can create an alarm filter that allows its operators to view and work with only urgent or high priority alarms.

When creating an alarm filter, you define criteria that an alarm must match in order to be displayed in the Offered Alarms view of the [Alarm Workflow widget](#). (The filter will have no effect on the widget's Adopted Alarms view.) Any alarm that matches all of your criteria will be displayed when specific users are logged in.

To define the filter criteria, you can select some combination of the following alarm attributes:

- **Partition:** If you select a partition name, only alarms activated in that partition will be displayed.
Individual users will see the alarms only if the selected partition is their native partition or if they have been [granted a user role in that partition](#). In addition, the Alarm Workflow widget will need to be configured to [allow multiple partition viewing](#).
- **State:** If you select an alarm state (Active, Escalated, Urgent, or Resolved), only alarms in that state will be displayed.
- **Name:** If you select an alarm name, or a subset of the name, only alarms with matching names will be displayed. (An alarm's name is the same as the name of the associated event.)
- **Priority:** If you select a priority number or a range of priority numbers, only alarms with matching priority numbers will be displayed. (An alarm's priority number is defined in the associated event definition. The highest priority is 1 and the lowest priority is 20.)

Once you have defined an alarm filter you can add it to an [alarm filter group](#) and then assign the group to individual users (via the Login tab of their person records). When these users are logged in, they will be able to view and work with only alarms matching the criteria defined for one or more filters in the group.

To create an alarm filter:

1. Enter a **Name** for the alarm filter, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the filter that explains its use.
3. To filter alarms by **Partition**, select a partition name, or select **All** to display alarms from all partitions.
4. To filter alarms by **State**, select an alarm state (Active, Escalated, Urgent, or Resolved), or select **All** to display alarms in all states.
5. To filter alarms by name, enter either the full alarm name or a subset of the name into in the **Alarm Text Filter box**.
For example, to display alarms with the names "HeldDoor" and "ForcedDoor, you can enter "Door" or "door." The search is not case sensitive.
6. To filter alarms by priority number, specify a **Priority Range**. For example, to display priority 1, 2, and 3 alarms, enter a 1 in the From box and a 3 in the To box. To display only priority 1 alarms, enter a 1 in both boxes.
7. Click **Save**.

See also: [Creating Alarm Filter Groups](#)

[Setting Up Events](#)

[Editing Person Records](#)

[Monitoring and Resolving Alarms in the Alarm Workflow Widget](#)

Creating Alarm Filter Groups

Select **Configuration : Alarms : Alarm Filter Groups**.

With this page you can create, edit, and delete alarm filter groups. When users to whom an alarm filter group is assigned (via the Login tab in their person records) are monitoring alarms in the [Alarm Workflow widget](#), they will be able to see only alarms matching the criteria defined for one or more filters in the group.

To add an alarm filter group to the system:

1. Enter a descriptive **Name** for the alarm filter group, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the group that explains its use.
3. For each alarm filter you want to add to this group, select it in the **Available** list and click the right-arrow button to move it to the **Selected** list.
4. Click **Save**.

To edit an alarm filter group:

1. Select an existing alarm filter group from the **Name** drop-down list.
The remaining fields on the page fill with the settings for the selected group.
2. Edit any part of the group definition.
3. Click **Save**.

To delete an alarm filter group:

1. Select an existing alarm filter group from the **Name** drop-down list.
2. Click **Delete**.

See also: [Creating Alarm Filters](#)

[Editing Person Records](#)

[Monitoring and Resolving Alarms in the Alarm Workflow Widget](#)

[How Groups are Used in the System](#)

Alarm Panel Setup

Setting Up Alarm Panels

Select **Configuration : Alarms : Alarm Panels**.

Once an alarm panel has been wired to a node in your security management system, you can use the **Alarm Panels** section of this page to:

- Add, change, or delete the panel.
- Assign two inputs for receiving armed status and zone status from the panel.
- Assign an output for arming or disarming the panel from the browser.

In the [Auto Arm](#) section of this page you can specify the arming, disarming and warning behavior of the panel.

In the [Events](#) section of this page you can specify system events to occur when a panel alarm occurs or when the panel fails to arm.

NOTE: A maximum of four alarm panels per node are allowed for each system. For instructions on wiring alarm panels to nodes in your system, see Tech Note 8.1, [Integrating Alarm Panels with a Security Management System](#).

To add an alarm panel to the system:

1. Enter a descriptive **Name** for the alarm panel, or click the **add** link and then enter the name.

NOTE: The **Name** drop-down list includes all alarm panels currently defined in the system. When you select an alarm panel, the page fills with the data that define that alarm panel.

2. From the **Network Node** drop-down list, select the node to which the panel's inputs and outputs are wired.
3. From the **Receive zone status input** drop-down list, select the input wired to the panel zone status line.
4. From the **Receive armed/disarmed state input** drop-down list, select the input wired to the panel armed state line.
5. From the **Toggle armed state output** drop-down list, select the output wired to the panel arming line. This output allows you to arm the panel from the browser interface.

NOTE: The output for arming and disarming the panel cannot be assigned to both an alarm panel and to another function. The only outputs that appear in this drop-down list are those not currently assigned elsewhere.

6. Click **Save**.

See also: [Arming and Disarming Alarm Panels](#)

[Setting Up Alarm Panel Arm/Disarm Behavior](#)

[Setting Up Alarm Panel Events](#)

[Integrating Alarm Panels with a Security Management System \(PDF\)](#)

Setting Up Alarm Panel Arm/Disarm Behavior

Select **Configuration : Alarms : Alarm Panels**.

In the **Arm/Disarm** section you can:

- Enable or disable automatic panel arming.
- Specify an alarm warning output and the alarm warning duration.
- Select a time spec to determine when the panel will automatically arm.
- Specify a reader group that will automatically disarm the panel.
- Specify a reader group that will be disabled whenever the panel is armed.

To set up the auto arm behavior of an alarm panel:

1. To enable auto arm behavior click to put a check in the **Auto-arm enable** checkbox.
2. Select from the **Panel arming warning output** drop-down list the output that is wired to the warning device (probably sonic).
3. In the **Warning duration** text box enter the number of seconds that the alarm state warning output fires prior to arming the panel.
4. Select from the **Auto-arm time specification** drop-down list the time spec or time spec group that defines the period when the panel is to be armed.
5. You can specify the length of time that the panel must show all zones inactive prior to auto-arming. In the **Auto-arm inactivity time** text box enter the required duration in minutes.
6. The **Arm panel request timeout** setting determines how long the security management system waits before assessing whether or not the panel has armed. Set this value in seconds and ensure that it is at least 5 seconds longer than the panel's own arming grace period.
7. Select from the **Disarm reader group** drop-down the reader group that will disarm the panel when a valid card read is performed.

NOTE: The alarm panel will disarm only if the cardholder has an [access level configured for auto-disarming](#) the alarm panel, and the reader must belong to a [reader group specified for disarming](#) the alarm panel.

8. Select from the **Disabled reader group** drop-down the group of readers that will always deny access when the alarm panel is armed.
9. Click **Save**.

See also: [Setting Up Alarm Panels](#)

[Setting Up Access Levels](#)

[Setting Up Alarm Panel Events](#)

[Setting Up Reader Groups](#)

[Arming and Disarming Alarm Panels](#)

Setting Up Alarm Panel Events

Select **Configuration : Alarms : Alarm Panels**.

In the **Events** section you can:

- Specify an event to be activated when the alarm panel should be auto-armed but the attempt to arm it was unsuccessful.
- Specify an event to be activated when zone activity from an armed panel triggers a panel alarm.

To specify events for panel states:

1. Select from the **Arming failure** drop-down list the event to be activated when the attempt to arm the alarm panel was unsuccessful.
2. Select from the **Zone active while armed** drop-down list the event to be activated when zone activity from an armed panel triggers a panel alarm.
3. Click **Save**.

See also: [Setting Up Events](#)

[Available Actions for Events](#)

[Setting Up Alarm Panels](#)

[Setting Up Alarm Panel Arm/Disarm Behavior](#)

[Setting Up Access Levels](#)

[Arming and Disarming Alarm Panels](#)

Creating Alarm Workflow Policies

Select **Configuration : Alarms : Alarm Workflow Policies**.

An alarm workflow policy defines a set of rules dictating when alarms will be moved from their initial Active state to the Escalated state and from the Escalated state to the Urgent state. When the policy is assigned to an [event definition](#) the system will apply these rules to all alarms that become active for the event.

Sites with central command centers that oversee locally monitored locations can use alarm workflow policies to ensure that alarms are handled effectively across the site. Alarms that occur at locations where no local operators are present or that are not handled in a timely manner can be automatically escalated and brought to the attention of the command center.

Note: Every system has a default alarm workflow policy that defines a single rule. According to this rule, alarms are never escalated. An alarm remains in the Active state until it is acknowledged (if acknowledgement is required according to the associated event definition) and its underlying cause has been cleared. At that point, it is considered resolved and is removed from the system.

To create an alarm workflow policy:

1. Click the **add** link and enter a **Name** for the new policy.
2. Optionally, enter a **Description** for the policy that explains its use.

3. Select the **Enabled** check box for any of the following options that you want applied to an event's alarms:
 - **Move alarm from Active to Escalated if no operator is present in local partition.** When this option is enabled, the system will move an alarm from its initial Active state to the Escalated state immediately if there are no local operators present. This means that either no local operators have the [Alarm Workflow widget](#) open in their browsers or that the "Operator is present" check box is unselected in all open instances of the widget.
 - **Number of minutes before moving alarm from Active to Escalated.** When this option is enabled, the system will move an alarm from its initial Active state to the Escalated state after the number of minutes you enter in the text box. If you enter a zero (0), the alarm will be moved to the Escalated state immediately.
 - **Number of minutes before moving alarm from Escalated to Urgent.** (available only if one or both of the "move to Escalated" options described above are enabled) When this option is enabled, the system will move an alarm from the Escalated state to the Urgent state after the number of minutes you enter in the text box. If you enter a zero (0), the alarm will be moved to the Urgent state immediately.
4. Click **Save**.

See also: [About the Alarm Workflow Widget](#)

[Monitoring and Resolving Alarms in the Alarm Workflow Widget](#)

[Setting Up Events](#)

Event Setup

Setting Up Events

Select **Configuration : Alarms : Events**.

Events can be a complex series of actions taken in response to a trigger, such as an input going into an alarm state, or credentials being presented by someone whose [access level](#) is configured to activate the event. Once an event is defined, it can be assigned to any number of inputs, virtual inputs, access levels, intrusion panels, and portals.

To set up an event:

1. Enter a **Name** for the event, or click the **add** link and then enter the name.

TIP: If the new event will be similar to an existing event, select that event and click the **clone** link. The new event will retain all attributes of the original event, including its defined actions. After naming the new event, you will need to change only the few attributes that it will not have in common with the original event.
2. Optionally, enter a **Description** for the event that explains its use.

If the Send Email or Send SMS message action is defined for this event, the description you enter will appear in all email or SMS messages that are sent when the event is activated.
3. Optionally, enter an **Operator short msg** and/or **Operator long msg**.

The short message will appear in the Name column for all alarms displayed on the Monitoring Desktop and Widget Desktop when the event is activated. The long message will appear when a user hovers over the Name column or clicks the Details icon in the Commands column.

4. From the **Enabled Timespec** drop-down list, select a [time spec](#). The event will be activated only during the times defined by this time spec.
5. From the **Priority** drop-down list, select a priority number for the event. One (1) is the highest priority and twenty (20) is the lowest priority. On the Monitoring Desktop and Widget Desktop, the highest priority events are listed first. If actions defined for two concurrent events conflict, the higher priority event takes precedence.
6. Select from the **Camera** drop-down the camera you want displayed on the [Monitoring Desktop](#) when this event is activated.
7. For **Alarm Mode**, select one of the following to determine whether, or how, operators will be able to view and handle alarms for this event in the [Events widget](#) and [Alarm Workflow widget](#):
 - **Activations do not display alarms:** No alarms will appear in either widget when the event is activated. Selecting this mode will disable all settings in the Acknowledgements section of the page.
 - **Multiple activations by the same trigger display a single alarm:** In each widget, an alarm will appear when the event is activated. If the event is activated by multiple triggers, a separate alarm will appear for each trigger. Any subsequent activation by the same trigger will result in a new alarm that replaces the previous alarm for that trigger—so operators will always see a single alarm for each trigger.

When this mode is selected, the event will require acknowledgement only if **Required** is selected in the Acknowledgements section.

- **Multiple activations display multiple alarms:** The behavior will be different in each widget. In the Events widget, the behavior will be as described above (that is, multiple activations by the same trigger will display a single alarm). In the Alarm Workflow widget, an alarm will appear when the event is activated, and subsequent activations (by any trigger) will result in additional alarms—so operators will always see a separate alarm for each activation.

When this mode is selected, the event will always require acknowledgement. It will remain active until all of its alarms have been acknowledged and its underlying cause has been cleared.

NOTE: Regardless of which alarm mode you select, a message will appear in the Activity Log when the event is activated. Subsequent activations will not result in additional Activity Log messages.

8. If you selected the third Alarm Mode option ("Multiple activations display multiple alarms") at step 7, apply an [alarm workflow policy](#) to the event by selecting it from the **Workflow** drop-down list, which appears next to that option whenever it is selected.

The rules defined in the selected alarm workflow policy will determine the conditions under which alarms for this event will be moved from the initial Active state to the Escalated state and from the Escalated state to the Urgent state. If you leave the default "No Escalation" policy selected, the system's default alarm workflow policy will be applied to this event.

9. Set the **Acknowledgements**:
 - **Required:** Select this check box if you want the event, once activated, to remain active until an operator acknowledges it. This will ensure that even if the cause of an alarm is momentary (such a vehicle moving past a detector) or is deactivated before

the alarm is noticed (for example, by an intruder who quickly closes an open door behind him), operators will be presented with an active alarm to be acknowledged.

- **Require Duty Log Entry:** Select this check box to force the operator to enter a Duty Log message when acknowledging the event.
- **Maximum Duration:** Enter a duration for the event in seconds. The event will auto-acknowledge when the duration has elapsed.

NOTE: The Maximum Duration option is available only when the Required check box is selected. Auto-acknowledge is not allowed for events that do not require acknowledgement.

- **Allow Clear Actions:** Select this check box to allow an operator to clear all of the event's actions once its underlying cause has been cleared.
- **While Active?:** Select this check box to allow an operator to clear all of the event's actions, even if its underlying cause has not been cleared.

NOTE: The Acknowledgements settings will be disabled if the **Activations do not display alarms** alarm mode is selected.

10. Under **Actions**, [define the actions](#) the system will perform when this event is activated.

11. Define the event **Notification** details:

- Select from the **Sound** drop-down list the sound file to be played when this event is activated. If you select **<add new>**, an **Upload Sound file** window appears and you can upload sound files to the Controller.

NOTE: You can upload a sound file (.wav) that is up to 100K in size, and you can store up to 256 sound files on the controller.

- Select the **Repeat** check box to have the selected sound file play in a loop until the event has cleared or has been acknowledged.
- Select from the **Color** drop-down list the text color for this event when it is displayed in the **Alarms** tab of the [Monitoring Desktop](#).

12. Click **Save**.

To edit or delete an event:

1. Select an existing event from the **Name** drop-down list.
2. To edit the event, change any of its settings.
3. To rename the event, click the **rename** link and enter a new name.
4. Click **Save**.
5. To remove the event from the system, click **Delete**.

See also: [Defining Event Actions](#)

[Available Actions for Events](#)

[Creating Alarm Workflow Policies](#)

[Setting Up Access Levels](#)

[Entering Duty Log Comments into the Activity Log](#)

[Using the Monitoring Desktop](#)

[Setting Up Threat Level Groups](#)

[Setting Threat Levels](#)

[Using Threat Levels to Change System Behavior](#)

Defining Event Actions

Select **Configuration : Alarms : Events**.

When [setting up an event](#), you can define actions that the system will perform when the event is activated.

To define actions for an event:

1. In the **Actions** section of the Events page, select **<add new>** in the **current actions** list box.
2. Enter a **Name** for the new action and select the **Enabled** box to enable the action.
3. From the **Action** drop-down list, select the action the system should take when this event is activated and, from the drop-down list that appears to the right, select the appropriate resource for that action. For information on the actions you can select for an event, see [Available Actions for Events](#).

NOTE: If you select the **Move Camera to Preset** or **Record Video** option, tooltips on the selected setting and the drop-down list items provide the full path to each preset or camera.

NOTE: If you select the **Set Threat Level** action, three options appear to the right. The threat level you select from the **Change to Threat Level** drop-down list will become the current threat level for the default [location](#) in the active partition—unless you select a different location from the **At Location** drop-down list. To change the threat level for all sub-locations of the specified location, select the **Apply to Sublocations** check box.

4. Select a **Priority** number for the action.
5. If you want the action to cease after a certain period, even if the event activation has not yet been resolved, enter a **Max Duration** in seconds.

NOTE: This setting will have an effect only if the event is one that changes the state of a system resource when activated—such as an event that puts a portal into an alarm condition when it is held open. If, in this example, the action will sound a siren when the portal goes into the alarm condition, the siren will cease after the specified number of seconds, rather than continue until the event is resolved.

6. Select the **Perform action every time the event is triggered** check box. See the section below for information how the setting for this option affects the behavior of an event action.
7. Select a **Threat Level Group** to assign to the action. This action will be performed only if the is a member of the assigned threat level group.

NOTE: Select **<not applicable>** if threat level changes should NOT affect the behavior of this event action.

8. Click the **Apply changes to action** button.
You can now add additional actions or edit any actions currently already applied to the event.
9. **NOTE:** The following event actions are supported for Mercury panels: **Lock Portal/Unlock Portal, Momentarily Unlock Portal, Arm Input Group/Disarm Input Group, Activate Output/Deactivate Output, Pulse Output, and Pulse Output Group**. Because of a difference in the Mercury panel hardware, the Arm Input Group and Disarm Input Group event actions will work only for Mercury inputs that are not attached to portals.

About the "Perform action every time the event is triggered" Option

The way you set the **Perform action every time the event is triggered** option for an event action will determine the conditions under which the action will be performed:

- When the check box for this option is selected, the action will be performed every time the event is activated, even if there are unresolved prior activations of the event.
- When the check box is not selected, the action will be performed only if all prior activations have been resolved when the event is activated.

The following table shows the default setting for each of the available event actions.

Event Action	Default Setting for "Perform action every time the event is triggered?"
Activate/Deactivate Intrusion Panel Output	OFF (unchecked)
Activate/Deactivate Output	OFF
Arm/Disarm Alarm Panel	OFF
Arm/Disarm Input Group	OFF
Arm/Disarm Intrusion Panel Area	OFF
Bypass/Reset Bypassed Intrusion Panel Zone	OFF
Lock Portal/Unlock Portal	OFF
Momentarily Unlock Portal	ON (checked)
Move Camera to Preset	ON
Pulse Output/Pulse Output Group	ON
Push Stream to Magic Monitor/Magic Monitor Group	OFF
Push View to Magic Monitor/Magic Monitor Group	OFF
Record Video	ON
Save to Activity Log	ON
Send Email/Send SMS Message	OFF
Set Threat Level	OFF

See also: [Setting Up Events](#)

[Available Actions for Events](#)

Available Actions for Events

Select **Configuration : Alarms : Events**.

When [setting up an event](#), you can specify the action the system will take when the event is activated. The available actions for standard nodes are listed below.

- **Activate/Deactivate Intrusion Panel Output** – You can have the event activate or deactivate an output associated with a DMP intrusion panel.
- **Activate Output/Deactivate Output** – You can have the event activate or deactivate an output. For instance, you might want a buzzer to sound at the main facility if there is a problem at a field office.
- **Arm Alarm Panel/Disarm Alarm Panel** – You can have the event arm or disarm an alarm panel, as defined on the [Alarm Panels](#) page.
- **Arm Input Group/Disarm Input Group** – You can have the event arm or disarm an input group. For instance, you may want certain inputs to be armed once the number of building occupants drops to zero.
- **Arm/Disarm Intrusion Panel Area** – You can have the event arm or disarm an area associated with a DMP intrusion panel.
- **Bypass/Reset Bypassed Intrusion Panel Zone** – You can have the event bypass, or ignore, an individual zone within an area associated with a DMP intrusion panel. You can also have the event reset a bypassed zone.
- **Lock Portal/Unlock Portal** – You can have the event lock or unlock one or more portals. For instance, you might want a single card read to unlock multiple doors.
- **Momentarily Unlock Portal** – You can have the event unlock a portal for the unlock duration configured in the [portal definition](#). An [online remote lockset](#) will be taken out of panic mode if necessary, then returned to panic mode at the end of the unlock duration.

NOTE: A portal associated with a Schlage AD-400 lockset configured for any Allegion AD-400 Lockset Mode other than None (on the [Readers page](#) or the [Access Control : Utilities page](#)) will not appear on the list of portals to which the Lock Portal, Unlock Portal, or Momentarily Unlock Portal action can be applied.

- **Move Camera to Preset** – You can have the event move a security camera to a predefined position. Hover over the selected setting or the items in the drop-down list to see the full path to each preset.
- **Pulse Output/Pulse Output Group** – You can have the event pulse an output or output group for a specific period of time. For instance, you might want an electronic sign to light up for 15 seconds whenever a car drives up to a sensor.
- **Push Stream to Magic Monitor** – You can have the event request that a Magic Monitor display a stream from a NetVR camera.
- **Push Stream to Magic Monitor Group** – You can have the event request that a set of Magic Monitors display a stream from a NetVR camera.

With these event actions, the Magic Monitor(s) will display the stream in the camera cell you specified and with the message type and border color you specified. On a Magic Monitor that does not include the specified stream, the user will see an error message.

NOTE: If the NetVR camera is removed from the system, the Magic Monitor Stream field will change to *<none>* and you will need to either remove the action or select a new stream.

- **Push View to Magic Monitor** – You can have the event request that a Magic Monitor display a Magic View.
- **Push View to Magic Monitor Group** – You can have the event request that a set of Magic Monitors display a Magic View.

With these event actions, the Magic Monitor(s) will display the Magic View you specified. On a Magic Monitor that does not include a view with that name, the user will see an error message.

NOTE: If the Magic View is removed from the system, the Magic View field will change to *<none>* and you will need to either remove the action or select a new view.

- **Record Video** – You can have the event record video. For instance, to capture video of everyone who accesses your building, you can have an event capture a video recording when it is activated by a valid access. Hover over the selected setting or the items in the drop-down list to see the full path to each camera.
- **Save to Activity Log** – You can have the event record an entry in the Activity Log.
- **Send Email/Send SMS Message** – You can have the event send email or an SMS text message to a specific user, such as the system administrator, or to an [email distribution group](#).

NOTE: If either of these actions is defined for an event that is activated by a momentary trigger (such as a request to exit at a REX push button, or a card presentation at a reader), the email or text message will be sent only if (1) the event requires acknowledgment, or (2) the [Perform action every time the event is triggered](#) check box is selected for the action.

- **Set Threat Level** – You can have the event change the threat level for a specific [location](#). By default, it will change the default location for the active partition, but you can specify a different location in the active partition.

The following event actions are supported for Mercury panels: Lock Portal/Unlock Portal, Momentarily Unlock Portal, Arm Input Group/Disarm Input Group, Activate Output/Deactivate Output, Pulse Output, and Pulse Output Group.

Because of a difference in the Mercury panel hardware, the Arm Input Group/Disarm Input Group event actions will work only for Mercury SIO inputs that are not attached to portals.

Creating Event Groups

Select **Configuration : Alarms : Event Groups**.

With this page you can create, edit, and delete event groups. When an event group is added to a customer [user role](#), users holding that role will be able to view and manage alarms for events in the group.

To create an event group:

1. Enter a descriptive **Name** for the event group, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the group that explains its use.
3. For each event you want to add to this group, select it in the **Available** list and click the right-arrow button to move it to the **Selected** list.
4. Click **Save**.

To edit an event group:

1. Select an existing event group from the **Name** drop-down list.
The remaining fields on the page fill with the settings for the selected group.
2. Edit any part of the event group definition.
3. Click **Save**.

To delete an event group:

1. Select an existing event group from the **Name** drop-down list.
2. Click **Delete**.

See also: [Creating Custom User Roles](#)

[Setting Up Events](#)

[How Groups are Used in the System](#)

Input Setup

Setting Up Alarm Inputs

Select **Configuration : Alarms : Inputs**.

With this page you can:

- Add inputs to the system.
- Enable and disable inputs
- Specify an output and/or event to be activated when an input goes into an alarm or trouble state.
- Edit and delete inputs

NOTE: You cannot delete an input that is in use anywhere in the system. The **Used By** list that appears on this page will indicate all of the resources that currently use an input. Inputs can be used by input groups, portals, alarm panels, and elevators.

Before you can complete the definition of [input groups](#), or [portals](#) you must configure the individual input devices.

Inputs have two, three, or four possible states, depending upon which Input Supervision Type is selected. Refer to the [Network Node Hardware Installation Guide \(PDF\)](#) for specifics regarding input states and resistance values.

To add an input to the system:

1. Enter a descriptive **Name** for the input, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the input that explains its use.
3. Select the **Enabled** check box to the right of the **Name** field.

4. Inputs that are not defined as part of an [input group](#) will not arm. You must either select the **Always Armed** check box, or create an input group and assign a time spec to the group that defines when the inputs in the group will be armed.
5. From the **Network Node** drop-down list, select the node to which this input is wired.
6. From the **Expansion Slot** drop-down list, select the [slot number](#) of the board to which the input is connected.
7. From the **Position** drop-down list, select the connector [position number](#) to which the input is connected.
8. If this input is to activate a particular output, select the output from the **Following Output** drop-down list.

A Following Output is fired in response to an input changing to the [Alarm](#) state. For example, a door switch monitor (DSM) input can be configured to have a Trigger Output turn on a hallway light whenever the door opens. This action takes place on the Node only.
9. (optional, for use with Mercury panels only) For **Debounce**, specify a scan multiplier value: the number of consecutive input scans that must agree before a change of state is reported. The scan period is 16.7 milliseconds. Valid scan multiplier values are 0 through 15.

The default setting is 5. The recommended setting is 2 for a REX and 4-6 for a standard input.
10. (optional, for use with Mercury panels only) To delay the input's change to the Alarm state, enter in the **Hold Time** field the number of seconds the state change should be delayed.

The default is 3 seconds. The recommended setting is 2-15 seconds.
11. (optional, for use with S2 nodes only) To delay the input's change to the Alarm state, select from the **Alarm Delay** drop-down list the number of seconds the state change should be delayed. This feature is not available for Mercury panels.

This is useful for portals that do not properly send a REX signal prior to sending a DSM state change. It allows you to delay the state change so the REX signal can be received and processed first. Note that if the physical input returns to the Normal state before the delay timer expires, the delay timer will be canceled and the input will remain in the Normal state.
12. From the **Input supervision type** drop-down list, select the circuit type (NO = normally open, NC = normally closed) and resistor configuration for this input.

It is critical that this selection accurately reflects the input circuit. The system supports 1K Ohm resistors only, and a circuit diagram is displayed on the page next to **Termination Circuit**. The various circuits and resistor configurations create resistance values used by the system in determining normal, alarm, and trouble states. For more specific information on these wiring configurations and resistance values see the section on connecting inputs in the [Network Node Hardware Installation Guide \(PDF\)](#).
13. In the **In group(s)** field, review the [input groups](#) that to which this input belongs.

NOTE: You cannot delete an input while it is part of an input group.
14. To have the input activate an event when it enters the Alarm state, select the appropriate event from the **Off-normal Event** drop-down list and check the **Enabled** box to the right.
15. To have the input activate an event when it enters a trouble state (Short or Open), select the appropriate event from the **Supervision Error Event** drop-down list and check the **Enabled** box to the right.

NOTE: You cannot set up supervision error events for an unsupervised input.
16. Click **Save**.

NOTE: The **Advanced Settings** allows you to set up multiple events to execute in response to an input entering any one of its states.

Using Advanced Settings to set up events

1. Click the **Advanced Settings** button in the **Events** section.
2. In the Advanced Settings window, select an input state from the **State** drop-down list.
3. From the **Event** drop-down list, select an event to execute when the input enters the selected state.
4. Click **Apply** to move the state/event pairing into the **Current Triggers** box.

NOTE: You can assign additional events to the same state.

5. Click **Save**.

To edit or delete an input:

1. Select an existing input from the **Name** drop-down list.
2. Edit any part of the input definition.
3. Click **Delete**.

If the input is not currently used by any input group, portal, alarm panel, or elevator, it will be removed from the system.

See also: [Slot and Position Numbers](#)

[Creating Alarm Input Groups](#)

[Setting Up Events](#)

[Setting Up Virtual Inputs for VMS Cameras](#)

[Network Node Hardware Installation Guide \(PDF\) - section on connecting inputs](#)

[Monitoring and Resolving Alarms](#)

Creating Alarm Input Groups

Select **Configuration : Alarms : Input Groups**.

With this page you can create, edit, and delete input groups. When an input group is assigned to an [event action](#), its inputs will automatically arm or disarm whenever the event is activated.

To add an input group to the system:

1. Enter a descriptive **Name** for the input group, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the input group that explains its use.
3. From the **Auto-arm Time spec** drop-down list, select a time spec or time spec group. The inputs in this group will be armed during the times defined by the selected time spec or time spec group.

For example, an input group containing interior motion detectors might be assigned an auto-arm time spec that defines the period from midnight to 5 AM, when no one is supposed to be in the building.

4. From the **Threat Level Group** drop-down list, you can select a threat level group to associate with this input group. This input group will arm only when the current system threat level is included in the selected threat level group.
5. For each input you want to add to this group, select it in the **Available** list and click the right-arrow button to move it to the **Selected** list.
6. Click **Save**.

NOTE: [Inputs](#), [Virtual Inputs](#), and [Temperature Inputs](#) can all be put into input groups.

To edit an input group:

1. Select an existing input group from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this input group.
2. Edit any part of the input group definition.
3. Click **Save**.

To delete an input group:

1. Select an existing input group from the **Name** drop-down list.
2. Click **Delete**.

See also: [Setting Up Alarm Inputs](#)

[Setting Up Temperature Inputs](#)

[Setting Up Virtual Inputs for VMS Cameras](#)

[Creating Time Specs](#)

[Setting Up Threat Level Groups](#)

[How Groups are Used in the System](#)

Setting Up Temperature Inputs

Select **Configuration : Alarms : Temperature Inputs**.

With this page you can:

- Create, edit, enable or disable, and delete temperature inputs.
- Specify maximum and minimum temperatures.
- Select events for temperature alarm states.

To add a temperature input to the system:

1. Enter a descriptive **Name** for the temperature input, or click the **add** link and then enter the name.

NOTE: If you are adding an input that is substantially similar to an existing one, you can save time by selecting the existing input, clicking **clone**, then entering a name for the new input and making any needed changes.

2. Optionally, enter a **Description** for the input that explains its use.
3. Be sure that the **Enabled** checkbox to the right of the **Name** field is checked.
4. Inputs that are not defined as part of an [Input Group](#) will not arm. You must either select the **Always Armed** check box, or create an input group and assign a [time spec](#) to the group that defines when the inputs in the group will be armed.
5. From the **Network Node** drop-down list, select the node to which this input is wired.
6. From the **Expansion Slot** drop-down list, select the [slot number](#) of the board to which this input is connected.
7. From the **Position** drop-down list, select the connector [position number](#) to which this input is connected.
8. Enter a **Max Temperature** and a **Min Temperature**. Temperatures exceeding these boundaries will generate an alarm state.

NOTE 1: You can set the temperature scale to Celsius or Fahrenheit on the [Network Controller page](#). Internally the temperature data is stored and calculated using whole integers and the Celsius scale. This may result in temperatures entered in Fahrenheit being rounded to the nearest whole degree Celsius. For example, setting the maximum temperature to 99° Fahrenheit will display as 98.6° F (37° C).

NOTE 2: The default and highest maximum temperature is 125° C. The default and lowest minimum temperature is -55° C. These defaults will not display.

9. From the **Local Status Output** drop-down list, select the output to fire if this temperature input falls outside the boundary of either temperature limit.
You can, for example, wire an output to a blinking light at the location of each temperature input point. This would make it easy to find the temperature point that has entered an alarm state.
10. Select a **High Temp Event** and a **Low Temp Event** and select their the **Enabled** check boxes.
11. From the **Point Fault Event** drop-down list, select an event to execute if the temperature point is no longer communicating temperature data to the system.
12. Click **Save**.

See also: [Setting Up the Network Controller](#)

[Creating Alarm Input Groups](#)

[Setting Up Events](#)

[Slot and Position Numbers](#)

[Network Node Hardware Installation Guide \(PDF\) - section on connecting temperature sensors](#)

Setting Up Virtual Inputs for VMS Cameras

Select **Configuration : Alarms : Virtual Inputs**.

Unlike other input types, virtual inputs do not correspond to physical, configured system resources. Instead, each virtual input corresponds to a camera that was set up during the configuration of an NVR through its own client or web interface.

Strictly speaking, you do not set up virtual inputs. They are created automatically when you integrate the video system and they are deleted if you delete the video integration. However, you can enable a virtual input, specify when it will be armed, and associate it with up to three events: one to be activated when the associated camera is in a normal state, one to be activated when the camera detects a motion event, and one to be activated when the camera fails.

Note that the activation of events associated with a virtual input might be constrained by either or both of the following:

- The times the associated camera is scheduled to record video (as specified during the configuration of the NVR through its own client or web interface). Events associated with the virtual input will be activated only during these scheduled times.
- If the virtual input is included in an input group, the times defined by the group's auto-arm time specification. At all other times, the virtual input will be unarmed and its associated events will not be activated.

Setting up a virtual input:

1. From the **Name** drop-down list, select a virtual input and select the **Enabled** check box.
2. To arm the virtual input, either select the **Always Armed** check box or include it in an [input group](#) so it will be armed according to the group's auto-arm time specification.
3. Select the **Store and Display Activity** check box if you want all events activated by changes in the state of the associated camera to be logged in the Activity Log and stored in the database.

NOTE: This check box is unchecked by default. If you select it, the Activity Log may receive an excessive number of alarms.

4. From the **Camera Normal Event** drop-down list, select the event to be activated when the camera is in a normal state. Select the **Enabled** check box to enable this event.
5. From the **Video Motion Event** drop-down list, select the event to be activated when the camera detects a motion event, then select the **Enabled** check box to enable this event. The event you select does NOT need to have the Record Video action defined. In this case, the camera will automatically record video when it detects a motion event, and the recording will be available via a camera icon in the Activity Log.
6. From the **Video Fail Event** drop-down list, select the event to be activated when the camera fails or stops sending data to the system. Select the **Enabled** check box to enable this event.
7. Click **Save**.

See also: [Setting Up Alarm Inputs](#)

[Creating Alarm Input Groups](#)

[Setting Up Events](#)

Configuring DMP Intrusion Panels

Select **Configuration : Alarms : Intrusion Panels**.

NOTE: This page is available only if your system license allows the addition of DMP intrusion panels.

To configure DMP intrusion panels to work with the system, you can:

- Add, edit, and delete panels.
- Specify the account number and/or IP address for a panel, and the port number assigned for outbound communications to the panel.
- Assign events to a panel, and to individual areas, zones, and outputs associated with the panel. These events will be activated by specific alarms and status changes on the panel.

NOTE: For information about integrating a Digital Monitoring Products (DMP) XR500 Series or XR550 Series control panel into a security management system, including important information about the ports that must be available for communications between the DMP panel and the system, see Tech Note 18, [DMP Intrusion Panel Integration \(PDF\)](#).

To configure a DMP intrusion panel:

1. Enter a descriptive name for the panel in the **Panel** field, or click the **add** link and then enter the name.
2. To rename the selected panel, click the **rename** link and enter the new name in the **Panel** box.
3. Select a panel type from the **Type** drop-down list: XR500, XR500E, XR500N, XR550, or XR550E.

If you do not select a panel type, the system will select one based on the information it receives from the panel on the first successful connection.

4. Enter or change the **Account** number, the **IP Address**, and the **Port** number assigned for outbound communications to the panel.

For DMP panels running firmware version 205 or earlier, the default port number is 2001. For DMP panels running firmware version 206 or later, the default port number is 2011.

5. Select the **Time Sync** check box to have the controller synchronize the panel time to its own time several times an hour.

Be sure that both the controller time and panel time are set to the appropriate time zone. For a DMP panel, you must use the DMP Remote Link application to set the *Hours from GMT* option on the System Options page. For example, set the option to 5 for Eastern, 6 for Central, 7 for Mountain, and 8 for Pacific. These offsets are valid throughout the year. The DMP panel automatically adjusts for Daylight Saving Time.

6. To assign an event to the panel, select the **Panel Event Type** (such as "AC Power"), the **State** that will activate the event (such as "Trouble"), and the **Event** name (such as "Intrusion panel power fail"). To enable the event, select the **Enabled** check box.
7. To assign events to individual areas, zones, 24-hour zones, and outputs associated with the panel, do any or all of the following:
 - After selecting an area on the **Areas** tab, select the **Area Event Type**, the status **State** that will activate the event, and the **Event** name. Repeat this step for any of the area's zones to which you want to assign an event.

- After selecting a zone on the **24-hour Zones** tab, select the **Zone Event Type**, the status **State** that will activate the event, and the **Event** name.
- After selecting an output on the **Outputs** tab, select the **Output Event Type**, the status **State** that will activate the event, and the **Event** name.

Be sure to select the **Enabled** check box for each event you want to enable. To delete an assigned event, click its **Delete** icon.

8. Click **Save**.
9. To delete a panel, select it and click the **Delete** button.

IMPORTANT: If a DMP intrusion panel's communication link to the central station is in error, the panel will stop sending messages to the controller. If this happens, consult the panel programming guide for instructions on changing the communication path settings.

NOTE: To control specific operations of a DMP intrusion panel, you can create events that perform actions on the panel when they are activated. For example, you can create an event that disarms an area associated with the panel when there is a valid card read at a specific portal. For information on the available actions for creating such an event, see [Available Actions for Events](#).

See also: [Setting Up the Network Controller](#)

[Setting Up Events](#)

[The DMP Intrusion Panel Widget](#)

[DMP Intrusion Panel Integration \(PDF\)](#)

Output Setup

Setting Up Outputs

Select **Configuration : Alarms : Outputs**.

With this page you can:

- Add outputs to the system.
- Enable or disable the outputs.
- View all of the places in the system where an output is used.
- Edit and delete outputs.

NOTE: You cannot delete an output that is in use anywhere in the system. The **Used By** list will indicate all of the resources that currently use an output. Outputs can be used by output groups, portals, alarm panels, elevators, inputs, event actions, and temperature inputs.

Before you can complete the definition of [output groups](#), or [portals](#) you must configure the individual output devices.

To add an output to the system:

1. Enter a descriptive **Name** for the output, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the output that explains its use.
3. Select the **Enabled** check box to the right of the **Name** field.
4. From the **Network Node** drop-down list, select the node to which this output is wired.
5. From the **Expansion Slot** drop-down list, select the [slot number](#) of the board to which the output is connected.
6. From the **Position** drop-down list, select the connector [position number](#) to which the output is connected.
7. From the **Default State Code** drop-down list, select the normal state for this output: either **Energized** or **Not Energized**.
Your selection will depend on how the output device has been wired and on the type of lock you are using (fail-safe or fail-secure).
8. Click **Save**.

To edit or delete an output:

1. Select an existing output from the **Name** drop-down list.
2. Edit any part of the input definition.
3. Click **Save**.
4. To delete the output, click **Delete**.
If the output is not currently used by any output group, portal, alarm panel, elevator, input, event action, or temperature input, it will be removed from the system.

See also: [Slot and Position Numbers](#)

[Creating Output Groups](#)

[Creating Floor Groups](#)

Creating Output Groups

Select **Configuration : Alarms : Output Groups**.

With this page you can create, edit, and delete output groups. The outputs in an output group will be activated during the time period defined by the group's Auto-activate Time spec.

When an output group is assigned to an [event action](#), its outputs will be pulsed automatically whenever the event is activated.

NOTE: Do not use an output group's Auto-activate Time spec to set an unlock time for a portal. Instead, include the portal in a [portal group](#) and select an Unlock Timespec for that portal group.

To add an output group to the system:

1. Enter a descriptive name for the output group, or click the **add** link and then enter the name.

2. Optionally, enter a **Description** for the output group that explains its use.
3. From the **Auto-activate Time spec** drop-down list, select a time spec or time spec group. The outputs in this group will be activated during the times defined by the selected time spec or time spec group.
For example, you might want to assign a time spec covering 8 PM through 6 AM to an output group that controls a building's exterior lighting. Outputs in the group can still be activated at other times if they are assigned to event actions or are configured as following outputs for [alarm inputs](#).
4. From the **Threat Level Group** drop-down list, you can select a threat level group to associate with this output group. This output group will activate only when the current system threat level is included in the selected threat level group.
5. For each output you want to add to this group, select it in the **Available** list and click the right-arrow button to move it to the **Selected** list.
6. Click **Save**.

To edit an output group:

1. Select an existing output group from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this output group.
2. Edit any part of the output group definition.
3. Click **Save**.

To delete an output group:

1. Select an existing output group from the **Name** drop-down list.
2. Click **Delete**.

See also: [Setting up Outputs](#)

[Creating Time Specs](#)

[Setting Up Threat Level Groups](#)

[How Groups are Used in the System](#)

Video

Select **Configuration : Video** to display the following options.

Choose this	To see information on
Camera Definitions	Changing the general settings for a camera including DNS name, camera type, IP information, username and password.
Camera Groups	Specifying groups of cameras for use in user roles.
Camera Menu Order	Setting the order of cameras in menus and lists.
Camera Presets	Configuring in the security management system the preset positions already defined at each camera web site.

Camera Types	Setting up the URLs for each camera used to control the pan, tilt, zoom, preset and brightness features.
Camera Views	Creating, changing, renaming, and deleting multi-camera views.
Camera Tours	Creating, changing, renaming, and deleting camera tour groups.
Configure NetVR Appliance	Setting up and maintaining the integration of NetVR servers.
Configure NVRs	Setting up and maintaining third-party video management systems.
Magic Monitors	Setting up communication to a Magic Monitor, allowing users to configure event actions that push NetVR camera streams and Magic Views to Magic Monitors and Magic Monitor groups.
Magic Monitor Groups	Creating Magic Monitor groups, which users who are defining event actions can select as targets to push NetVR camera streams and Magic Views to multiple Magic Monitors.
NetVR Appliances	Entering configuration information for NetVR appliances.

See also: [Monitoring Cameras](#)

[Monitoring NetVR Cameras](#)

[Monitoring Multi-Camera Views](#)

[Monitoring NetVR Multi-Camera Views](#)

[Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Updating an NVR Integration](#)

Creating Camera Definitions

Select **Configuration : Video : Camera Definitions**.

On this page you can:

- Create, change, rename, or delete camera definitions.
- See definitions of all cameras currently defined in the system.

All networked cameras used in the system (except NetVR cameras, which are configured using the NetVR Setup Tool) must be defined in the software using this page. All fields are required.

NOTE: Cameras connected to the DVR are defined using the DVR web site. Those cameras should not be defined here.

To complete the creation of camera definitions the network administrator will have to provide an **IP Address** and **DNS Name**, and assign an **IP Port** to the camera.

NOTE: If the **Camera Type** drop-down list does not contain your camera type, you will need to [create this camera type](#) and then return to this page.

To add a camera definition to the system:

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for the camera in the **Name** text box, such as "Parking garage."
3. **Browser Address:** Enter the address used for the video feed. You can enter this as a DNS name or as an IP address. A DNS name is preferred if the camera and the Network Controller are on different sides of a firewall.
4. **Control Address:** Enter the address used for camera control signals such as Zoom or Move Left. You can enter this as a DNS name or as an IP address. A DNS name is preferred if the camera and the Network Controller are on different sides of a firewall.
5. **IP Port:** Enter the port number set up for the camera. Get this number from the network administrator.
6. **Admin Username/Password:** If PTZ controls are password-protected for this camera, enter the username and password specified during the camera setup. These credentials are used for the use of PTZ controls only.
7. Select from the **Camera Type** drop-down list the correct camera type for this camera.
8. Click **Save**.

To delete a camera definition from the system:

1. Select from the **Name** drop-down list the camera you wish to delete.
2. Click **Delete**.

To change a camera definition:

1. Select from the **Name** drop-down list the camera definition you wish to edit.
2. Make any necessary changes in the other fields.
3. Click **Save**.

To rename a camera:

1. Select from the **Name** drop-down list the camera you wish to rename.
2. Click the **rename** link just under the **Name** drop-down list.
3. Edit the camera name.
4. Click **Save**.

See also: [Setting Up Camera Types](#)

[Creating Camera Groups](#)

[Setting Up Camera Tours](#)

[Setup : Cameras Menu](#)

Creating Camera Groups

Select **Configuration : Video : Camera Groups**.

With this page you can create, change, rename, and delete camera groups. These groups are for use in specifying user roles and defining collections of cameras on the NetVR Forensic Desktop.

To create a camera group:

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for the camera group in the **Name** text box.
3. In the **Cameras Available** list, select a specific camera needed for this group.
4. Click the right arrow button to move the selected camera from the **Available** list to the **Selected** list. Repeat this process until all cameras needed for this group appear in the **Selected** list.
5. Click **Save**.

To delete a camera group:

1. Select from the **Name** drop-down list the camera group you want to delete.
2. Click **Delete**.

See also: [Creating Custom User Roles](#)

[Setting Up Camera Types](#)

[Setting Up Multi-Camera Views](#)

[Setting Up Video Recording](#)

[Setting Up Camera Tours](#)

[How Groups are Used in the System](#)



Setting the Camera Menu Order


Select **Configuration : Video : Camera Menu Order**.

With this page you can change the order in which cameras are listed in the UI. By default, the cameras appear in the order they were added to the system.

NOTE: The first two cameras in the menu order are displayed by default in the camera monitors on the [Monitoring Desktop](#).

To change the camera order:

1. Click a camera in the list to select it.
2. Click the **Move up** or **Move down** arrow to move the selected camera up or down in the list.
3. To display the list in alphabetical or reverse alphabetical order, click the button labeled  or , respectively.

4. To return to the default sorting order, click the button labeled .
5. Click **Save**.

See also: [Monitoring Cameras](#)

Creating Camera Preset Positions

Select **Configuration : Video : Camera Presets**.

With this page you can:

- Create, change, or delete camera preset positions in the system.
- Save changes to camera preset positions to the camera website.

Camera preset positions must first be set at each camera web site. See the camera manufacturer's documentation for how to set presets for your camera.

For setting up camera presets in the system you will need to enter the preset **Name** and **Preset Number** exactly as it is entered on the camera's web site.

To add a camera preset position to the system:

1. Click the **add** link just under the **Name** drop-down list.
2. Select from the **Cameras** drop-down list the camera for which you want to create a preset.
3. Enter in the **Name** text box the exact name for this preset position that was entered on the camera's web site.
4. If this is the home position place a check in the **Home Preset?** checkbox.
5. Enter in the **Preset Number** text box the exact number for this preset position that was entered on the camera's web site.
6. Click **Save**.

To save position changes to camera websites:

1. Select from the **Name** drop-down list a camera preset position. The **Camera** text box will have the name of the camera with the selected preset position.
2. The current image from that camera will display in the camera view. Use the camera movement controls beneath the camera image to alter the selected camera preset position.



Click an arrow to move the camera one step in that direction.

Click (+) to zoom in.

Click (-) to zoom out.

3. Click **Save to Camera**.

See also: [Monitoring Cameras](#)

[Monitoring Multi-Camera Views](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

[Creating Camera Definitions](#)

[Setting Up Camera Types](#)

Setting Up Camera Tours

Select **Configuration : Video : Tours**.

With this page you can create, change, rename, or delete camera tour groups for cycling through views in a selected window. You can select any combination of NetVR cameras.

These tours will be available from the [Monitoring Desktop](#) or from **Monitor : Camera Views** or from any NetVR camera view widget.

These camera tour groups are selected from the **Tour** drop-down menu, opened by clicking on the camera name in any NetVR camera viewer title bar.

To create a camera tour:

1. Click the **add** link under the **Name** drop-down list
2. Enter a name for the camera tour in the **Name** text box .
3. Enter a **Description** of the camera tour you are creating.
4. Enter a **Dwell time** for the number of seconds each camera is displayed in the sequence.
5. Select from the **Cameras Available** list a camera you want to include in the tour. You can select any combination of NetVR cameras.
6. Click the right arrow button to move the selected camera to the **Selected** list.
7. Continue moving cameras to the **Selected** list until you have all the cameras needed for your tour.
8. You can change the positions of cameras in the **Selected** list by selecting a camera and clicking the **Move up** or **Move down** arrow. This determines each camera's order in the tour.
9. Click **Save**.

To delete a camera tour:

1. Select from the **Name** drop-down list the tour you wish to delete.
2. Click **Delete**.

To rename a camera tour:

1. Select from the **Name** drop-down list the tour you wish to rename.
2. Click the **rename** link under the **Name** drop-down list.
3. Edit the name.
4. Click **Save**.

See also: [Monitoring NetVR Multi-Camera Views](#)

[Creating Camera Definitions](#)

[The Monitoring Desktop](#)

Setting Up Camera Types

Select **Configuration : Video : Camera Types**.

With this page you can add, delete, and rename camera types, and edit camera type URLs.

The system has been tested with the following camera types although most standard IP cameras should work:

- Axis 2120, 232D
- Axis 205, 206
- IQinVision (various IQeye models)
- Panasonic WV-NM100
- Panasonic WV NS324
- Sony SNC-DF40N/DF40P
- Sony SNC-P1
- Sony SNC-RZ30N
- Vivotek IP2111

NOTE: Both the Axis and Vivotek camera types support active images using Motion JPEGs. Motion JPEGs provide smoother motion but require up to 5 megabits per second of network bandwidth. We recommend that Motion JPEGs not be used on 10 megabit networks or over remote (DSL, WAN) connections.

Axis and Vivotek camera types both default to the use of Motion JPEGs. To stop the use of Motion JPEGs and force these camera types to use standard JPEG images delete the Motion JPEG URL from the **Motion JPEG URL** text box and click **Save**. This will significantly reduce network bandwidth usage.

Motion JPEGs are supported by the Mozilla Firefox browser.

Motion JPEGs are **not** supported in Internet Explorer.

To add a camera type:

1. Click the **add** link just under the **Name** drop-down list.
2. Enter the new camera type in the **Name** textbox.
3. The camera's web site has URLs for pan, tilt, zoom, preset, and brightness functions. Enter these URLs into the appropriate URL text boxes. See the camera manufacturer documentation for these exact URLs.
4. Click **Save**.

See also: [Creating Camera Definitions](#)

Setting Up Multi-Camera Views

Select **Configuration : Video : Camera Views**.

With this page you can create, change, rename, or delete camera views of multiple cameras. These views will be available from the [Monitoring Desktop](#) or from **Monitor : Camera Views**.

To create a camera view:

1. Click the **add** link under the **Name** drop-down list
2. In the **Name** text box enter a name for the camera view you are creating.
3. Select from the **View Type** drop-down list the type of view you want to create.
4. Select from the **Cameras Available** list a camera you want to include in the view. You can select IP cameras and/or DVR cameras, depending on your system.
For a NetVR system, you can select NetVR cameras.
5. Click the right arrow button to move the selected camera to the **Selected** list.
6. Continue moving cameras to the **Selected** list until you have all the cameras needed for your view. For a **Quadview** you can select up to four cameras.
For a **NetVR 2x2** view you can choose up to four NetVR cameras; for a **NetVR 1+7** view you can choose up to eight NetVR cameras.
7. You can change the positions of cameras in the **Selected** list by selecting a camera and clicking the **Move up** or **Move down** arrow. This determines each camera's placement in the view.

Cameras are placed in a view from left to right starting with the top row. For a **Quadview**, the first camera in the view list is in the upper left position, the second camera is in the upper right, the third camera is in the lower left, and the fourth camera is in the lower right position.

For a **NetVR 2x2** view, the first camera in the list is in the upper left position (Spot Monitor), the second camera is in the upper right, the third camera is in the lower left, and the fourth camera is in the lower right position (see figure).

For a **NetVR 1+7** view, the first camera in the list is in the upper left main window (Spot Monitor), camera 2 is in the upper right with 3 and 4 below that, cameras 5 through 8 are left-to-right across the bottom of the layout (see figure).



8. Click **Save**.

To delete a camera view:

1. Select from the **Name** drop-down list the view you wish to delete.
2. Click **Delete**.

To rename a camera view:

1. Select from the **Name** drop-down list the view you wish to rename.
2. Click the **rename** link under the **Name** drop-down list.
3. Edit the name.
4. Click **Save**.

See also: [Monitoring Multi-Camera Views](#)

[Monitoring NetVR Multi-Camera Views](#)

[Creating Camera Definitions](#)

[The Monitoring Desktop](#)

NetVR Appliances

Configuring a NetVR Appliance

Select **Configuration : Video : NetVR Appliances**.

For a more complete treatment of this topic, see the [NetVR Setup and Configuration Guide \(PDF\)](#).

On this page you can add a NetVR appliance to the system.

NOTE: Click the **Install NetVR Setup Tool** link on this page to download, install, and open the NetVR setup and configuration application.

To set up a NetVR embedded appliance:

1. The **NetVR IP Address** for the appliance is displayed as an internal connection between the controller and the embedded NetVR appliance.
2. Use your custom login or the default entries in the **NetVR Username** and **NetVR Password** fields with the secure login name and password you entered when configuring the appliance.

NOTE: The username and password you enter here must exactly match the username and password you entered when you configured the NetVR appliance through the NetVR Setup Tool. The name and password are case sensitive.

3. Click **Check connection**.

In the **Discovered Information** section that appears, the serial number, vendor, model, and camera count are filled in automatically.

4. Click **Save**.

5. In the **Discovered Information** section, click the **List VMS Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NetVR appliance through its own web interface.
6. To rename the NetVR appliance, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

To set up the NetVR freestanding appliance:

NOTE 1: Before configuring the NetVR appliance on the network controller, ensure that the appliance and cameras have been set up and verified through the NetVR Client, installed by using the **NetVR Setup Tool**.

NOTE 2: We recommend the use of a static IP address for a NetVR appliance. If the IP address of the appliance changes, the connection between it and the network controller will be lost. The static IP address must be set using the NetVR Client / System Setup / Network Tab.

NOTE 3: Using live streaming video consumes considerable network bandwidth.

1. Enter the **NetVR IP Address** for the appliance.
2. Replace the default entries in the **NetVR Username** and **NetVR Password** fields with the secure login name and password you entered when configuring the appliance.

NOTE: The username and password you enter here must exactly match the username and password you entered when you configured the NetVR appliance through its own web interface. The name and password are case sensitive.

3. Click **Check connection**.

In the **Discovered Information** section that appears, the serial number, vendor, model, and camera count are filled in automatically.

4. Click **Save**.
5. In the **Discovered Information** section, click the **List VMS Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NetVR appliance through its own web interface.
6. To rename the NetVR appliance, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

To configure public settings:

1. **NetVR Public IP Address:** This IP address fills in automatically when you save a new NetVR appliance configuration.

NOTE: If this address is on another subnet or behind a firewall, you may have to change this to the external public address of the router or firewall. The network administrator will have to set up the port translation for communications and video to and from this address.

2. **NetVR Public Service Port:** This port number defaults to 80.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. Click **Save**.

See also: [Setting Up Virtual Inputs for VMS Cameras](#)

[Updating an NVR Integration](#)

[Changing the Default IP Address for a NetVR System \(PDF\)](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

[Setting Up Multi-Camera Views](#)

[Setting Up Camera Tours](#)

[Configuring the NetVR Web Service \(PDF\)](#)

Setting the Network Connection for a NetVR Appliance

Following the NetVR hardware setup, while the NetVR appliance is still connected directly to a local PC or laptop (not on the corporate network), you can set the network connection.

To set the network connection for a NetVR appliance:

1. Set the local PC or laptop to a static IP address of 192.168.0.X (where X is a number other than 251, 250, and 249).
2. Set the Subnet Mask to **255.255.255.0**.
3. Set the Gateway to **192.168.0.1**.
4. Browse to the NetVR at 192.168.0.249.
The Software License page opens.
5. Accept the terms and click **Apply**.
6. Log in:
 - Enter the username: **admin**.
 - Enter and confirm the password: **admin**.
7. On the S2 NetVR Downloads page, download, install, and open the S2 NetVR Setup Tool.
8. Select **Add System** in the menu and do the following:
 - Click **New**.
 - Enter the default NetVR IP address: **192.168.0.249**.
 - Enter the username: **admin**.
 - Enter and confirm the password: **admin**.
 - Click **Apply**.

The screen indicates "Connected" when the NetVR server has been added.

9. Select **System Setup** and click the **Network** tab.
 - Enter your preferred **IP address** and **Netmask** for the NetVR server.

- Enter the **Gateway** and, optionally, the **Primary DNS**.
 - Click **Apply**.
10. Set the PC or laptop back to an IP address on your network.
 11. Browse to NetVR at the new NetVR server IP address.
 12. Return to the NetVR Setup Tool's Add System page to register the new IP address.
 13. On the **Users** menu, create a new Admin password (recommended) to use for logging in to NetVR.
 14. Use the NetVR Setup Tool to configure cameras and the NetVR appliance.
See [Configuring a NetVR Appliance](#) and the [NetVR Setup and Configuration Guide \(PDF\)](#) for detailed camera setup and configuration instructions.

See also: [Beginning a Forensic Search](#)

[Using the Forensic Desktop Activity Log](#)

[Using the Forensic Desktop Video Player](#)

[Creating and Saving Clips](#)

[Using the Forensic Desktop Timeline](#)

[Composing Forensic Cases](#)

[Printing and Exporting Forensic Cases](#)

[Accessing Recorded Video from a Person Record](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

NVRs/DVRs

Select **Configuration : Video: Configure NVRs** to display the following options.

Choose this	To see information on
Configure Avigilon NVR	Setting up and maintaining the integration of Avigilon NVRs.
Configure Cisco VSM	Setting up and maintaining the integration of Cisco Video Surveillance Managers.
Configure exacqVision NVR	Setting up and maintaining the integration of exacqVision NVRs.
Configure Milestone Systems NVR	Setting up and maintaining the integration of Milestone Systems NVRs.

Configure OnSSI NVR	Setting up and maintaining the integration of OnSSI NVRs.
Configure Salient CompleteView NVR	Setting up and maintaining the integration of Salient Systems CompleteView NVRs.
Configure ViconNet Nucleus	Setting up and maintaining the integration of ViconNet video.
Configure Video Insight NVR	Setting up and maintaining the integration of Video Insight NVRs.

See also: [Avigilon NVR Integration Guide \(PDF\)](#)

[Cisco Video Surveillance Manager Setup and Integration Guide \(PDF\)](#)

[exacqVision \(v5.10 and 6.0\) NVR Integration Guide \(PDF\)](#)

[exacqVision \(v4.5\) NVR Integration Guide \(PDF\)](#)

[exacqVision \(v3.6\) NVR Integration Guide \(PDF\)](#)

[Milestone XProtect Enterprise/Professional 2014 \(v8.6d\) NVR Integration Guide \(Release 4.7\)](#)

[Milestone XProtect Enterprise/Professional \(v7.0b/c/d, 8.0/8.1a\) NVR Integration Guide \(PDF\) \(Release 4.5\)](#)

[Milestone XProtect Enterprise/Professional \(v7.0b/c/d, 8.0\) NVR Integration Guide \(PDF\) \(up to Release 4.4\)](#)

[Milestone XProtect Corporate 2014 \(v7.0c/d\) NVR Integration Guide \(Release 4.8\)](#)

[Milestone XProtect Corporate \(v3.1a/4.0a/4.1a/5.0a\) NVR Integration Guide \(PDF\) \(Release 4.5\)](#)

[Milestone XProtect Corporate \(v3.1a/4.0a/4.1a/5.0a\) NVR Integration Guide \(up to Release 4.4\)](#)

[Milestone Systems \(v6.5\) NVR Integration Guide \(PDF\)](#)

[NetBox VR/NetVR Setup and Configuration Guide \(PDF\)](#)

[OnSSI Ocularis CS/IS \(2.0\) NVR Integration Guide \(PDF\) \(Release 4.4\)](#)

[OnSSI Ocularis CS/IS \(2.0\) NVR Integration Guide \(PDF\) \(up to Release 4.3\)](#)

[OnSSI NetDVMS \(6.5\) NVR Integration Guide \(Release 4.4\)](#)

[OnSSI NetDVMS \(6.5\) NVR Integration Guide \(up to Release 4.3\)](#)

[Salient Systems NVR Integration Guide \(PDF\)](#)

[Video Insight NVR Integration Guide \(PDF\)](#)

[Updating an NVR Integration](#)

Updating an NVR Integration

Whenever you make changes to the cameras configured for your NVR integration, such as adding and removing cameras or defining new presets, you will need to update the integration. This ensures that the controller has up-to-date camera information.

To update your NVR integration:

1. Select **Configuration : Video : Configure NVRs : Configure <your NVR>**.
2. Click the **Check Connection** button.
3. If the system prompts you to update the NVR integration because it has detected changes, click **OK**.
If the system does not detect changes, it will indicate that the NVR is accessible.
4. Once the system indicates that it has successfully merged the new configuration with the old one, click **Save** to save the changes to the integration.

See also: [Setting Up Virtual Inputs for VMS Cameras](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

[Setting Up Multi-Camera Views](#)

Configuring an Avigilon NVR

Select **Configuration : Video : Configure NVRs : Configure Avigilon NVR**.

For a more complete treatment of this topic, see the [Avigilon NVR Integration Guide \(PDF\)](#).

With this page you can add an Avigilon NVR to the system.

NOTE 1: Before configuring the video management system on the network controller, ensure that the NVR and cameras have been set up and verified through the NVR's interface.

NOTE 2: We strongly recommend the use of a static IP address for the NVR. If the IP address of the NVR changes, the connection between the NVR and the network controller will be lost. The static IP address must be set using the NVR's own web interface.

NOTE 3: Using live streaming video consumes considerable network bandwidth.

To set up the Avigilon NVR:

1. Enter the IP address of the NVR into the **Avigilon IP Address** field.
2. Accept the default of **8080** for the **Avigilon Port** number, or enter a port number provided by your network administrator.
3. Replace the default entries in the **Avigilon Username** and **Avigilon Password** fields with the secure username and password you created on the Avigilon Server for the user associated with the security management system.

NOTE: The username and password you enter here must exactly match the username and password you created on the Avigilon server. The name and password are case sensitive.

4. Click **Check Connection**.

In the **Discovered Information** section that appears, the serial number and camera count are filled in automatically.

5. Click **Save**.
6. In the **Discovered Information** section, click the **List NVR Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NVR through its own interface.
7. To rename the NVR, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

To configure public settings:

1. **Public IP Address:** This IP address fills in automatically when you save a new NVR configuration.

NOTE: If this address is on another subnet or behind a firewall, you may have to change this to the external public address of the router or firewall. The network administrator will have to set up the port translation for communications and video to and from this address.

2. **Public HTTP port:** This port number defaults to 80.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. Click **Save**.

See also: [Avigilon NVR Integration Guide \(PDF\)](#)

[Updating an NVR Integration](#)

[Setting Up Virtual Inputs for VMS Cameras](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

Configuring a Cisco VSM

Select **Configuration : Video : Configure NVRs : Configure Cisco VSM**.

With this page you can add a Cisco Video Surveillance Manager (VSM) to the security management system.

Note the following:

- Before configuring the VSM on the controller, ensure that the VSM Operations Manager and all cameras to be used for the integration have been set up, and that the cameras have been verified through the Operations Manager's own web interface.

- We strongly recommend the use of a static IP address for the VSM Operations Manager. If the IP address of the Operations Manager changes, its connection to the S2 controller will be lost. The static IP address must be set using the Operations Manager's own web interface.
- Using live streaming video consumes considerable network bandwidth.

For information on setting up a Cisco VSM integration, see the [Cisco Video Surveillance Manager Setup and Integration Guide \(PDF\)](#).

To point the controller to the Cisco VSM Operations Manager:

1. Enter the static IP address of the Cisco VSM Operations Manager into the **Cisco VSM IP Address** field.
2. Replace the default entries in the **Cisco VSM Username** and **Cisco VSM Password** fields with the secure username and password you created on the VSM Server for the user associated with the security management system.
The username and password you enter here must exactly match the username and password you created on the VSM server. The name and password are case sensitive.
3. Click **Check Connection**.

In the **Discovered Information** section that appears, the serial number, vendor, VSM model number, and camera count are filled in automatically.

4. Click **Save**.
5. In the **Discovered Information** section, click the **List NVR Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the VSM through its own web interface.
6. To rename the VSM, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

IMPORTANT: The S2 controller will install a soft trigger named **S2 NetBox Record Trigger** on all camera templates. Do not delete this trigger, which is managed by the S2 controller and is used to trigger an action on a Cisco VSM camera.

To configure public settings:

1. **Public IP Address:** This IP address fills in automatically when you save a new VSM configuration.

If this address is on another subnet or behind a firewall, you may have to change this to the external public address of the router or firewall. The network administrator will have to set up the port translation for communications and video to and from this address.

2. **Public HTTP port:** This port number defaults to 80.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. Click **Save**.

See also: [Cisco Video Surveillance Manager Setup and Integration Guide \(PDF\)](#)

[Creating Camera Definitions](#)

[Setting Up Camera Types](#)

[Setting Up Virtual Inputs for VMS Cameras](#)

[Moving Video Management Systems Between Partitions](#)

Configuring an exacqVision NVR

Select **Configuration : Video : Configure NVRs : Configure exacqVision**.

For a more complete treatment of this topic, see the [exacqVision \(v3.6\) NVR Integration Guide \(PDF\)](#), the [exacqVision \(v4.5\) NVR Integration Guide \(PDF\)](#), or the [exacqVision \(v5.10 and 6.0\) NVR Integration Guide \(PDF\)](#).

With this page you can add an exacqVision NVR to the system.

NOTE 1: Before configuring the video management system on the network controller, ensure that the NVR and cameras have been set up and verified through the NVR's own web interface.

NOTE 2: We strongly recommend the use of a static IP address for the NVR. If the IP address of the NVR changes, the connection between the NVR and the network controller will be lost. The static IP address must be set using the NVR's own web interface.

NOTE 3: Using live streaming video consumes considerable network bandwidth.

To set up the exacqVision NVR:

1. Enter the IP address of the NVR into the **exacqVision IP Address** field.
2. Replace the default entries in the **exacqVision Username** and **exacqVision Password** fields with the secure username and password you created on the exacqVision Server for the user associated with the security management system.

NOTE: The username and password you enter here must exactly match the username and password you created on the exacqVision server. The name and password are case sensitive.

3. Click **Check Connection**.

In the **Discovered Information** section that appears, the serial number and camera count are filled in automatically.

4. Click **Save**.
5. In the **Discovered Information** section, click the **List NVR Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NVR through its own web interface.
6. To rename the NVR, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

To configure public settings:

1. **Public IP Address:** This IP address fills in automatically when you save a new NVR configuration.

NOTE: If this address is on another subnet or behind a firewall, you may have to change this to the external public address of the router or firewall. The network administrator will have to set up the port translation for communications and video to and from this address.

2. **Public HTTP port:** This port number defaults to 80.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. Click **Save**.

See also: [exacqVision \(v5.10 and 6.0\) NVR Integration Guide \(PDF\)](#)

[exacqVision \(v4.5\) NVR Integration Guide \(PDF\)](#)

[exacqVision \(v3.6\) NVR Integration Guide \(PDF\)](#)

[Updating an NVR Integration](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Virtual Inputs for VMS Cameras](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

Configuring a Milestone Systems NVR

Select **Configuration : Video : Configure NVRs : Configure Milestone Systems NVR**.

For a more complete treatment of this topic, see the *Setup and Integration Guide* for your Milestone system. Links to the Milestone guides are available in Guides and Technical Notes.

With this page you can add a Milestone Systems video management system (referred to as an NVR below, for the sake of brevity) to the security management system.

NOTES: Before configuring the NVR on the network controller, ensure that the NVR and cameras have been set up and verified through the NVR's own web interface.

We strongly recommend the use of a static IP address for the NVR. If the IP address of the NVR changes, the connection between the NVR and the network controller will be lost. The static IP address must be set using the NVR's own web interface.

If you plan to move the NVR to a new partition, be sure to move it BEFORE configuring its cameras, assigning its cameras to camera views or floorplans, or either linking its cameras to events or using them in event actions.

Using live streaming video consumes considerable network bandwidth.

To set up the Milestone Systems NVR:

1. Enter the IP address of the NVR into the **NVR IP Address** field.
2. Replace the default entries in the **Engine Username** and **Engine Password** fields with the secure login name and password you entered when configuring the Milestone XProtect Central settings in the Milestone system. These fields are not used in Milestone XProtect Corporate 2014 integrations.

The username and password you enter here must exactly match the username and password you entered in the Milestone system. The name and password are case sensitive.

3. Replace the default entries in the **Image Server Username** and **Image Server Password** fields with the secure username and password you entered when you created a security management system user account in the Milestone system.

NOTE: The username and password you enter here must exactly match the username and password you entered in the Milestone system. The name and password are case sensitive.

4. The **Image Server Port** defaults to 80. If you change this in the Milestone System, you will need to change it here.
5. The **Engine Listener Port** defaults to 1237. We recommend that you do not change the default. This field is not used in Milestone XProtect Corporate 2014 integrations.
6. The **Event Trigger Port** defaults to 1234. We recommend that you do not change this default.
7. Click **Check Connection**.

In the **Discovered Information** section that appears, the serial number and camera count are filled in automatically.

8. Click **Save**.
9. In the **Discovered Information** section, click the **List VMS Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NVR through its own web interface.

For Milestone XProtect Corporate integrations, each camera name is listed with the name of the associated XProtect Corporate Recording Server.

10. To rename the NVR, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

IMPORTANT: In a partitioned system, the Video Servers table on the [Partitions page](#) will display multiple entries for a Milestone XProtect Corporate NVR: one for the management server and another for each of its associated recording servers.

If you plan to move the management server and/or its recording servers [to different partitions](#), be sure to move them BEFORE configuring the associated cameras. If any camera has associations with virtual inputs, camera views, floorplans, or events, you will not be able to move the camera to a different partition until you remove these associations.

To configure public settings:

1. **Public IP Address:** This IP address fills in automatically when you save a new NVR configuration.

NOTE: If this address is on another subnet or behind a firewall, you may have to change this to the external public address of the router or firewall. The network administrator will have to set up the port translation for communications and video to and from this address.

2. **Public HTTP port:** This port number defaults to 80.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. Click **Save**.

See also: [Setting Up Virtual Inputs for VMS Cameras](#)

[Updating an NVR Integration](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

[Setting Up Multi-Camera Views](#)

[Milestone XProtect Enterprise/Professional 2014 \(v8.6d\) NVR Integration Guide](#) (Release 4.7)

[Milestone XProtect Corporate 2014 \(v7.0c/d\) NVR Integration Guide](#) (Release 4.8)

Configuring an OnSSI NVR

Select **Configuration : Video : Configure NVRs : Configure OnSSI NVR**.

For a more complete treatment of this topic, see the *Setup and Integration Guide* for your OnSSI system. Links to the OnSSI guides are available in Guides and Technical Notes.

With this page you can add an OnSSI NVR to the system.

NOTE 1: Before configuring the video management system on the network controller, ensure that the NVR and cameras have been set up and verified through the NVR's own web interface.

NOTE 2: We strongly recommend the use of a static IP address for the NVR. If the IP address of the NVR changes, the connection between the NVR and the network controller will be lost. The static IP address must be set using the NVR's own web interface.

NOTE 3: Using live streaming video consumes considerable network bandwidth.

To set up the OnSSI NVR:

1. Enter the IP address of the NVR into the **NVR IP Address** field.
2. Replace the default entries in the **Engine Username** and **Engine Password** fields with the secure username and password you established for the security management system in the NetDVMS Administrator.

NOTE: The username and password you enter here must exactly match the username and password you established in the NetDVMS Administrator. The name and password are case sensitive.

3. Replace the default entries in the **Image Server Username** and **Image Server Password** fields with the secure username and password you established for the security management system in the Image Server Administrator.

NOTE: The username and password you enter here must exactly match the username and password you established in the Image Server Administrator. The name and password are case sensitive.

4. The **Image Server Port** field defaults to 80. If you change this in the OnSSI system you will need to change it here.
5. The **Engine Listener Port** defaults to 1237. We recommend that you do not change this default.
6. The **Event Trigger Port** defaults to 1234. We recommend that you do not change this default.
7. Click **Check Connection**.
In the **Discovered Information** section that appears, the serial number and camera count are filled in automatically.
8. Click **Save**.
9. In the **Discovered Information** section, click the **List VMS Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NVR through its own web interface.
10. To rename the NVR, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

To configure public settings:

1. **Public IP Address:** This IP address fills in automatically when you save a new NVR configuration.
NOTE: If this address is on another subnet or behind a firewall, you may have to change it to the external public address of the router or firewall. The network administrator will have to set up the port translation for communications and video to and from this address.
2. **Public HTTP port:** This port number defaults to 80.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.
Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.
4. Click **Save**.

See also: [OnSSI Ocularis CS/IS \(2.0\) NVR Integration Guide \(PDF\)](#) (Release 4.4)

[OnSSI NetDVMS \(6.5\) NVR Integration Guide](#) (Release 4.4)

[Updating an NVR Integration](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Virtual Inputs for VMS Cameras](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

[Setting Up Multi-Camera Views](#)

Configuring a Salient Systems CompleteView NVR

Select **Configuration : Video : Configure NVRs : Configure Salient CompleteView NVR**.

With this page you can add a Salient Systems CompleteView™ NVR to the system.

NOTE 1: Before configuring the NVR on the network controller, ensure that the NVR and cameras have been set up and verified through the NVR's own web interface.

NOTE 2: We strongly recommend the use of a static IP address for the NVR. If the IP address of the NVR changes, the connection between the NVR and the network controller will be lost. The static IP address must be set using the NVR's own web interface.

NOTE 3: Using live streaming video consumes considerable network bandwidth.

To set up the Salient CompleteView NVR:

1. Enter the IP address or hostname of the CompleteView server into the **NVR IP Address** field.
2. Replace the default entries in the **Engine Username** and **Engine Password** fields with the secure login name and password of the administrator account with API Access configured on the CompleteView recording server.

NOTE: The username and password you enter here must exactly match the username and password you entered in the Salient system. The name and password are case sensitive.
3. The **Image Server Port** defaults to 80. If you change this in the Salient system, you will need to change it here.
4. The **Engine Listener Port** defaults to 1237. We recommend that you do not change this default.
5. The **Event Trigger Port** defaults to 1234. We recommend that you do not change this default.
6. Click **Check Connection**.
7. The Discovered Information section appears. Click **List NVR Cameras** and verify that the cameras set up on the CompleteView server are available.
8. Click **Save**.

The Settings section appears. If the CompleteView server is on another subnet or behind a firewall, you may need to change this information to the "public" IP and port information, or the IP and port number accessible from the security management system.

9. Optionally, change the setting for **Combine VMD events arriving within seconds**. Video Motion events arriving within the specified number of seconds will be combined into one network controller event.

To verify live video from the security management system:

1. Select **Monitor : Cameras**.
2. Select a camera that is connected to the CompleteView server.
3. Download the Salient Active X control when prompted. This is required.
4. Verify that you can see live video from this CompleteView-connected camera.

See also: [Setting Up Virtual Inputs for VMS Cameras](#)

[Salient Systems NVR Integration Guide \(PDF\)](#)

[Updating an NVR Integration](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

[Setting Up Multi-Camera Views](#)

Configuring a ViconNet Nucleus

Select **Configuration : Video : Configure NVRs : Configure ViconNet Nucleus**.

For a more complete treatment of this topic, refer to the ViconNet/SMS Integration CD.

With this page you can:

- Establish a connection between a ViconNet Nucleus and the security management system.
- View information discovered about the ViconNet Nucleus, such as its serial number and the number of cameras available from ViconNet.

To configure a ViconNet Nucleus:

1. Enter the IP address of the ViconNet Nucleus.
2. Enter the user name and password for the ViconNet administrator.
3. Click the **Check connection** button to determine whether the ViconNet Nucleus is available for connection with the security management system. If the ViconNet Nucleus is available, establish the connection when prompted.

NOTE: In the **Discovered Information** section that appears, the serial number and camera count are filled in automatically.

4. (optional) Enter a different number in the **Combine VMD events arriving within seconds** field. Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

5. Click the link in the **Discovered Information** section and verify that the list of cameras available from ViconNet is correct and complete.
6. To rename the ViconNet Nucleus, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

NOTE: Any changes you make to the video settings, such as adding or removing cameras, require you to click the **Check connection** button on the **Configure ViconNet Nucleus** page.

See also: [Setting Up Virtual Inputs for VMS Cameras](#)

[Updating an NVR Integration](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Multi-Camera Views](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

Configuring a Video Insight NVR

Select **Configuration : Video : Configure NVRs : Configure Video Insight IP Enterprise Server NVR**.

For a more complete treatment of this topic, see the [Video Insight NVR Integration Guide \(PDF\)](#).

With this page you can add a Video Insight video management system to your security management system.

NOTE 1: Before configuring the video management system on the network controller, ensure that the NVR and cameras have been set up and verified through the NVR's own web interface.

NOTE 2: We strongly recommend the use of a static IP address for the NVR. If the IP address of the NVR changes, the connection between the NVR and the network controller will be lost. The static IP address must be set using the NVR's own web interface.

NOTE 3: Using live streaming video consumes considerable network bandwidth.

To set up the Video Insight NVR:

1. Enter the IP address of the NVR into the **NVR IP Address** field.
2. Click **Check Connection**.
In the **Discovered Information** section that appears, the serial number and camera count are filled in automatically.
3. Click **Save**.
4. In the **Discovered Information** section, click the **List NVR Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NVR through its own web interface.
5. To rename the NVR, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

To configure public settings:

1. **Public IP Address:** This IP address fills in automatically when you save a new NVR configuration.
NOTE: If this address is on another subnet or behind a firewall, you may have to change this to the external public address of the router or firewall. The network administrator will have to set up the port translation for communications and video to and from this address.
2. **Public HTTP port:** This port number defaults to 80.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.
Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.
4. Click **Save**.

See also: [Setting Up Virtual Inputs for VMS Cameras](#)

[Updating an NVR Integration](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

[Setting Up Multi-Camera Views](#)

[Video Insight NVR Integration Guide \(PDF\)](#)

Magic Monitors

Configuring Magic Monitors

Select **Configuration : Video : Magic Monitors**.

Magic Monitor is an application that lets users view surveillance video, forensics, and digital signage content on desktop computers, laptops, and video walls. Users can command video from the S2 system or from S2 Mobile Security Officer.

You can use this page to set up communication to a Magic Monitor. Users will then be able to configure [event actions](#) that push NetVR camera streams and Magic Views to Magic Monitors and Magic Monitor groups.

To configure a Magic Monitor:

1. Enter a **Name** for the Magic Monitor.
2. Enter the **IP Address** of the computer running the S2 system.
3. Enter the Magic Monitor **Username** and **Password**.
4. Click **Check connection**.

If the system discovers the Magic Monitor, it displays a *Connection successful* message.

5. Click **OK** in the message box.
In the **Discovered Information** section, you are presented with lists of Magic Views and cameras on the Magic Monitor.
6. Click **Save**.
7. If you make changes to the set of Magic Views or to the available cameras on the Magic Monitor, you can refresh the list on the controller by clicking **Refresh Views and Cameras** and clicking **Save**.

NOTE: If the Magic Monitor belongs to a group, the **Delete** button will be disabled.

See also: [Configuring Magic Monitor Groups](#)

[Defining Event Actions](#)

[Available Actions for Events](#)

[S2 Mobile Security Officer User Guide](#)

Creating Magic Monitor Groups

Select **Configuration : Video : Magic Monitor Groups**.

On this page you can add a Magic Monitor group to the system. When defining [event actions](#), users will be able to select the group as a target to push a NetVR camera stream or a Magic View to multiple Magic Monitors.

To create a Magic Monitor group:

1. Enter a **Name** for the group and, optionally, a **Description** that explains its use.
2. For each Magic Monitor you want to add to the group, select it in the **Available** list and click the right-arrow button to move it to the **Selected** list.
3. Click **Save**.

See also: [Configuring Magic Monitors](#)

[Defining Event Actions](#)

[Available Actions for Events](#)

Creating Evacuation Plans

Select **Configuration : Evacuation Plans**.

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.

To create an evacuation plan:

1. Enter a descriptive **Plan Name**, or click the **add** link and then enter the name.
2. Optionally, enter a **Description** for the plan that explains its use.
3. For **Mustering Region**, select the region you want to designate as the plan's mustering station for evacuations.
4. To designate the regions to be evacuated under the plan, select them in the Available list and click the right-arrow button to move them to the Selected list.
5. Click **Save Plan**.

The new plan is added to the [Evaluation Start](#) page. Users with administration or setup privileges can use this page to start the plan in response to an emergency or disaster.

See also: [Starting Evacuation Plans](#)

[Ending Evacuation Plans](#)

[Configuring Regional Anti-Passback](#)

[S2 Mobile Security Officer User Guide \(PDF\)](#)

Floorplans

Select **Configuration : Floorplans** to display the following options.

Choose this	To see information on
Floorplan Compose	Placing system resources into a floorplan image.
Floorplan Groups	Specifying groups of floorplans for use in user roles.
Floorplan Upload	Uploading an image of a site floorplan to the network controller in jpeg format.

See also: [Monitoring Floorplans](#)

[Using the Monitoring Desktop](#)

[Using the Widget Desktop](#)

[Creating Custom User Roles](#)

Composing Floorplans

Select **Configuration : Floorplans : Floorplan Compose**.

With this page you can:

- Compose a floorplan and save it in the system.
- Edit an existing floorplan—for example, by changing or deleting its references to existing system resources.
- Link a floorplan to another floorplan.
- Delete a floorplan from the system.

NOTE: Viewing and composing floorplans requires a browser plug-in from Macromedia called Flash Player 9.0 or later.

Because composing floorplans requires referencing existing system resources such as [portals](#), [cameras](#), and [alarm events](#), you should create those resources beforehand. For information on scheduling actions for portals, inputs, and outputs from a floorplan, see [Scheduling Actions for Portals, Inputs, and Outputs](#).

To compose a floorplan:

1. In the **Floorplan** section, select **add new** from the drop-down list.
2. In the **Floorplan Details** section, do the following:
 - a. Enter a name for the floorplan in the **Name** text box. Once you save the floorplan, this name will be added to the drop-down list in the **Floorplan** section so the floorplan can later be viewed and edited.
 - b. From the **Background** drop-down list, select the jpeg image of the floor you want to add.
 - c. To specify a different background color for the floorplan, enter the character code for its RGB values in the **BG Color #** text box.

NOTE: The **Background** drop-down lists all previously uploaded floorplan jpegs. If you need to upload a jpeg file to use as a background, see [Uploading Floorplan Background Images](#).

3. To add a system resource or a link to another floorplan to the jpeg image, do the following:
 - a. In the **Resource** section, select the type of resource you want to add from the **Type** drop-down.
 - b. Move the pointer to the location on the floorplan image where you want to add the resource. The pointer changes to a hand icon.
 - c. Click to add an icon representing the selected resource type to the image. To move the icon, click and drag it to a new location.
 - d. In the **Resource** section, select the name of an existing resource from the **Name** drop-down.

For example, after selecting **Camera** from the **Type** drop-down, click anywhere in the floorplan image to add the following icon to the image, and then give it the name of a camera currently defined in the system.



4. Click **Save Floorplan**.

To edit an existing floorplan:

1. In the **Floorplan** section, select the floorplan you want to change.
2. To rename the floorplan, edit its name in the **Name** text box.

3. To edit any of the system resources, select its icon and do any of the following in the **Resource** section:
 - Change the resource type by selecting a different entry from the **Type** drop-down list.
 - Delete the resource by clicking the **Delete** button. The floorplan turns gray and you must confirm the deletion by clicking **Delete Icons**, which appears on the gray background.
 - Rename the resource by selecting a different name from the **Name** drop-down.
 - Move the resource by clicking and dragging it to a new location.
4. Click **Save Floorplan**.

To delete a floorplan:

1. In the **Floorplan** section, select the name of the floorplan you want to delete.
2. Click **Delete Floorplan**. The floorplan image turns gray and displays a confirmation message.
3. Click **Delete** to confirm the deletion.

NOTE: This deletes the defined floorplan but not the uploaded floorplan jpeg image. The image is still available on the **Background** drop-down list for inclusion in a new floorplan definition.

See also: [Monitoring Floorplans](#)

[Uploading Floorplan Background Images](#)

[Scheduling Actions for Portals, Inputs, and Outputs](#)

[Using the Widget Desktop](#)

Creating Floorplan Groups

Select **Configuration : Floorplans : Floorplan Groups**.

With this page you can create, edit, rename, and delete floorplan groups, which can be used in specifying user roles. When a floorplan group is added to a customer [user role](#), users holding that role will be able to view floorplans in the group.

To create a floorplan group:

1. Click the **add** link under the **Name** field.
2. Enter a **Name** for the new floorplan group and, optionally, a **Description** that explains its use.
3. In the **Floorplans Available** list, select each floorplan you want to include in the group and click the right-arrow button to move it to the **Selected** list.
4. Click **Save**.

To delete a floorplan group:

1. Select an existing floorplan group from the **Name** drop-down list.
2. Click **Delete**.

See also: [Creating Custom User Roles](#)

[Uploading Floorplan Background Images](#)

[Composing, Editing, and Deleting Floorplans](#)

[How Groups are Used in the System](#)

Uploading Floorplan Background Images

Select **Configuration : Floorplans : Floorplan Upload**.

With this page you can upload a jpeg or jpg image to the Network Controller to use as a background image for a floorplan.

NOTE: The maximum size of a floorplan jpeg image is 256K. The upload function enforces this limit.

To upload a floorplan image:

1. Click the **Browse** button.
2. In the **File Upload** dialog browse to the jpeg or jpg file you want to upload, select it and click **Save**.
3. The full path to the file now displays in the **Select file** text box.
4. Click **Save**.

Now that the floorplan background image is uploaded, you will need to create a floorplan and configure it with system resources. For instructions, see [Composing, Editing, and Deleting Floorplans](#).

See also: [Monitoring Floorplans](#)

[Using the Monitoring Desktop](#)

Network Resources

Select **Configuration : Network Resources** to display the following options.

Choose this	To see information on
Directory Services	Configuring an Active Directory, or LDAP server.
Domain Name Servers	Entering names for the primary and secondary DNS servers.
Email Settings	Entering the name of the email server that will relay messages sent from the Network Controller, the email address that will appear as the sender of email notifications, and the name that will appear in the From field of all email notifications.

FTP Backup	Entering the server, user name, password, and directory for system backup via FTP.
Network Storage	Entering the domain name, server name, and share name for a network storage location, and a username and password.
Remote Logging	Set up remote logging to have syslog messages sent to a remote host.
Time Server	Entering names for the primary and secondary time servers used for setting system time.

See also: [Backing Up the System Data](#)

Setting Up an LDAP Server

Select **Configuration : Network Resources : Directory Services**.

Once you have configured an LDAP server for password authentication, some or all of your users' login passwords can be stored in a centralized, network based repository that is accessed through the Lightweight Directory Access Protocol (LDAP). Because password authentication for these users will be managed by an LDAP directory service (such as Microsoft's Active Directory), administrators will not enter login passwords into their person records—but instead will configure the person records to use the LDAP directory service. To log in, the users will enter their directory service domain passwords, which will be authenticated by the directory service.

By default, LDAP traffic is transmitted unsecured. When configuring the LDAP server, you can protect connections to the directory service over LDAP by specifying that the LDAP server will use a security protocol (TLS/SSL or LDAPS) for these connections. When the server uses one of these protocols, data is encrypted when it is sent across the network and will not be vulnerable if it is intercepted.

NOTE: Before system users can log in via an LDAP directory service, you must correctly configure each user on the [Login tab of his or her person record](#). Rather than enter a password for each user, you will select a check box specifying that the person can log in using his or her directory services domain password.

Configuring an LDAP server

1. In the **Name** field enter a name for the LDAP server.
2. In the **Domain** field enter the DNS domain for the LDAP server.
3. In the **Directory Services server** field enter the IP address of the LDAP server.
4. In the **Port** field enter the port number specified for use in obtaining directory services. Typically this is port 389.
The network administrator can supply you with the needed names, IP address, and port number.
5. Select one of the following options to specify the security protocol to be used for LDAP traffic:
 - **None** - The server uses unsecured (non-SSL) LDAP connections through a configurable port (port 389 by default). When this option is selected, the Certificate Required check box is cleared and disabled.
 - **Standard Transport Layer Security (TLS/SSL)** - This is the preferred protocol. The server uses secure LDAP connections through a configurable port (port 389 by

default). When a user presents his or her login credentials, the server first establishes an unencrypted connection with the client machine, then start the TLS layer using the StartTLS operation.

- **LDAP over SSL (LDAPS)** - The server uses secured LDAP connections through a configurable port (port 636 by default). When a user presents his or her login credentials, the server establishes an SSL-encrypted connection with the client machine.

6. Click **Save**.

Testing the LDAP connection

1. Click the **Test Connection** button.
2. **User Name** and **Password** fields appear. Enter your directory services user name and password, and click **Test Login**.
- or -

Click **Cancel** to cancel the test and hide the Test Connection fields.

See also: [Changing Your Password](#)

Domain Name Server Settings

Select **Configuration : Network Resources : Domain Name Servers**.

The network administrator will need to supply you with the IP addresses of the domain name servers. The address must be in the form of a numeric IP address such as 192.168.1.240.

To set up Domain Name Servers:

1. Enter in the **Server 1** text box the IP address of the primary domain name server. This entry is required.
2. Enter in the **Server 2** text box the IP address of the secondary domain name server. This entry is optional but highly recommended.
3. Click **Save**.

See also: [IP Setup Using Initmode](#)

Setting Up Remote Logging

Select **Configuration : Network Resources : Remote Logging**.

By setting up remote logging, you can have messages generated by your security management system forwarded to a remote host running the Rsyslog daemon. To reduce administration costs, you can have multiple systems forward their log messages to one Rsyslog server and manage them centrally.

NOTE: Consult your system administrator if you need to configure server-side logging.

To set up remote logging:

1. Select the **Enabled** check box.
2. In the **Selectors** box, do one of the following:
 - Enter *.* to log all messages.
 - Enter a line containing one or more selectors to specify which messages you want to log. Use the syntax described below.
3. For **Network transport**, select one of the available transports: UDP or TCP.
4. For **Port**, enter the port number used for the selected network transport.
For UDP transport, the port number will always be port 514. For TCP transport it will be port 514, *except* on Ubuntu 12.04 systems, which require a port number higher than 1024—such as 5144.
5. For **Remote computer**, enter the IP address (for example, 192.168.0.1) or network domain name (for example, MyRemoteLogServer.com) for the remote system to which log messages should be redirected.
6. Click **Save**.

Selector Syntax

Selectors are used to filter Rsyslog messages. Each selector consists of two parts: a facility and a priority, separated by a period (.). Both are case insensitive. You can specify multiple selectors using the semicolon (;) separator.

- The facility, which specifies the subsystem that produced the message, is one of the following keywords: auth, authpriv, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, and local0 through local7.
- The priority, which defines the severity of the message, is one of the following keywords, in ascending order: debug, info, notice, warning, err, crit, alert, emerg.

For more information on using selectors to filter Rsyslog messages, see the Rsyslog documentation, which is available from www.rsyslog.com.

Example:

The table below describes the meaning of each selector in the following line:

```
*.info;authpriv.*;mail.none;cron.none
```

Selector	Meaning
*.info	Log messages of priority level info (and higher) from all facilities.
authpriv.*	Log access control related messages of all priority levels.
mail.none	Exclude all messages generated by a mail system.
cron.none	Exclude all messages generated by cron.

Setting Up an Email Server for the Controller

Select **Configuration : Network Resources : Email Settings**.

To set up an email server for the controller, you can:

- Specify the name of the email server that has been set up to allow the relay of email messages sent from the Network Controller.
- Specify a valid email address for the Network Controller. Email messages sent by the Network Controller will appear to have come from this address.
- Specify the name that will appear in the From field of all email messages sent from the Network Controller.
- Specify the port number to be used for outgoing email messages. You can specify SMTP port 25 for unencrypted connections, or a commonly used SSL SMTP port such as 587 for encrypted connections. Refer to your network administrator or email service provider for information on the port to use.
- Optionally, specify an SMTP login password.

NOTE: For the system to provide email notification of alert conditions, the network administrator will have to set up the network email server to relay email messages sent from the IP address of the Network Controller.

To set up an email server:

1. In the **Email Server** text box, enter the mail relay server name. Enter this in the form of an IP address or DNS name.
2. In the **From email address** box, enter the address that should appear as the sender of email notifications sent from the controller. This should be a valid email address.
All email messages sent by the controller will appear to have come from this address. If the security administrator will want to see replies to emails sent by the controller, you should enter an address that will be forwarded to the security administrator.
3. In the **Full name to use in From field** box, enter the name that should appear in the From field of all email notifications sent from the controller.
4. In the **Port** field, enter the network port number to be used for outgoing email.
If you enter a port number other than 25, the system will attempt to use encrypted (SSL) connections. If an encrypted connection to the recipient server is not available, the system will fall back to port 25 for an unencrypted connection.
5. (optional) To specify an SMTP login password, select the **Server requires authentication** check box and enter the password in the text box that appears.
6. Click **Save**.

See also: [IP Setup Using Initmode](#)

[Managing Email Distribution Groups](#)

FTP Backup Settings

Select **Configuration : Network Resources : FTP Backup**.

With this page you can specify:

- The FTP server that is configured to accept backups from the controller.
- The user name, password, and directory for FTP backups.
- Use of the Secure File Transfer Protocol (SFTP) to protect FTP transfers.

You can also perform an immediate FTP backup.

NOTE: The system does not support DOS file systems on FTP servers.

The system is backed up daily at 00:15 hours. These backups are written to the network controller and to an FTP server if one is configured here. Backups are also written to network attached storage if a local share location is configured using [Configuration : Network Resources : Network Storage](#).

Backup to an FTP server will back up the following:

- Security database with all configuration information.
- Photos and badge designs
- Floorplans
- Sound files
- Other images that you may have uploaded to the network controller

NOTE: To complete the setup of **FTP Backup** you will need the assistance of a network administrator. After completing the Network administrator tasks below, your network administrator can supply you with the information you'll need to complete the System setup tasks that follow.

You can also perform manual backups to the network controller and manually download them to off-controller storage by selecting [Configuration : System Maintenance : Backup System](#).

Setting Up the Network Storage Location

Network administrator tasks:

1. On the FTP Server create a user name, password, and directory for the security management 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 will be used and ensure that firewalls will not block the needed ports.

When using Active mode FTP, TCP ports 20 and 21 must be open to the FTP server for FTP backups from the controller. When using Passive mode FTP, port 20 is not required.

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

System setup tasks:

1. Select the **Enabled** check box.

2. For **FTP Server**, enter the DNS name or IP address of the FTP server.
3. For **Username**, enter the network controller's user account name for the FTP Server.
4. For **Password**, enter the network controller's password for the FTP Server account. A password is optional.
5. For **Directory**, enter the name of the directory on the FTP Server used to save backups. This directory must be at the root level on the server.
6. Select the **Passive Mode** check box if Passive mode FTP is used. If this box is not selected, Active mode FTP is used by default.
Because SFTP does not support Active mode or Passive mode FTP, this setting will be ignored if you enable Secure FTP below.
7. Select the **Use Secure FTP (SFTP)** check box to use the Secure File Transfer Protocol to protect FTP transfers by encrypting commands and data transferred over the network. Note that depending on your SFTP server implementation, you may experience varying file transfer times.
For FTP transfers to be secured by SFTP, TCP port 22 must be open to the SFTP server for backups from the controller, and the SFTP server must be listening on that port.
8. Click **Save**.
9. Click **Test Connection** to test the connection between the controller and the FTP server.
10. Click **Backup Now** if you want to perform an immediate backup.

See also: [Backing Up the System Data](#)

[About Archive Files](#)

[System Maintenance Utilities](#)

[Setting Up the Network Storage Location](#)

Setting Up the Network Storage Location

Select **Configuration : Network Resources : Network Storage**.

For backups to be stored automatically to a network drive, this page must be completed.

The system is backed up each day at 00:15 hours. These backups are written to the network controller and automatically written to network storage if a local share location is configured here. In this release, the security management system provides no integration with Active Directory or Domain level shares.

Backup to a network storage location will backup the following:

- Security database with all configuration information
- Photos and badge designs
- Floorplans
- Sound files
- Other images that you may have uploaded to the network controller

NOTE: To complete the setup of network storage, you will need the assistance of a network administrator. Once the network administrator has completed their steps they can supply you with the information for the fields on this page.

You can also perform manual backups of the security database to the network controller and manually download them to off-controller storage by selecting [Configuration : System Maintenance : Backup System](#).

Setting Up the Network Storage Location

Network administrator tasks:

1. Create a network share.
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.

System setup tasks:

1. **Server Computer Name:** Enter the computer name for the server where the network share is located. Get this name from the network administrator.
2. **Server IP Address:** Enter the IP address of the server where the network share is located. Get this IP address from the network administrator.
3. **Share name:** Enter the name for the network share. Get this share name from the network administrator.
NOTE: The share name may **not** include spaces.
4. **Directory:** Enter the directory name in the network share for saving backups. Get this directory name from the network administrator.
5. **User Name:** Enter the network controller's local user account name for the network share. Get this account name from the network administrator.
6. **Password:** Enter the network controller's password for the local user account. Get this password from the network administrator.
7. Click **Save**.
8. Now that the NAS server is configured you can click the **Backup Now** button to perform an immediate backup.

See also: [Backing Up the System Data](#)

[About Archive Files](#)

[System Maintenance Utilities](#)

[FTP Backup Settings](#)

Setting Up the Network Time Server

Select **Configuration : Network Resources : Time Server**.

NOTE: You can manually force the time to synchronize with the time servers by clicking the **Run time sync now** button.

To setup a network time server:

1. Enter in the **Server 1** text box the DNS host address name of the primary network time server. This entry is required. Get this time server name from the network administrator.
2. Enter in the **Server 2** text box the DNS host address name of the secondary network time server. This entry is optional but highly recommended.
3. Enter in the **Server 3** text box the DNS host address name of the tertiary network time server. This entry is optional.
4. Select from the **Timezone** drop-down the correct time zone for this installation. This enables the network controller to determine the correct local time.
5. Click **Save**.

NOTE: If you have specified an internet time server and there is no Internet connection, then there will be several minutes delay when booting the Network Controller.

See also: [Setting the Time Zone](#)

[IP Setup Using Initmode](#)

Site Settings

Select **Configuration : Site Settings** to display the following options.

Choose this	To see information on
ASSA ABLOY Remote Locksets	Integrating ASSA ABLOY remote locksets.
Custom Menus	Setting up customized menus that can be assigned to users.
DMP Intrusion Panels	Configuring DMP intrusion panels to work with the system. This page is available only if your system license allows the addition of DMP intrusion panels.
Mercury Panels	Configuring Mercury panels.
Network Controller	Specifying the name and location of the controller and configuring various Network Controller settings.
Network Nodes	Enabling and configuring Network Nodes.
Node Status	Viewing the current status of enabled and connected nodes.
Partitions	Setting up partitions.
Remote Lockset Profiles	Creating and editing remote lockset profiles, to assist in the configuration and management of large numbers of ASSA ABLOY remote locksets .
Report Groups	Defining groups of Custom History and Custom People reports for use in defining custom user roles.
Report Settings	Configuring system-wide default settings for Custom History and Custom

	People reports.
Software License	Uploading and applying a software license file.
System Rules	Defining system rules for portal group behavior.
User Roles	Selecting roles and privileges for authorized security management system users.

See also: [Tech Note 4: Connecting Nodes and Controllers Across Subnets \(PDF\)](#)

[Tech Note 15: Integrating ASSA ABLOY Remote Locksets \(PDF\)](#)

[Tech Note 18: DMP Intrusion Panel Integration \(PDF\)](#)

[Tech Note 17: Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

[IP Setup Using Initmode](#)

Creating Custom Menus

Select **Configuration : Site Settings : Custom Menus**.

On this page you can create custom menus, each containing a specific set of options, which can then be assigned to users. A user's assigned custom menu will appear in the [navigation palette](#) when he or she clicks this control on the page bar:






Custom menus can be assigned:

- **Per user:** Selecting a custom menu on the [Login tab](#) of a person record defines it as the custom menu for that user.
- **Per role:** Selecting a custom menu for a [user role](#) defines it as the custom menu for all users with that role who do not have individually assigned custom menus via their person records.
- **Per partition:** Selecting a custom menu for the active partition (on the [Admin tab](#) of the Network Controller page) defines it as the custom menu for all users in that partition who do not have custom menus assigned via their user roles or person records.

NOTE: The predefined *User Tasks* custom menu includes the same set of options that in earlier releases appeared in the User Tasks widget on the Home page.

To create a custom menu:

1. Do one of the following:
 - To start from an existing custom menu, such as the predefined *User Tasks* menu, click the **rename** link and enter a new name.
 - To create a custom menu from scratch, click the **add** link and then enter the name.

2. Optionally, enter a **Description** for the menu that explains its use.
3. Select menu items from the Available list and click the right arrow button to move them to the Selected list.
To move multiple items at once, **SHIFT**-click to select contiguous items or **CTRL**-click to select non-contiguous items.
4. To reorder the Available or Selected list:
 - Click  to sort the list in descending order.
 - Click  to sort the list in ascending order.
 - Click  to return the list to its original order.
5. To re-position an item in the Selected list, select it and click the up and down arrow buttons to move it up and down in the list.
6. Click **Save**.

See also: [Configuring the Controller's Administration Settings](#)

[Creating User Roles](#)

[Editing Person Records](#)

[The Page Bar](#)

[The Navigation Palette](#)

[The Command Palette](#)

Mercury Panel Setup

Configuring Mercury Panels

Select **Configuration : Site Settings : Mercury Panels**.

Within the security management system, a Mercury panel is equivalent to a Network Node (with a few [differences](#)), and a Mercury SIO is equivalent to an application extension blade.

Once your Mercury devices have been installed and are available on the network, you can use this page to:

- [Configure a Mercury panel to work with the controller.](#)
- [Change IP settings for a Mercury panel.](#)
- [Configure timeout and disconnect events for a Mercury panel.](#)
- [Reset Mercury panel factory defaults or swap Mercury panel serial numbers.](#)
- [View and manage SIOs for a Mercury panel.](#)

The Guides and Technical Notes help topic includes links to technical notes describing all available Mercury and Mercury-powered hardware integrations.

To configure a Mercury Panel to work with the controller:

1. In the **Name** box, enter a name for the Mercury panel.
Give the panel a name that will help you identify it, such as "Floor1 Mercury Panel."
2. Select the **Enabled** check box to allow communication between the panel and the controller.
You can choose to wait until the hardware is set up to enable the panel. Once you select the check box, the panel will begin communicating with the controller. If you then clear the check box, the panel will continue to operate on its own, but it will no longer be able to communicate with the controller.
3. From the **Timezone** drop-down list, select a time zone for the Mercury panel.
NOTE: Each Mercury panel can have its own specified time zone.
3. From the **Type** drop-down list, select the appropriate model number for the panel:
 - The EP2500, EP1502, and EP1501 are Mercury EP-Series intelligent controllers.
 - The M5-IC is a Mercury M5 Bridge intelligent controller.
 - The PIM400-1501 is a Schlage Panel Interface Module (PIM). The PIM is required for communication between a Schlage wireless device and the built-in Mercury EP-1501 panel that will manage the device.
 - The PW6K1IC is a Mercury-powered Honeywell PW-Series intelligent controller.
4. On the **Network** tab, enter the IP address for the Mercury panel into the **IP Address** box.
5. Click **Save**.
6. Select **Configuration : Site Settings : Network Controller** to verify that the Mercury panel is connected. Mercury panels shown in **green** are enabled and communicating with the controller. Mercury panels shown in **red** are not currently communicating with the controller. It may take a few moments for the color of the Mercury panel to change.

See also: [Setting Up the Network Controller](#)

[Differences Between Mercury Panels and Network Nodes](#)

[Changing IP Settings for Mercury Panels](#)

[Specifying Events for Mercury Panels](#)

[Using Mercury Panel Command Buttons](#)

[Viewing and Managing SIOs for a Mercury Panel](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

[Setting Up Portals](#)

[Specifying Card/Keypad Formats](#)

Differences Between Mercury Panels and Network Nodes

Select **Configuration : Site Settings : Mercury Panels**.

Once a Mercury panel has been integrated into the security management system, it has the same functionality as a Network Node, with the exceptions described below.

Features that are Unsupported for Mercury panels:

- Alarm Delay setting for delaying an input's change to the alarm state.
- Alarm panel integration.
- Auto-arming of inputs
- Autodiscovery. All Mercury panel and SIO resources must be defined manually.
- Double Card Presentation mode.
- Enabling and disabling of portals from the Portal Status page and the Portal Status widget.
- FIPS-201 75-bit card format.
- Keypad command mode.
- Keypad timed unlock.
- Portal secondary outputs.
- Reset to Factory Defaults and Reset Node Networking buttons (on the Network Nodes page). Resetting a Mercury panel to its factory defaults, or resetting its networking settings, must be done at the board level.

NOTE: For information on using the bulk erase function to erase all configuration and cardholder databases, see the Mercury installation and specifications document for your panel. To reset the networking settings, set DIP switch 1 to OFF, set DIP switch 2 to ON, and set DIP switch 4 to OFF on the panel.

- Scheduled actions for inputs/input groups, outputs/output groups, and portal groups (but scheduled unlock for portals is supported).
- Scheduled actions for elevator floor-select buttons.
- Soft Always or Hard Always regional anti-passback privileges. When setting an individual's regional anti-passback privileges on the person record, selecting Soft Always or Hard Always has the same effect as selecting (none).
- Sub-locations. For Mercury panels, portals can be assigned only to the default location. Support for sub-locations will be added in a future build.
- System rules (First-in Unlock).

Features that are Partially Supported for Mercury panels:

- Event actions. Because of a difference in the Mercury panel hardware, the Arm Input Group/Disarm Input Group event actions will work only for Mercury inputs that are not attached to portals.
- Holiday start and end times. Mercury panels recognize the start and end dates specified for a holiday, but not the start and end times. For a Mercury panel, a holiday always begins at 00:00:00 on the specified start date and ends at 23:59:59 on the specified end date.

For information on a procedure you can use to work around this limitation, see [Configuring Partial-Day Holidays for Mercury Panels](#).

- Regional anti-passback. Because Mercury panels do not distinguish between passback violations and tailgate violations, the passback violation behaviors you specify for a region are executed for both passback violations and tailgate violations.

NOTE: Unlike standard nodes, which can have up to 512 access levels and 32 card formats, each Mercury panel is restricted to 32 access levels and 8 card formats.

See also: [Configuring Mercury Panels](#)

[Changing IP Settings for Mercury Panels](#)

[Specifying Events for Mercury Panels](#)

[Using Mercury Panel Command Buttons](#)

[Viewing and Managing SIOs for a Mercury Panel](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

Changing IP Settings for Mercury Panels

Select **Configuration : Site Settings : Mercury Panels** and click the **Network** tab.

Within the security management system, a **Mercury panel** is equivalent to a Network Node (with a few [differences](#)), and a **Mercury SIO** is equivalent to an application extension blade. Once you have [configured a Mercury panel](#) to work with the controller, you can use this page to:

- Determine the type of communications the controller will establish with the Mercury panel: either *outbound* by connecting to an IP address or *inbound* by listening on a particular port.
- Change the IP address used for outbound communications.
- Allow for the encryption of communications between the controller and the Mercury panel.
- Set connection options for normal and failover communications.

To change network settings for a Mercury panel:

1. Select the name of the Mercury panel from the **Name** drop-down.
2. For **Communication Type**, select one of the following for the normal communications channel and, optionally, for a failover communications channel:
 - **Outbound** if the controller will establish communications with the Mercury panel by connecting to its IP address.
 - **Inbound** if the controller will establish communications with the Mercury panel by listening on its port number.
3. Set the following connection options for each of the communications channels you specified at step 3:
 - For outbound communications, enter the IP address to which the controller will connect into the **IP Address** box.
 - (optional) Select the **Encrypt Communications** check box to allow for the encryption of communications with the Mercury panel.
 - For **Retry Count**, select the number of times the controller will retry after failing to connect to the Mercury panel.
 - For **Poll Delay**, select the number of milliseconds the controller will wait between polls to the Mercury panel. The default is 500 milliseconds.
 - For **Reply Timeout**, select the number of milliseconds the controller will wait for a reply from the Mercury panel before timing out. The default is 700 milliseconds.

- For **Retry Interval**, select the number of milliseconds the controller will wait before attempting to re-establish an outbound connection to the Mercury panel after a timeout. The default is 10,000 milliseconds.
4. Click **Save**. It may take several minutes for the Mercury panel and the controller to complete this communication.

See also: [Setting Up the Network Controller](#)

[Differences Between Mercury Panels and Network Nodes](#)

[Configuring Mercury Panels](#)

[Specifying Events for Mercury Panels](#)

[Using Mercury Panel Command Buttons](#)

[Viewing and Managing SIOs for a Mercury Panels](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

Specifying Events for Mercury Panels

Select **Configuration : Site Settings : Mercury Panels** and click the **Events** tab.

Within the security management system, a **Mercury panel** is equivalent to a Network Node (with a few [differences](#)), and a **Mercury SIO** is equivalent to an application extension blade.

On this page you can configure timeout and disconnect events for a Mercury panel. Before you can configure events, you must define them using the [Events](#) page.

To configure events for a Mercury panel:

1. Select the name of the Mercury panel from the **Name** drop-down.
2. For **Timeout Event**, select the event to be executed if the Mercury panel times out by failing to respond to the controller once per minute, and then select the **Enabled** box to the right.
3. For **Disconnect Event**, select the event to be executed if the Mercury panel disconnects from the controller, and then select the **Enabled** check box to the right.

Reasons that a Mercury panel might disconnect from the controller include a network outage, a loss of power to the Mercury panel, or a series of timeouts.

4. Click **Save**.

NOTE: Of the [available actions](#) that can be defined for an event, the following are supported for Mercury panels: **Lock Portal/Unlock Portal**, **Momentarily Unlock Portal**, **Arm Input Group/Disarm Input Group**, **Activate Output/Deactivate Output**, **Pulse Output**, and **Pulse Output Group**. Because of a difference in the Mercury panel hardware, the Arm Input Group/Disarm Input Group event actions will work only for Mercury SIO inputs that are not attached to portals.

See also: [Setting Up Events](#)

[Setting Up the Network Controller](#)

[Configuring Mercury Panels](#)

[Differences Between Mercury Panels and Network Nodes](#)

[Changing IP Settings for Mercury Panels](#)

[Using Mercury Panel Command Buttons](#)

[Viewing and Managing SIOs for a Mercury Panel](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

Using Mercury Panel Command Buttons

Select **Configuration : Site Settings : Mercury Panels** and click the **Commands** tab.

Within the security management system, a **Mercury panel** is equivalent to a Network Node (with a few [differences](#)), and a **Mercury SIO** is equivalent to an application extension blade.

On this page you can:

- [Reset a Mercury panel](#). The Reset function causes the Mercury panel to restart. This can take from one to several minutes. Resources (such as portals and inputs) associated with the Mercury panel will be inaccessible during that time. *Call for support if you have any questions or problems when using this option.*
- [Replace a Mercury panel](#). The Mercury panel Replace function lets you replace a Mercury panel's serial number with the serial number of another Mercury panel. Typically, this option will be used only when replacing the Mercury panel for service reasons, or when replacing Mercury panels in a pre-configured system once you are at a customer site. The new Mercury panel is automatically associated with the old Mercury panel's serial number, so the resource details do not have to be re-entered for the new Mercury panel's serial number. *Call for support if you have any questions or problems when using this option.*

To reset a Mercury panel:

Call for support if you have any questions or problems when using this option.

1. Select the name of the Mercury panel from the **Name** drop-down.
2. Click **Reset**.

Check the [Activity Log](#) for confirmation that the Mercury panel reset has completed.

To replace a Mercury panel:

Call for support if you have any questions or problems when using this option.

1. Select **Configuration : Site Settings : Mercury Panels**.
2. Click the **Commands** tab.
3. In the **Name field**, select the name of the Mercury panel you will replace.
4. Click the **Replace** button.

5. Disconnect and uninstall the old Mercury panel.
6. Install and connect the new Mercury panel.
The newly installed Mercury panel is automatically associated with the resources formerly managed by the old Mercury panel.

See also: [Setting Up the Network Controller](#)

[Differences Between Mercury Panels and Network Nodes](#)

[Configuring Mercury Panels](#)

[Changing IP Settings for Mercury Panels](#)

[Specifying Events for Mercury Panels](#)

[Viewing and Managing SIOs for a Mercury Panel](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

Viewing and Managing SIOs for a Mercury Panel

Select **Configuration : Site Settings : Mercury Panels** and click the **SIOs** tab.

Within the security management system, a [Mercury Panel](#) is equivalent to a Network Node (with a few [differences](#)), and a Mercury SIO is equivalent to an application extension blade. On this page you can:

- [View the SIOs and configured resources for a Mercury panel.](#)
- [Configure resources for an SIO.](#)
- [Add, modify, and delete SIOs.](#)

To view the SIOs and configured resources for a Mercury panel:

1. On the SIOs tab, select the name of the Mercury panel from the **Name** drop-down.
The SIOs for the selected panel are listed on the left.
2. Click the entry for the SIO you want to view.

A diagram of the SIO board appears on the page. To the right of the diagram is a link for each resource that can be configured for the SIO.

To configure resources for an SIO:

1. On the SIOs tab, select a Mercury panel and click the entry for the SIO you want to configure.
2. To set up a reader, output, or input for the SIO, click the link for that resource in the Resource Details list on the right.
3. Use the configuration page that appears to configure the resource.


Alternatively, you can click any reader, output, or input pictured on the diagram to display the configuration page for that resource type. The page is the same as the one used to set up [readers](#), [outputs](#), or [inputs](#) for a standard node.


4. Click **Save**.

For special configuration requirements, see the following topics:

- [Special Requirements for Configuring Schlage Wireless Devices](#)
- [Special Requirements for Configuring Mercury M5 Bridge Panels](#)


To add, modify, or delete an SIO:

1. On the SIOs tab, select a Mercury panel.
2. To add an SIO to the panel, click the **add** icon  above the list of SIOs.
- or -

To modify an SIO, select it in the list of SIOs and then click the **edit** icon .

2. If you are adding an SIO, enter its **Name** on the **Mercury SIO** page that appears.
3. Enter or change any or all of the following settings, and then click **Save** to save your changes.
 - **Channel:** The RS-485 channel used for communications between the SIO and the Mercury panel, either **0** or **1**.

The setting for the on-board SIO (EP-1502) is always 0.

- **Address:** The SIO's address on the selected channel.
This number should match the dip switch setting on the SIO hardware.
 - **Model:** The model number of the SIO.
4. To delete an SIO, select it in the list of SIOs and then click the **delete** icon .
 5. Click **Save**.

See also: [Configuring Mercury Panels](#)

[Differences Between Mercury Panels and Network Nodes](#)

[Changing IP Settings for Mercury Panels](#)

[Specifying Events for Mercury Panels](#)

[Using Mercury Panel Command Buttons](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

[Integrating Mercury-Powered Allegion Schlage Wireless Devices](#)

Configuring Partial-Day Holidays for Mercury Panels

Mercury panels recognize the start and end dates you specify when [creating a holiday](#), but not the start and end times. For a Mercury panel, a holiday always begins at 00:00:00 on the specified start date and ends at 23:59:59 on the specified end date.

If you need to have your Mercury portals lock or unlock for fewer than 24 hours a day on holidays, you can use the procedures outlined in the example below as a workaround.

In the example, you are creating a New Year's Eve holiday that can be used to unlock your Mercury portals for half the normal workday on December 31. The example assumes that you already have a time spec and portal group configured to unlock the portals during normal working hours on weekdays.

Example: Configuring a Half-Day New Year's Eve Holiday

1. Define a December 31 holiday covering the full 24-hour time period:
 - Select **Configuration : Time : Holidays**.
 - Enter a **Name** (*New Year's Eve*, for example) and an optional **Description** for the holiday.
 - Select the check box for a **Holiday Group**, such as Holiday group 1.
 - Select December 31 as both the **Start Date** and **End Date**.
 - Enter 00:00 as the **Start Time** and 23:59 as the **End Time**.
 - Click **Save**.
2. Define a time spec to be used specifically for half-day holidays:
 - Select **Configuration : Time : Time Specs**.
 - Enter a **Name** (*Half-Day Holidays 9 AM to 1PM*, for example) and an optional **Description** for the time spec.
 - Enter the **Start Time** and **End Time** for the period the time spec will be in effect.
For example, if you will want your Mercury portals to unlock between 9AM and 1PM on half-day holidays, enter 09:00 as the Start Time and 13:00 as the End Time.
 - For **Days of the Week**, select the check box corresponding to the holiday group you selected at Step 1, such as hol1.
 - Click **Save**.
3. Define a time spec group that combines the holiday and time spec you defined at Steps 1 and 2 with your existing "weekdays" time spec:
 - Select **Configuration : Time : Time Spec Groups**.
 - Enter a **Name** (*Weekdays and Half-Day Holidays*, for example) and an optional **Description** for the time spec group.
 - Move your existing "weekdays" time spec (used to unlock portals during normal working hours on weekdays) from the Available list to the Selected list.
 - Move the *Half-Day Holidays 9 AM to 1PM* time spec you created at step 2 from the Available list to the Selected list.
The time schedule matrix indicates that the time spec group will be in effect during normal working hours on weekdays, and between 9AM and 1 PM on December 31.
 - Click **Save**.
4. Edit your existing "weekdays" portal group:
 - Select **Configuration : Access Control : Portal Groups**.
 - From the **Name** drop-down list, select your existing "weekdays" portal group (used to unlock your Mercury portals during normal working hours on weekdays).

- From the **Unlock Timespec** drop down list, select the *Weekdays and Half-Day Holidays* time spec group you created at step 3.
- Click **Save**.

The portal group is now configured to unlock its portals during normal working hours on weekdays and between 9AM and 1PM on December 31. The advantage to using this method is that it becomes part of your security configuration and remains in place until you change it.

Alternatively, you can schedule an extended unlock for individual portals for a specific period of time on a holiday (using the [Schedule Action page](#) or the [Portal Status or Portal Unlock widget](#)). This must be done separately for each portal, however, and repeated every year. It does not become a permanent part of your security system configuration.

See also: [Configuring Mercury Panels](#)

[About Time Specs](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

Special Considerations for Configuring Schlage Wireless Devices

Select **Configuration : Site Settings : Mercury Panels** and click the **SIOs** tab.

Configuring a PIM400-1501

You can configure up to 15 wireless AD-400 wireless locks using a PIM400-1501.

Note the following special requirements for configuring a Schlage PIM400-1501 panel interface module:

- The resources (two inputs, a reader, and an output) usually stay in the Init state until you configure them for a [portal](#). This is because they do not exist independently of the lock in a portal definition.
- It is important to know the door number the lock is linked as, because this will tell you which resources displayed on the SIO tab will correspond to the lock:
 - DSM: input $((\text{door number} * 2) + 1)$
 - REX: input $((\text{door number} + 1) * 2)$
 - Reader: reader (door number+1)
 - Lock: output (door number+1)

For example, If you link your lockset as door 2, you should configure the following resources on the SIO tab:

- input 5 (DSM)
- input 6 (REX)
- reader 3 (reader)
- output 3 (lock)

Configuring these, or any other inputs, outputs, or readers, in any other positions will not work for this lock. They will belong to other locks whose door numbers correspond to those positions (regardless of whether those locks actually exist).

This also means that the portal definition for the lockset is restricted to that particular grouping of four resources. You cannot add any other resources to the portal definition and you cannot use those resources elsewhere.

Configuring an AD-400 or WRI400

Note the following special requirement for configuring a Schlage AD-400 wireless lockset or WRI400 wireless access point module:

- When configuring a portal's Reader 1 inputs for an AD-400 or WRI400, you must map input 1 to the DSM and input 2 to the RTX.

Similarly, when configuring a portal's Reader 2 inputs, you must map input 3 to the DSM and input 4 to the RTX—and so on for additional readers.

Reduced Functionality Associated with Allegion AD-400 Lockset Modes

When configuring an AD-400 lockset on the on the [Readers/Keypads page](#), you can set an Allegion AD-400 Lockset Mode (Office, Privacy, or Apartment) for the lockset. You can also set these modes for multiple locksets at once on the [Access Control : Utilities page](#).

A lockset configured for any Allegion AD-400 Lockset Mode other than None does not support the available portal unlock/lock mechanisms. For the portal associated with such a lockset, you cannot:

- Add it to a [portal group](#) that has an unlock time spec other than Never.
- Enable [Double Card Presentation Mode](#) in the portal definition.
- Perform a [momentary unlock](#).
- Schedule an [extended unlock or lock](#).
- Switch it to an [unlocked or locked state](#).
- Assign it an event for which an [unlock or lock event action](#) is defined.

IMPORTANT: When a Mercury panel restarts (following a UI reset, software upgrade, or hardware power cycle), any AD-400 lockset on the panel that is configured for an Allegion AD-400 Lockset Mode other than None will be locked—regardless of the lockset's state prior to the reset.

See also: [Configuring Mercury Panels](#)

[Viewing and Managing SIOs for a Mercury Panel](#)

[Differences Between Mercury Panels and Network Nodes](#)

[Changing IP Settings for Mercury Panels](#)

[Specifying Events for Mercury Panels](#)

[Using Mercury Panel Command Buttons](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

[Integrating Mercury-Powered Allegion Schlage Wireless Devices \(PDF\)](#)

Special Requirements for Configuring Mercury M5 Bridge Panels

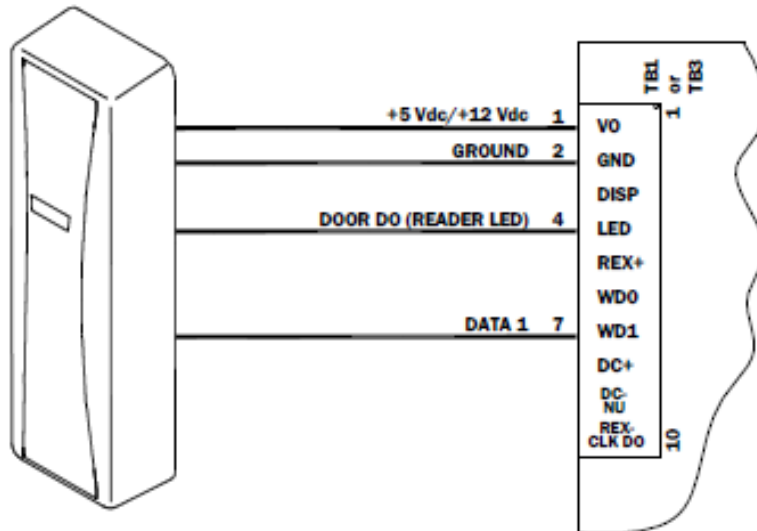
Select **Configuration : Site Settings : Mercury Panels** and click the SIOs tab.

When configuring resources (inputs and outputs) for a Mercury M5 Bridge Intelligent Controller M5-(IC) panel on the [SIOs tab](#), note the following special requirements for configuring Casi F2F readers and reader/keypad devices, M5 Bridge reader interface boards, and the M5 Bridge 20IN input board.

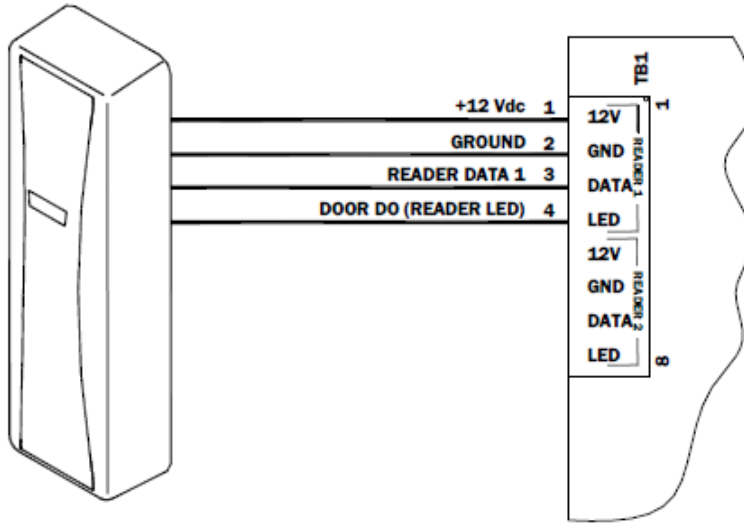
Configuring Casi F2F Readers and Reader/Keypad Devices

The Mercury M5 Bridge 2RP, 2SRP, and 8RP reader interface boards support Casi F2F readers and reader/keypad devices. When configuring a Mercury Casi F2F reader or reader/keypad device, note the following requirements:

- The card format you create must be a [magnetic stripe ABA Track 2 format](#) with a length of 15 bytes.
- When creating the card format, the **Casi F2F** check box must be selected on the Card/Keypad Formats page.
- If the reader type is "Supervised (Inputs)", the inputs must be configured on the portal. Otherwise, valid credential reads at the reader will always result in "Access not completed" messages.
- The F2F reader/keypad device must be wired to the Mercury 2RP or 2SRP panel, or to the 8RP panel, as shown in the figures below:



Wiring a Casi F2F reader to a Mercury 2RP or 2SRP panel.



Wiring a Casi F2F reader to a Mercury 8RP panel.

Configuring M5 Bridge Reader Interface Board

The Mercury M5 Bridge2RP and 2SRP boards support Wiegand readers and Form-C relay outputs.

When resources are going through an F2F or Wiegand reader on these boards, they are hard-coded and need to be assigned to the proper position.

Resource	Position Number	Reader Number
REX	Input 1	1
DSM	Input 2	1
Internal/External Relay* Output 1		1
REX	Input 3	2
DSM	Input 4	2
Internal/External Relay* Output 2		2

*The 8RP board supports external relays only.

Configuring the M5 Bridge 20IN Input Board

When you are configuring the Mercury M5 Bridge 20IN input board, it will be treated as if there were actually two SIO modules, each with ten inputs. SIOs need to be defined using consecutive addresses; slot numbers do not. On the SIOs tab, it will appear as if you have two separate devices, even though there is only one physical device.

In the example SIO configuration table below, the CASI 20IN inputs 1 through 10 are configured in Slot 2, Channel/Address 0/3. The CASI 20IN inputs 11 through 20 are configured in Slot 4 (consecutive addresses), Channel/Address 0/4 (non-consecutive slots).

Example SIO Name	Slot	Channel/Address	Model
CASI 8RP	1	0/1	M5-8RP
CASI 20IN Inputs 1-10	2	0/3	M5-20IN
CASI 2RP	3	0/2	M5-2RP
CASI 20IN Inputs 11-20	4	0/4	M5-20IN

See also: [Configuring Mercury Panels](#)

[Viewing and Managing SIOs for a Mercury Panel](#)

[Differences Between Mercury Panels and Network Nodes](#)

[Changing IP Settings for Mercury Panels](#)

[Specifying Events for Mercury Panels](#)

[Using Mercury Panel Command Buttons](#)

[Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)

Network Controller Setup

Setting Up the Network Controller

Select **Configuration : Site Settings : Network Controller**.

To set up the Network Controller, you can configure settings on the following tabs:

- **System** tab: See [Configuring the Controller's System Settings](#).
- **Nodes** tab: See [Configuring the Controller's Node Settings](#).
- **Web Site** tab: See [Configuring the Controller's Web Site Settings](#).
- **Access Control** tab: See [Configuring the Controller's Access Control Settings](#).
- **Admin** tab: See [Configuring the Controller's Administration Settings](#).
- **Events and Activity** tab: See [Configuring the Controller's Events and Activity Settings](#).
- **Data Integration** tab: See [Configuring the Controller's Data Integration Settings](#).

Configuring the Controller's System Settings

Select **Configuration : Site Settings : Network Controller**.

NOTE: Some of the options described in help will appear on the Network Controller page only if the Master partition is selected and you have the full system setup role.

Controller Information

- **Company name:** Enter the organization name here.

- **Location name:** Enter the name of the controller's location here. The name you enter will appear in the header of the application window whenever you are logged in to this controller.

Network Controller Time Settings

- Use the drop-down menus in this section to manually set the correct time and date on the controller.

See also: [Setting the time zone and specifying a network time server](#)

Initmode Settings

- Click the link in this section to open the Intimode page, which you can use to view and change the controller's network settings, time settings, email settings, and web server settings. [Click here for help on Initmode.](#)

Localization

- Click the link in this section to select the language and date format to be used in the user interface and Help system.
- **Temperature Scale:** Select Celsius or Fahrenheit for temperature inputs.

Support Information

- **Company:** Enter the name of the organization that will provide support for this installation.
- **Contact:** Enter the name of the person who will be the primary support contact for this installation.
- **Phone:** Enter the support contact phone number.
- **Email:** Enter the support contact email address.
- **URL:** Enter the URL (Universal Resource Locator) of the organization that will provide support for this installation.

See also: [Updating the Security Management System Software](#)

[Configuring the Controller's Node Settings](#)

[Configuring the Controllers Web Site Settings](#)

[Configuring the Controller's Access Controller Settings](#)

[Configuring the Controller's Administration Settings](#)

[Configuring the Controller's Events and Activity Settings](#)

[Configuring the Controller's Data Integration Settings](#)

Configuring the Controller's Node Settings

Select **Configuration : Site Settings : Network Controller.**

NOTE: Some of the options described in help will appear on the Network Controller page only if the Master partition is selected and you have the full system setup role.

- **Disable telnet on S2 nodes:** Select this check box to disable telnet capability on all S2 nodes. When this option is selected, you can use the **Enable Telnet** button on the [Network Nodes page](#) to temporarily enable telnet capability on a specific node.

See also: [Configuring the Controller's System Settings](#)

[Configuring the Controllers Web Site Settings](#)

[Configuring the Controller's Access Controller Settings](#)

[Configuring the Controller's Administration Settings](#)

[Configuring the Controller's Events and Activity Settings](#)

[Configuring the Controller's Data Integration Settings](#)

Configuring the Controller's Web Site Settings

Select **Configuration : Site Settings : Network Controller**.

NOTE: Some of the options described in help will appear on the Network Controller page only if the Master partition is selected and you have the full system setup role.

SSL

- **SSL Certificates:** Click the **Configure SSL** button to display the [SSL Certificates window](#), where you can enter certificate information.

Sessions

- **Limit Session to single IP address:** The default value here is **YES**. This is the more secure setting. This ensures that if an IP address changes during a session that the user will be required to login again. Changing this to **NO** will allow more than one IP address to participate in a single session.
- **Session Timeout:** Select from the drop-down the timeout duration for each session. If there is no system activity for the duration of the timeout counter, you are automatically logged out and will have to log in again.

NOTE: If you are [monitoring the activity log](#), the session will not time out. This is because the log continually updates, thus maintaining system activity.

Passwords

- **Minimum password length:** Enter the minimum number of characters that system users must include in their login passwords.
- **Password must contain letters, numbers, and special characters:** Select this check box to require that system users' login passwords contain a combination of letters, numbers, and special characters.

The following special characters can be used in a login password

:

At sign	@	Greater-than sign	>
Ampersand	&	Less-than sign	<

Asterisk	*	Number sign	#
Brackets, curly	{ }	Parentheses	()
Brackets, square	[]	Period	.
Caret	^	Plus sign	+
Colon	:	Question mark	?
Comma	,	Quotes, single	'
Equals sign	=	Quotes, double	"
Exclamation mark	!	Semicolon	;
Forward slash	/	Underscore	_
Hyphen	-	Vertical bar	

- **Password expiration (months):** To ensure that users change their passwords regularly, select an expiration period, in months, for all passwords in the active partition. Whenever a user changes his or her password, it will remain in effect for the selected number of months. If a user changes his or her password before it expires, the expiration period is reset and the new password will remain in effect for a full new expiration period.

Login Throttling

- Login throttling: Select this check box to limit the number of login attempts from the same IP address within a given number of minutes.
- **Maximum number of login attempts** and **Within this number of minutes:** After selecting the Login throttling check box, specify the maximum number of failed login attempts (the default is 3) and the number of minutes (the default is 1). If the number of failed attempts from a given IP address reaches the specified maximum within the specified number of minutes, the next attempt is ignored. The system displays a login failure message indicating the number of minutes the user must wait before trying again.

Refresh

- **Floorplan refresh every:** Select the frequency in seconds for refreshing the floorplan displays.

Banner

- **Appropriate use banner:** To display text (such as an appropriate use statement) on the login page, enter the statement in this text box. The character limit is 1024 characters.

See also: [Updating the Controller's System Settings](#)

[Configuring the Controller's Node Settings](#)

[Configuring the Controller's Access Controller Settings](#)

[Configuring the Controller's Administration Settings](#)

[Configuring the Controller's Events and Activity Settings](#)

[Configuring the Controller's Data Integration Settings](#)

Configuring the Controller's Access Control Settings

Select **Configuration : Site Settings : Network Controller**.

NOTE: Some of the options described in help will appear on the Network Controller page only if the Master partition is selected and you have the full system setup role.

Credentials

- **Disable credentials after "n" days of non-use:** Select this check box to ensure that any credential in the active partition that is not used within a specific number of days from the date it was issued will be disabled. In the text box that appears, enter the number of days of non-use that will be allowed before an unused card will be disabled.

NOTE: To exempt an individual user from this rule, you can select the **Exempt from credential non-use rules** check box on his or her person record.

- **Enable credential profiles:** Select this check box to allow administrators to use the [Credential Profiles](#) page to create credential profiles in the active partition. A credential profile can be assigned to individual credentials to ensure that they will be disabled if they are not used within a specific number of days from the date they were issued.
- **Enable maximum # active cards per person:** To limit the number of access cards that can be active for a person at a given time, select this check box and then enter the maximum number of active cards per person in the text box. Once the maximum number is reached for a person, attempting to add another card for the person will result in an error message. To add the additional card, you will need to either revoke or disable one of the person's currently active cards. By default, the check box is not selected and each person in the system can have an unlimited number of active access cards.
- **Enable temporary credential workflow:** Select this check box to display controls in all person records supporting a fast and accurate workflow for issuing, extending, and returning temporary credentials.
- **Enable expiration notification:** Select this check box to have the system notify members of the [email distribution group](#) selected in a person record if any of the person's credentials or access levels, or the person record itself, is about to expire. In the **Notification period** text box, enter the number of days (0 through 120) prior to an expiration that you want the notification to be sent. The default is 7 days.

When this option is enabled, a **Notify on expirations** drop-down list from which an email distribution group can be selected appears on the Access Control tab of each [person record](#).

- **Enrollment reader:** Select from the drop-down list the reader that you want to use for issuing access cards.
- **Default Card Format:** Select from the drop-down list the most common card format. You can change this, if necessary, when issuing cards.
- **Use Magnetic Stripe Encoding:** Select this check box to enable magnetic stripe encoding—the encoding of a magnetic stripe card with fields to be used for access control or other purposes.
- **Enable auto-incrementing of encoded credential numbers:** Select this check box to have the system automatically increment the highest encoded credential number in the database by one for each new credential that is added.


- **Highest encoded number in database:** This read-only field shows the highest encoded credential number currently in the database.

PINs

- **Enable duress PINs.** Select this check box to enable duress PINs for the active partition. This will allow a valid user in this partition to raise an alarm if compelled under duress to use his or her credentials (card and PIN) to give another person access to a portal. In such a situation, the cardholder can present his or her card and then enter a duress PIN into the keypad. This will result in an apparently normal access. However, an **Access granted [DURESS]** message will be logged in the Activity Log, indicating that a duress entry has occurred. For any event whose trigger is a duress entry, the event actions will be activated.

Each cardholder's duress PIN is his or her assigned PIN with the last digit incremented by 1 (such as 1->2, 9->0, or 0->1). For example, for a cardholder whose assigned PIN is **127649**, the duress PIN will be **127640**.

NOTE: To include information on duress accesses in a Custom History report, administrators can select the system event "Duress access completed" on the Events tab when entering filter criteria for the report.

- **PIN entry timeout (secs):** Sets the number of seconds allowed for PIN entry after a card read at a portal.
- **Two man entry timeout (secs):** Sets the maximum number of seconds that can elapse between the two valid credential reads required for access to a portal for which a two-man entry restriction is in effect.
- **Auto-generated PIN digits:** Enter the number of digits in the automatically generated PIN the system assigns to a person when an administrator clicks this icon  in the person record.

Passback

- **Auto-passback Grace at time:** Specify the time of day when all card holders will be granted passback grace. At the specified time every day, each individual's next card read will be allowed and no violations will be triggered. Thereafter, all anti-passback rules will be in effect.
- **Auto-passback Grace to Region:** Select the region to which all individuals' cards will be set automatically at the **Auto-passback Grace** time specified above.

See also: [Configuring the Controller's System Settings](#)

[Configuring the Controller's Node Settings](#)

[Configuring the Controllers Web Site Settings](#)

[Configuring the Controller's Administration Settings](#)

[Configuring the Controller's Events and Activity Settings](#)

[Configuring the Controller's Data Integration Settings](#)

Configuring the Controller's Administration Settings

Select **Configuration : Site Settings : Network Controller**.

NOTE: Some of the options described in help will appear on the Network Controller page only if the Master partition is selected and you have the full system setup role.

Cross-Partition

- **Enable cross-partition searches by default:** This check box will appear only if the Partitions feature is enabled for your system. Selecting it changes the default Partition setting on the person search page from <visible> to <all> for users who have access to multiple partitions. When such a user performs a person search, the search results will, by default, include records from all partitions to which the user has access.

After finding a person record located in another partition, the user can switch to that partition directly from the person record—and possibly edit the record, depending on his or her access rights in that partition. For more information, see [Searching for Person Records](#).

- **Make this partition name visible to all administrators in other partitions:** Select this check box to permit administrators in other partitions, even those who do not have at least administrative privilege in the active partition, to view and select it on the [Partitions](#) tab of a **Person Record**.
- **Share all people with every partition:** Select this check box to make every person record in the system visible across all partitions. Unless "Allow edit of persons made visible" is also selected, administrators in each partition will be responsible for giving users who visit that partition appropriate access to its person records.
- **Allow edit of persons made visible:** Select this check box to allow person records that have been made visible in a partition (either via the "Share all people with every partition" option above or via the Partitions tab of the person record) to be edited as well.

Person Data

- **Enforce unique person IDs:** Select this check box to enforce the requirement that each person in the system must have a unique ID number. When you select the check box, the system checks the database to determine if the **ID#** field in each person record contains a unique value. If all person IDs are unique, you will be able to enable and save this option.

If all person IDs are not unique, you will need to make them unique before you can enable and save this option. To search for a set of people with non-unique person IDs, select the **include only records with non-unique person IDs** check box before [running a search for person records](#).

Once this option is enabled and saved, a user will not be able to change the **ID#** field in a person record to a value that is already in use in another person record.

After an upgrade of an existing database, **Enforce unique person IDs** will be enabled by default if all person IDs in the database are already unique. It will be disabled by default if all person IDs are not unique.

- **Person ID required:** Select this check box to make **ID#** a required field in person records. A user will not be able to save a person record if this field is blank.
- **Auto-fill Person ID:** Select this check box to have the system automatically fill in the **ID#** field in each new person record.

If this option is enabled and a person record with a blank **ID#** field is accessed by the NAPI, Data Management Tool, or Data Operations, the field will be auto-filled with a value consisting of the underscore character (_) followed by a unique number.

- **Auto-fill prefix:** To have the system automatically add a prefix to each auto-filled ID number, enter the prefix in this field. The prefix you enter, followed by the underscore character (_), will be added to each auto-filled person ID.
- **Display the Person PIN in the Person Detail page?:** The default value is **YES**. To hide the display of individual PIN numbers, select **NO** from this drop-down list.

- **Allow edit of persons made visible.** Select this check box to allow person records that have been made visible in a partition (either via the "Share all people with every partition" option above or via the Partitions tab of the person record) to be edited as well.
- **Show Region and Passback Grace info in the Roster and People Reports** is, by default, unchecked. Selecting the check box forces the display of region information and **Grace** buttons in Roster and People reports.
- **Photo ID Size Limit:** (Extreme and Enterprise systems only) Select the maximum file size (in KB) for images uploaded to a person record. The available size limits range from 80KB (the default) to 1024KB.

NOTE: Increasing the size limit can have a significant effect on storage requirements. For example, suppose you have a 3,200 cardholder database. Increasing the size limit from 80KB to 1024KB can increase the space required for the images alone from just under a quarter GB to over 3GB.

- **Default Photo ID Layout:** Select the badge design you want to use for most ID cards. You can change this, if necessary, when issuing cards.

Roles

- **Hide unpermitted Access Levels:** Selecting **Yes** will hide access levels from system users who do not have the proper [User Role](#) to see these access levels.
- **Display the Card Number for Monitor/Administration roles?:** The default value here is **YES**. With this setting, the card numbers of users with Monitor or Administration roles will appear in certain reports and on the Personal Information page. To hide the display of card numbers for these users, select **NO** from this drop-down. With this setting, the card numbers will be displayed as a series of asterisks (*****).
- **Show Passback Grace as Menu Option:** By default, this is unchecked. Selecting the check box allows system users with only a Monitor user role to grant passback grace to card holders (if the following option, **Show Region and Passback Grace info in the Roster and People Reports**, is also checked).
- **Custom Menu:** Select the **Custom Menu** to be assigned to all users in the active partition who do not have custom menus assigned to them via the [Login tab](#) of their person records or via their [user roles](#). The drop-down list shows all available [custom menus](#) in the active partition.

A user's assigned custom menu will be displayed in the [navigation palette](#) when he or she user clicks the custom menu control on the page bar.

Trace Person

- **Trace person event:** To have access requests by people whose activity is being [traced](#) activate an event, select the event from the drop-down list. Select the **Enabled** check box to enable the event system-wide. All activations of the event will be logged in the Activity Log, and you can report on them by setting a Trace people filter for a Custom History report.
- **Trace person log color:** To have the Activity Log use a particular color to display entries for people whose activity is being traced, select that color from the drop-down list. This color will also be used in the Photo ID History widget to display information about people whose activity is being traced.

See also: [Configuring the Controller's System Settings](#)

[Configuring the Controller's Node Settings](#)

[Configuring the Controllers Web Site Settings](#)

[Configuring the Controller's Access Controller Settings](#)

[Configuring the Controller's Events and Activity Settings](#)

[Configuring the Controller's Data Integration Settings](#)

Configuring the Controller's Events and Activity Settings

Select **Configuration : Site Settings : Network Controller**.

NOTE: Some of the options described in help will appear on the Network Controller page only if the Master partition is selected and you have the full system setup role.

Activity Log

- **Always show device and controller time in Activity Log:** Select this check box to include in each Activity Log message the time when the event actually occurred on the node. The node time will appear in square brackets to the right of the controller time. If the check box is not selected, each log message will include only the time when the event was communicated to the controller.
- **Maximum number of Activity Log entries maintained in active database:** To increase the number of Activity Log records the system maintains in the active database for reporting purposes, enter the new number here. By default, the system maintains a maximum of 100,000 Activity Log records in the active database. Each Sunday, after the full backup, the system checks the number of Activity Log records. If this number exceeds 150,000, the oldest records in excess of 100,000 are zipped into an [archive file](#).
- **Access control messages identify credentials by:** To have each access control message in the Activity Log display additional information further identifying the person or credential associated with the access request, select the information you want displayed from the drop-down list.
- **Enable text filtering on the Monitoring Desktop:** Select this check box to allow monitors to filter the data shown in the Activity Log during a monitoring session. When the check box is selected, a **Filter** text box appears at the top of the Activity Log on the Monitoring Desktop. By entering text in the box and pressing ENTER, monitors can narrow down the data to view only log entries containing that text.

Events

- **Controller Tamper Alarm Event:** To enable a tamper event for an Extreme system that includes a Serial Adaptor Module (SAM), select the event from the drop-down list and select the **Enabled** check box. If the Extreme cabinet is tampered with, the SAM's tamper detection feature will activate the event. If your system does not include a SAM, the **Enabled** check box for this option will be disabled.
- **Controller Failed Login Event:** To configure a defined event as a failed login event, select the event from drop-down list and select the **Enabled** check box. This event will be activated by failed attempts to log in to the system.

Audio

- **Unacknowledged Event Audio:** Select **Yes** to have the system play a wav file once per minute as long as an unacknowledged alarm is active. From the **Sound** drop-down select the sound file you want to hear.

See also: [Configuring the Controller's System Settings](#)

[Configuring the Controller's Node Settings](#)

[Configuring the Controllers Web Site Settings](#)

[Configuring the Controller's Access Controller Settings](#)

[Configuring the Controller's Administration Settings](#)

[Configuring the Controller's Data Integration Settings](#)

Configuring the Controller's Data Integration Settings

Select **Configuration : Site Settings : Network Controller**.

NOTE: Some of the options described in help will appear on the Network Controller page only if the Master partition is selected and you have the full system setup role.

API

In this section you can enable the API for programmatic data exchange between existing personnel systems and security database records. By default this API interface is disabled.

When using API commands the security management system uses SHA (Secure Hash Algorithm) authentication, and message sequence numbers to ensure the security and integrity of the system. Each API command is accompanied by a MAC (message authentication code) and a sequence number. The MAC must be correct and the sequence number must be greater than sequence number of the previous command or the system will ignore the message.

- **Enabled:** Click to check this box if you want to enable the use of the API for data exchange.
- **Use Authentication:** This box is checked by default. It is strongly recommended that this be left checked. SHA authentication makes API usage secure.
- **Use login username/password for authentication (requires setup privilege):** Select this check box to have the system use a user's login username and password for API authentication.
- **SHA Secret:** Enter your SHA secret password. This password is used, along with other data, by the SHA calculator in creating a unique message authentication code.
- **Re-enter SHA Secret:** Enter the SHA secret again to ensure accuracy.
- **Sequence Number:** This number increments sequentially. You cannot enter anything in this box.
- **Reset Sequence Number to '0':** Click to check this box and then click **Save**. This resets the sequence number to zero.

ODBC

- **Enabled:** Select this check box to allow users to connect directly to the controller using ODBC and create reports from the security database.
- **ODBC Report user password:** Enter the password a user will need to enter to use this feature. The default password is "report." The Username is "report."

CSV Export

- **Enabled:** If an FTP server or NAS drive is configured for system backups, you can select this check box to have the system automatically generate nightly CSV Export reports and save them in the same location as the nightly backups.

Each nightly CSV Export report will contain the events logged in the Activity Log on that day, for all partitions. The report will be saved as a comma-separated values (CSV) file, with a file name indicating the date on which the event data was logged. For example, the report containing data for June 28, 2009 will be named 2009-06-28.csv.

See also: [Configuring the Controller's System Settings](#)

[Configuring the Controller's Node Settings](#)

[Configuring the Controllers Web Site Settings](#)

[Configuring the Controller's Access Controller Settings](#)

[Configuring the Controller's Administration Settings](#)

[Configuring the Controller's Events and Activity Settings](#)

IP Setup Using Initmode

There are two ways to get to the Initmode page:

- At installation time, when the Network Controller is first booted, browse to the default IP address of the Network Controller: **192.168.0.250**.
- Select **Configuration : Site Settings : Network Controller** and click the link in the Initmode Settings section.

With this page you can edit the initial IP (network) settings for the Network Controller and Network Node. This may require information from the network administrator.

IMPORTANT: Once the IP settings are completed you must do the following three things:

1. Near the bottom of the page, you must select **No** in the **Initmode Settings** drop-down list. This will ensure that the Initmode page will not re-appear.

2. Click **Save**. The webserver restarts and beeps when done. This saves the IP settings into the Network Controller database.

NOTE: If you set Initmode to **No** and did **not** change any IP address values, click **Save**, then **Reboot**, and **OK**. You will hear two beeps when the system shuts down, and one when it restarts. Refresh the browser to proceed.

3. Browse to the new controller IP address.

Network Controller Network Settings

IP address:

Any valid IP address in dot notation is a valid value. The default value is 192.168.0.250. An IP address entered here is a static IP address. That is, it will not change. See the network administrator for an appropriate IP address.

Subnet mask:

Any valid subnet mask in dot notation is a valid value. The default value is 255.255.255.0. The network administrator can supply you with this netmask number.

Gateway:

Any valid IP address in dot notation is a valid value. The default value is 192.168.0.1. The network administrator can supply you with this gateway IP address. This is the address of the router that connects the Network Controller to the rest of your network or to the Internet.

DNS 1:

Domain Name Server address. Any valid IP address in dot notation is a valid value. The default value is 192.168.0.1. The network administrator can supply you with this DNS IP address.

DNS 2:

Backup Domain Name Server address (optional). Any valid IP address in dot notation is a valid value. The default value is 192.168.0.1. The network administrator can supply you with this DNS IP address.

Avance IP Address:

The IP address of the HA server pair, if a High Availability implementation is configured for your system. See [Monitoring High Availability \(HA\) Status](#) for more information.

Network Controller Time Settings

Use of an NTP network time server ensures that the Network Controller will be regularly synchronized with the exact time used by all other network resources. At least one time server must be designated for the Network Controller to synchronize its own time. If no timeserver is available the Network Controller time will drift.

You can also manually set the time using this page.

Current Network Controller Time:

This displays the current time of the Network Controller clock.

Manually Set Date/Time:

If there will be no network time server available for the Network Controller, select from the date and time drop-down lists to manually set the time for the Network Controller.

Timeserver 1: <DNS host address name>

The default preset name in this field is pool.ntp.org. If the Network Controller is installed on a network with Internet access, this setting need not be changed.

NOTE: If there is no Internet access:

- The network administrator must supply you with a local network timeserver name or the time will have to be manually set.
- If the time must be manually set, remove the time server name from this field, to avoid having the Network Controller spend several minutes searching for this server. Until the search times out, you will not be able to continue editing the settings on this page.

Timeserver 2:

The default preset name in this field is pool.ntp.org.

Timeserver 3:

The default preset name in this field is pool.ntp.org.

Timezone:

Select the appropriate time zone for your area from the drop-down. The default preset value in this field is US/Eastern.

Email Settings

Email Server:

The IP address or DNS name of the mail relay server. The network administrator can supply you with this address or name.

NOTE: For the system to provide email notification of alert conditions, the network administrator will have to set up the network email server to relay email sent from the IP address of the Network Controller.

From email address:

The address that should appear as the sender of email notifications sent from the Network Controller. This should be a valid email address.

All email messages sent by the Network Controller will appear to have come from this address. If the security administrator will want to see replies to emails sent by the Network Controller, you should enter an address that will be forwarded to the security administrator.

Full name to use in From field:

The name that should appear in the **From** field of all email notifications sent from the Network Controller.

Web Server Settings

Web Server Port:

The default preset value in this field is 80. See the network administrator for the web server port number.

Initmode Settings

Initmode:

Typically this value should be changed to **No**.

If this value is left at **Yes**, the Initmode page will display after each boot of the Network Controller. You can return to the Initmode page from the security management system by selecting **Configuration : Site Settings : Network Controller** and click the link in the **Initmode Settings** section.

Factory Defaults

WARNING: When you reset your system to factory defaults, all information for your database is deleted and all configuration and log information is lost.

Resetting to factory defaults also does the following:

- Resets the controller web server port to 80.
- Resets the password for the default administrator account to "admin."
- Resets the interface language to English.

To reset your system to factory defaults:

1. Select the **Check here to reset to factory defaults** check box.
2. Enter the word **DEFAULTS** into the text box.
The word must be typed in all capital letters.
3. Click **Reset to Factory Defaults**.

See also: [Installing Nodes and Controllers Across Subnets \(PDF\)](#)

[Initial Software Setup Guide \(PDF\)](#)

[Rebooting and Resetting IP/Login Defaults \(PDF\)](#)

Configuring Secure Socket Layer (SSL) Certificates

Select **Configuration : Site Settings : Network Controller**.

Clicking **Configure SSL** in the Web Site section of this page displays the SSL Configuration window, which you can use to configure an *SSL certificate*. This is an electronic document that will make communications between the security application's embedded web server and web browsers more secure.

Depending on the option you choose to configure the SSL certificate, it will provide either encryption alone, or encryption plus authentication. Encryption makes the information sent between the web server and web browsers unreadable by unauthorized parties. Authentication verifies that your organization is the source of information sent by the web server.

The available options for configuring SSL certificates are:

- **SSL Disabled:** (default) When this option is selected, information sent between your web server and web browsers is unencrypted and unauthenticated.
- **Self-Signed SSL:** This simple and cost-free option lets you generate an SSL certificate that is signed with your web server's own private key. The certificate will provide encryption but not authentication.
- **SSL Upload Certificate from CSR:** This option lets you generate a certificate signing request (CSR), which you can send to a certificate authority (CA). The CA will use the CSR to issue a trusted SSL certificate containing a public key and information that identifies your organization. The certificate, which certifies your ownership of the public key, will provide both encryption and authentication.
- **SSL Upload Certificate and Key:** If you have decided to use your own SSL certificate and matching key, you can use this option to upload them to the controller. Optionally, you can also upload an intermediate CA file, (sometimes called a chained certificate) that links your certificate to a trusted root certificate.

To generate a self-signed SSL certificate:

1. Select the **SSL Self-Signed** option.
2. Enter identity information for your organization in the following fields:
 - **Country:** The two-letter ISO code for the country where your organization is located.
 - **Locality or City:** The city or other locality where your organization is located.
 - **Organization:** The legal name of your organization.
 - **Common Name:** The fully qualified domain name of your server, which immediately follows `http://` or `https://` in the address you enter in a browser to reach the server. The common name will be either an IP address or a DNS name assigned by your network administrator, such as "mySMS/mycompany.com" in the example below:

- **SSL Port:** Port used by HTTPS URLs.
- **State or Province:** The state or region where your organization is located.

- **Email Address:** An email address used to contact your organization.
 - **Organizational Unit:** The division or department of your organization handling the certificate.
3. To force users to use HTTPS so their data will always be encrypted, select the **SSL Required** check box.
 4. Click **Save Changes**.
This generates the internal request and signs it, using an authority inside the server itself, with no chain of trust. It then configures the web server to use the internal server key and certificate.

To generate a Certificate Signing Request:

1. Select the **SSL Upload Certificate from CSR** option.
2. Enter identity information for your organization in the following fields:
 - **Country:** The two-letter ISO code for the country where your organization is located.
 - **Locality or City:** The city or other locality where your organization is located.
 - **Organization:** The legal name of your organization.
 - **Common Name:** The fully qualified domain name of your server, which immediately follows http:// or https:// in the address you enter in a browser to reach the server. The common name will be either an IP address or a DNS name assigned by your network administrator, such as "mySMS/mycompany.com" in the example below:

https://mySMS/mycompany.com ▼
 - **SSL Port:** Port used by HTTPS URLs.
 - **State or Province:** The state or region where your organization is located.
 - **Email Address:** An email address used to contact your organization.
 - **Organizational Unit:** The division or department of your organization handling the certificate.
3. To force users to use HTTPS so their data will always be encrypted, select the **SSL Required** check box.
4. Click **Generate CSR**.
This generates a certificate signing request (CSR) that is based on the server's internal key and downloads it to your hard drive. This CSR can be sent to a certificate authority (CA), who will generate a server certificate.
5. For **Certificate File**, browse to the web server certificate file generated by the CA, then click **Upload** to upload the file to the controller.
6. Click **Upload** to upload the certificate file to the controller.
Once the certificate file has been successfully uploaded, a green light appears next to the Upload button and the Save Changes button becomes available.
7. Click **Save Changes** to configure the web server to use this certificate.

To upload a web server certificate and matching key:

1. Select the **SSL Upload Certificate and Key** option.
2. For **Certificate File**, browse to the web server certificate file, then click **Upload** to upload the file to the controller.

3. For **Server Name**, enter the name that will match your common name (the fully qualified domain name of your server) when the certificate is generated.
4. For **Key File**, click **Choose File** and browse to the private key file. Click **Upload** to upload the file to the controller.
Once the certificate file and matching key have been successfully uploaded, a green light appears next to their Upload buttons and the Save Changes button becomes available.
5. (optional) For **Chain File**, click **Choose File** and browse to the chain certificate file. Click **Upload** to upload the file to the controller.
6. Click **Save Changes** to install the files and configure the web server to use them.

See also: [Configuring the Controller's Data Integration Settings](#)

Network Node Setup

Viewing Node Status

Select **Configuration : Site Settings : Node Status**.

This page shows all nodes (including Mercury panels) in the active partition. If you have the full system setup role, it shows all nodes in the system, organized by partition. Nodes shown in **green** are enabled and communicating with the controller. Nodes shown in **red** are not currently communicating with the controller.

As a shortcut, you can click the link for a node to open its configuration page. If the node is not in the active partition, clicking its link also makes its partition the active partition.

NOTE: Any nodes that were set up for ASSA ABLOY remote locksets appear in a table at the bottom of the page. For more information, see [Viewing the Status of Remote Locksets](#).

See also: Configuring Network Nodes

[Configuring Mercury Panels](#)

[Enabling and Configuring ASSA ABLOY Remote Locksets](#)

[Network Node Hardware Installation Guide \(PDF\)](#)

[MicroNode Plus Hardware Installation Guide \(PDF\)](#)

[MicroNode Hardware Installation Guide \(PDF\)](#)

Changing Network Node IP Settings

Select **Configuration : Site Settings : Network Nodes** and click the **Network** tab.

As indicated below, some of the options on this page are available only for MicroNodes and earlier generation Network Nodes that use a CBM blade. They are not available for Network Nodes that use an M1-3200 blade. For more information on the functional differences between the earlier generation and current generation Network Nodes, see the [Initial Software Setup Guide](#).

With this page you can:

- Enable a selected node for communication with the controller.
- [Change node network address settings](#).
- [Set the discovery method](#) used by the node to find the controller (not available for Network Nodes that use an M1-3200 blade).
- [Protect a node's IP configuration](#) to keep it from changing (not available for Network Nodes that use an M1-3200 blade).
- [View network settings for a remote lockset](#).

To change node network address settings:

This procedure allows you to change network address settings for nodes that are either on the same subnet as the controller or on a different subnet but are already connected. To see if a node is connected, select *Configuration : Site Settings : Node Status*. Nodes that are connected are shown in green and have the status *Connected*.

If a MicroNode or Network Node that uses a CBM blade is on a different subnet than the controller, you will need to use the `nnconfig` utility (`nnconfig.exe`) to give the node the IP address of the controller to which it should connect. For more information, see [Tech Note 4: Connecting Nodes and Controllers Across Subnets \(PDF\)](#).

NOTE: You cannot change a node's network address settings and its discovery method settings at the same time. Change one first, save your changes, and then change the other.

1. Select the node you want to change from the **Name** drop-down list.
2. Click the **Network** tab.
3. For **Node IP Addressing Scheme**, is strongly recommended that you select **Static**.
4. Change any of the values for **IP Address**, **Subnet Mask**, and **Gateway** associated with the selected node.
5. Select the **Configuration Protected** check box to ensure that the node IP settings cannot be changed until this box is cleared. This option is not available for Network Nodes that use an M1-3200 blade.
6. Click **Save**. It may take several minutes for the node and controller to complete this communication.

To set the discovery method for a MicroNode or Network Node that uses a CBM blade:

MicroNodes and Network Nodes that use a CBM blade can find controllers through the process of **auto-discovery**, or by using a specified **Network Controller IP address**.

Using auto-discovery, nodes multicast their 16-character unique IDs over the network to register with any available controllers. Once registered, they will appear on the Node Status page and in the Name drop-down list of the Network Nodes page.

If you specify a particular Network Controller IP address on the Network Nodes page, the node will talk directly to that address rather than multicast its unique ID.

1. Select the node you want to change from the **Name** drop-down list.
2. Click the **Network** tab.
3. For **Node IP Addressing Scheme**, it is strongly recommended that you select **Static**.
The text boxes for **IP Address**, **Subnet Mask**, and **Gateway** display the values associated with the selected node.
4. Select the **Configuration Protected** check box to ensure that the node IP settings cannot be changed until this box is cleared.
5. You can enable auto-discovery by the node by selecting the **Allow Network Controller autodiscovery** check box, or you can clear the check box and enter the IP address of the controller in the **Network Controller IP Address** text box.
6. Click **Save**.

To protect the IP settings of a MicroNode or Network Node that uses a CBM blade:

Once the node's configuration is set and it is connected to a controller we recommend that you protect the IP configuration. If the IP configuration is not protected, the `nnconfig.exe` utility could be used to compromise the system.

Once the IP configuration is protected using this procedure, only a system user with at least Setup privileges can unprotect it by clearing this box.

1. Select the node you want to change from the **Name** drop-down list.
2. Click the **Network** tab.
3. Select the **Configuration Protected** check box to ensure that the node IP settings cannot be changed until this box is cleared.
4. Click **Save**.

See also: [IP Setup Using Initmode](#)

[Setting Up the Network Controller](#)

[Tech Note 1: How Nodes and the Network Controller Use the Network](#)

[Tech Note 4: Connecting Nodes and Controllers Across Subnets \(PDF\)](#)

[Tech Note 35: USB Commissioning of S2 Nodes](#)

Specifying Node Events

Select **Configuration : Site Settings : Network Nodes** and select the **Events** tab.

On the Events tab you can configure power fail, tamper, timeout, and disconnect events for a node. You can also configure low battery events for a node that uses an M1-3200 blade, and an ACM fault event for a MicroNode Plus.

Before you can configure an event for a node, the event must be defined on the [Events page](#).

NOTE: For information on configuring events for an ASSA ABLOY remote lockset, see [Enabling and Configuring ASSA ABLOY Remote Locksets](#).

To configure events for a node:

1. Select the name of the node you want to configure and do any or all of the following.
2. Select a **Power Fail Event** to be activated if the power to the node fails (even if it switches to battery backup).
3. Select a **Tamper Alarm Event** to be activated if the tamper switch enters an alarm state when the enclosure door is opened.
4. Select a **Timeout Event** to be activated if the node "times out" by not responding to the controller once per minute.
5. Select a **Disconnect Event** to be activated if the node disconnects from the controller.

NOTE: A node can disconnect from a controller because of a network outage, a loss of power to the node, or the occurrence of several timeouts in a row.

6. For a Network Node that uses an **M1-3200** blade, do either or both of the following:
 - Select a **Low Battery Capacity Event** to be activated when the node indicates the battery capacity is low.
 - Select a **Low Battery Voltage Event** to be activated when the node indicates the battery voltage is low.
7. For a **MicroNode Plus**, select an **ACM Fault Event** to be activated when it draws more power than is available.

When the MicroNode Plus draws more power than is available, its ACM portion is powered down (fault state) while its Node portion remains operational and reports the event. The ACM remains powered down until recovery procedures allow it to operate with power available to the MicroNode Plus.

7. Click **Save**.

See also: [Setting Up Events](#)

Configuring Network Nodes

[Setting Up the Network Controller](#)

Using Node Command Buttons

Select **Configuration: Site Settings : Network Nodes** and click the **Commands** tab.

On this page you can:

- [Reboot a node](#).
- [Reset a node to factory defaults](#). *Call for support if you have any questions or problems when using this option.*
- [Swap node unique identifiers](#) after replacing a node for service reasons. *Call for support if you have any questions or problems when using this option.*
- [Reset node networking settings](#) (not available for Network Nodes that use an M1-3200 blade).

- [Temporarily enable telnet capabilities on a node](#) if **Disable telnet on S2 nodes** is selected on the [Network Controller page](#).

NOTE: For information on reloading node configuration information into a remote lockset, see [Enabling and Configuring Remote Locksets](#).

To reboot a node:

1. Select the node you want to reboot from the **Name** drop-down list.
2. Click the **Commands** tab.
3. Click **Reboot**.

The **Reboot** button restarts the node. This can take from one to several minutes. Resources (such as portals and inputs) associated with this node will be inaccessible during that time. Look in the Activity Log for confirmation that the node reboot has completed.

To reset a node to its factory defaults:

1. Select the node you want to reset from the **Name** drop-down list.
2. Click **Reset to Factory Defaults**.

Call for support if you have any questions or problems when using this option.

The **Reset to Factory Defaults** button clears the current system configuration from the node and reverts to its factory installed application code. When the node reconnects to the controller, it is upgraded to the most recent application code on the controller. The current system configuration of portals, people, data, and so forth is loaded onto the node.

CAUTION: If you reset a node that is on a different subnet than the controller, the node might not reconnect. In this case, you will need to use the Network Node Configurator (nnconfig.exe) to give the node the specific IP address of the controller to which it should connect. For more information, see [Tech Note 4: Connecting Nodes and Controllers Across Subnets \(PDF\)](#).

To swap node unique identifiers:

1. Select **Configuration : Site Settings : Network Nodes** and note the name of the node you will replace.
2. Power down the system.
3. Replace the old node blade with the new node blade.
4. Power up the system.
5. Select **Configuration : Site Settings : Network Nodes**.
6. Select the new node from the **Name** drop-down and rename it "Temp Node."
7. Click **Save**.
8. Click the **Commands** tab.
9. Click **Swap**. A message window appears.
10. In the message window, select the old node from the **with node** drop-down.
11. In the message window, click **Save**.

NOTE: The newly installed node blade is now associated with the resources (inputs, portals, and so forth) formerly managed by the old node.

12. Select **Temp Node** from the **Name** drop-down list.
13. Click **Delete**.

Call for support if you have any questions or problems when using this option.

Typically the node ID swapping option will be used only when replacing a node or service reasons, or when replacing panels in a pre-configured system once you are at a customer site. The new node can be associated with the old node's **Unique Identifier** so that the **Resource Details** will not have to be re-entered for the new node blade.

To reset networking settings for a MicroNode or Network Node that uses a CBM blade:

NOTE: For a Network Node that uses an M1-3200 blade, resetting the network configuration is part of resetting it to factory defaults, using the Revert button on the blade.

1. Select **Configuration : Site Settings : Network Nodes** and select the node you want to reset from the **Name** drop-down list.
2. Click the **Commands** tab.
3. Click **Reset Node Networking**.

This resets the node's networking settings to the factory defaults. The node's IP address is reset to a Zeroconf address.

If the node is on the same subnet as the controller and is connected and functioning correctly, clicking the button will appear to have no effect. The controller will be aware of the node's new IP address and the node will remain connected. If the node is on a different subnet, however, it will be disconnected from the controller and you will need to use the `nnconfig.exe` utility to reconnect it. For instructions, see [Tech Note 4: Connecting Nodes and Controllers Across Subnets \(PDF\)](#).

To temporarily enable telnet on a node:

1. Confirm that **Disable telnet on S2 nodes** is selected on the [Network Controller page](#).
2. Select **Configuration : Site Settings : Network Nodes** and select the node for which you want to enable telnet from the **Name** drop-down list.
3. Click the **Commands** tab.
4. Click **Enable Telnet**.
5. Enter the number of minutes telnet capability should be enabled for the node. The default is 30 minutes.
6. Click **Save**.

NOTE: When telnet is temporarily enabled for a node, issuing subsequent **Enable Telnet** commands for the node will override the command currently in effect. For example, if you enable telnet for 30 minutes and immediately issue a second command to enable it for 10 minutes, telnet capability will expire on the node in 10 minutes.

See also: [Setting Up Alarm Inputs](#)

[Setting Up Temperature Inputs](#)

[Setting Up Outputs](#)

[Setting Up Readers/Keypads](#)

[Setting Up the Network Controller](#)

[Tech Note 4: Connecting Nodes and Controllers Across Subnets \(PDF\)](#)

Viewing Node Application Blades and Resources

Select **Configuration : Site Settings : Network Nodes** and then click the **Blades** tab.

On this tab you can:

- View the slot positions and resources of Access, Input, Output, and Temperature application blades.
- Use the links in the **Resource Details** column to pop-up input, output, and reader configuration pages.

To view blade positions and configured resources:

1. Select the node from the **Name** drop-down list.
2. Click the **Blades** tab.
3. In the **Blade Type** column, click the link for the blade you wish to view.

NOTE: A picture of the application blade appears and to the right are links for **Resource Details** and the **Status** of each resource.

See also: [Configuration Reports](#)

[Setting Up Alarm Inputs](#)

[Setting Up Temperature Inputs](#)

[Setting Up Outputs](#)

[Setting Up Readers/Keypads](#)

[Setting Up the Network Controller](#)

[Viewing and Managing SIOs for a Mercury Panel](#)

Slot and Position Numbers

To set up and configure system resources properly, installers must understand how the system determines slot numbers and position numbers.

Each resource configuration must specify the:

- Network node
- Slot number
- Position number

NOTE: If there are multiple network controllers in the installation, the address expands to include the controller name.

Slot numbers in the software are determined by the connector on the ribbon cable that is plugged into the board. The ribbon cable is essentially a bus and a board's place in the bus determines the number.

Position numbers are determined by the connector position on the board itself.

To see a graphic with position numbers:

1. Select **Configuration : Site Settings : Network Nodes**.
2. Select from the **Name** drop-down list the Nodes whose blades you wish to view.
3. Click the **Blades** tab.
4. In the **Blade Type** column, click the link for the blade you wish to view.
The **Resource Details** column displays what is currently configured for each position.

See also: [Network Node Hardware Installation Guide \(PDF\)](#)

Partition Setup

Overview of Setting Up a Partitioned System

A partitioned system is a single security management system that emulates the behavior of multiple installed systems. Setting up such a system involves creating one or more virtual systems called partitions.

Every system has an initial, default partition called the Master partition. This partition cannot be renamed or deleted. When a new node is discovered, it is added to the Master partition automatically.

For a site in which all portals, access levels, and other resources are shared and there is no need to manage individual populations separately, the Master partition is sufficient. Only sites that need to manage multiple resources and/or populations separately will need to create additional partitions. After a corporate acquisition, for example, the purchasing firm may want to add a new partition into which it can import the acquired firm's population, so it can be managed separately.

An administrator who has the full system setup role can set up a partitioned system. The basic steps are as follows:

1. Select **Configuration : Site Settings : Partitions**.
2. [Set up named partitions](#) and [move nodes to the appropriate partitions](#).

IMPORTANT: You must move a node to the appropriate partition before configuring its resources.

3. Grant users access levels and roles in individual partitions as needed. For instructions, see [Granting User Roles and Access Levels in a Partition](#).

4. Create card formats in the Master partition. See [Specifying Card/Keypad Formats](#). Card key formats cannot be created in the individual partitions.
5. Select **Monitor : Select Partition**, select each partition in turn, and configure its portals, access levels, readers, cameras, and other resources.

See also: [Setting Up Partitions](#)

[Selecting a Different Partition](#)

Setting Up Partitions

Select **Configuration : Site Settings : Partitions**.

Partitions are virtual systems that allow a single security management system to emulate multiple installed systems. Within a partitioned system, nodes (and all of their resources) located in one partition are managed separately from those in other partitions. Similarly, video management systems configured in one partition are managed separately from those in other partitions.

Initially, each system has a default partition called the **Master** partition. If a decision is made to set up a partitioned system, an administrator with the **full system setup** role can use this page to:

- Create and delete named partitions, as described below.
- [Grant user roles and access levels and roles in a partition.](#)
- [Move a new node to a named partition.](#)
- [Move nodes between partitions, as described below.](#)
- [Move video management systems between partitions.](#)

To create a partition:

1. Select **Configuration : Site Settings : Partitions**.
Tables on the page show all user roles, access levels, nodes, and video servers in the active partition.
3. Click the **add** link under the **Name** drop-down list and enter a name for the new partition.
4. Enter a **Description** that will help identify the partition.
5. If you want the partition to send its node status to the Master partition, select the **Forward Node Activity** check box.
6. Click **Save**.

The User Roles table changes to reflect the default user roles defined in the new partition. The Access Levels table will be blank until access levels are defined in the partition. These tables can be used to [grant user roles and access levels](#) in the partition to users in other partitions.

The Network Nodes and Video Management Systems tables will be blank until nodes and video management systems are moved to the new partition.

To delete a partition:

1. Select **Configuration : Site Settings : Partitions**.
2. Select a partition (other than the Master partition) from the **Name** drop-down list.

3. Click **Delete**, and then click **Yes** to confirm the deletion.

If resources such as inputs, outputs, and portals are defined in the partition, you will see an error message indicating that the partition is in use by one or more items. You will need to remove those resources before you can delete the partition.

To move a node to a different partition:

IMPORTANT: If you have moved a node to the wrong partition you can move it to a different partition, *as long as you have not yet configured its resources*. Once you start to define resources for a node in one partition, you will not be able to move it to a different partition without first moving ALL resources currently assigned to it.

1. Select **Configuration : Site Settings : Partitions**.
2. Select a partition from the **Name** drop-down list.
All nodes defined in the active partition are listed in the Network Nodes table.
4. On the **Move to partition** drop-down list for the node or video management system you want to move, select the name of the destination partition.
5. Click **Save**.
Now you can select **Monitor : Select Partition**, change to the partition you just moved, and specify its inputs, outputs, portals, and other resources.

See also: [Selecting a Different Partition](#)

[Overview of Setting Up a Partitioned System](#)

[Granting User Roles and Access Levels in a Partition](#)

[Adding a New Node to a Partition](#)

[Granting administrators in other partitions limited access to person records](#)

Granting User Roles and Access Levels in a Partition

Select **Configuration : Site Settings : Partitions**.

Sometimes users in other partitions will need access to resources and/or populations in your partition. To give the users the access they need, you can grant them access levels and roles in your partition based on their access levels and roles in other partitions.

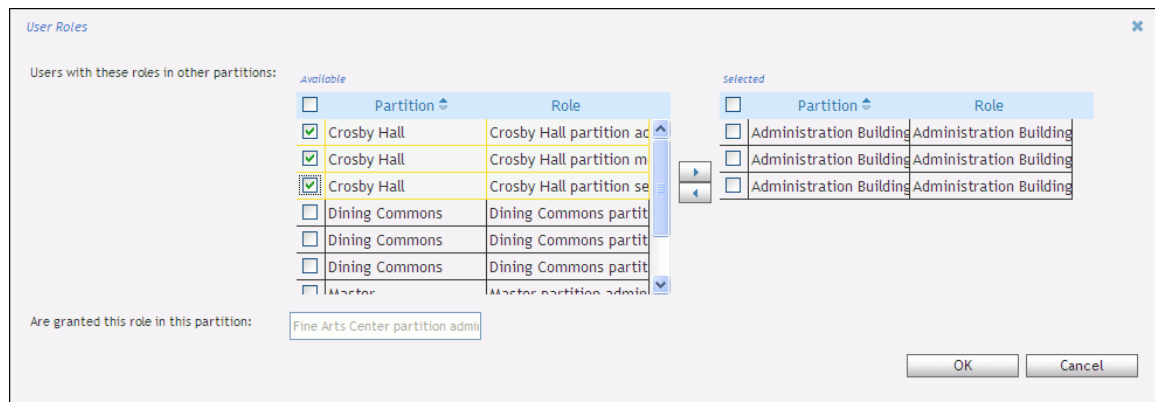
To grant user roles in a partition:

1. Select **Configuration : Site Settings : Partitions**, and select a partition from the **Name** drop-down list.
The user roles defined in the selected partition are listed in the right column of the **User Roles** table.
2. Click the edit icon for a user role.

The **User Roles** dialog box appears. The **Available** list shows all user roles defined in other partitions.

3. Select one or more of the entries in the **Available** list and click the right-arrow button to move them to the **Selected** list. To remove an entry, select it and click the left-arrow button to move it back to the **Available** list.

For example, suppose you want to grant the Fine Arts Center's administrator role to users with any of the roles defined for the Administration Building and Crosby Hall. The following example shows the dialog box after the three roles defined in the Administration Building partition have been moved to the Selected list for the Fine Arts Center partition. The three roles defined in the Crosby Hall partition are selected and ready to be moved to the Selected box as well.



4. Select the check boxes for the roles you moved to the **Selected** list.
5. Click **OK** to close the dialog box.

For the user role you modified, the left column of the **User Roles** table now indicates the roles a person must have in other partitions to be granted that role in the selected partition.

6. Repeat steps 2 through 4 for each additional user role you want to grant to users in the selected partition.
7. Click **Save**.

To grant access levels in a partition:

1. Select **Configuration : Site Settings : Partitions**, and select a partition from the **Name** drop-down list.
The access levels defined in the selected partition are listed in the right column of the **Access Levels** table.
2. Click the edit icon for an access level.
The **Access Levels** dialog box appears. The **Available** lists shows all access levels defined in other partitions.
3. Select one or more of the entries in the **Available** list and click the right-arrow button to move them to the **Selected** list. To remove an entry, select it and click the left-arrow button to move it back to the **Available** list.
4. Select the check boxes for the access levels you moved to the **Selected** list.
5. Click **OK** to close the dialog box.

For the access level you modified, the left column of the **Access Levels** table now indicates the access levels a person must have in other partitions to be granted that access level in the selected partition.

6. Repeat steps 2 through 4 for each additional access level you want to grant to users in the selected partition.
7. Click **Save**.

See also: [Setting Up Partitions](#)

[Overview of Setting Up a Partitioned System](#)

[Selecting a Different Partition](#)

Selecting a Different Partition

Select **Change Partition** from the [command palette](#).

In the dialog box that appears, you can select a different partition to make it the active partition. You will then be able to do the following, depending on your permissions in the partition:

- Monitor activity in the partition.
- Perform administrative functions in the partition.
- Set up and configure resources for the partition.

To select a different partition:

1. After selecting **Change Partition** from the command palette, select the partition in which you want to work.
2. Click **OK** to close the dialog box.
3. Click **OK** to confirm that you want to make that partition the active partition.

NOTE: If you have the full system setup role, you can also select a different partition from the [Node Status](#) page. Clicking the link for a node automatically makes its partition the active partition.

See also: [Setting Up Partitions](#)

[Overview of Setting Up a Partitioned System](#)

Moving a New Node to a Named Partition

Select **Configuration : Site Settings : Partitions**.

After creating a new node and pointing it to the controller, you can move the node from the Master partition to a named partition and then configure it in the named partition.

IMPORTANT: Once a node has been enabled and configured in the Master partition, moving the node to another partition would require that you first move ALL resources currently assigned to it.

To move a new node to a partition:

1. Add a node to the network and use the Network Node Configurator (nnconfig.exe) to point it to the controller. For instructions, see [Tech Note 4: Connecting Nodes and Controllers Across Subnets \(PDF\)](#).

IMPORTANT: Do not configure the new node in the Master partition. You must move it to the correct partition before configuring it.

2. Select **Configuration : Site Settings : Partitions**.
3. Select the **Master** partition from the **Name** drop-down list.
In the **Network Nodes** section at the bottom of the page, you will see the unique identifier of the node you added at step 1.
5. On the **Move to partition** drop-down list, select the partition to which you want to move the new node.
6. Click **Save**.
7. Select **Monitor : Select Partition** and switch to the partition where you moved the node, or select **Configuration : Site Settings : Network Controller** and click the new node to switch to its new partition automatically.
8. Select **Configuration : Network Nodes**, rename the node, enter all the settings you applied to it using the nnconfig utility, and then click **Save**.
9. Select the **Enabled** check box, and then click **Save** again.

See also: [Setting Up Partitions](#)

[Selecting a Different Partition](#)

[Overview of Setting Up a Partitioned System](#)

[Granting User Roles and Access Levels in a Partition](#)

[Granting administrators in other partitions limited access to person records](#)

Moving Video Management Systems Between Partitions

Select **Configuration : Site Settings : Partitions**.

Once a video management system has been configured in one partition, you can reassign it to a different partition by moving its video server.

IMPORTANT: Be sure to move a video server BEFORE doing any of the following: configuring virtual events for its cameras, assigning its cameras to camera views or floorplans, or either linking its cameras to events or using them in event actions. If any camera has associations with virtual inputs, camera views, floorplans, or events, you will not be able to move the camera to a different partition until you remove these associations.

Special Requirements for Milestone XProtect Corporate Integrations

For a Milestone XProtect Corporate integration, which includes a management server and separate recording servers rather than a single video server, the management server and/or its individual recording servers can be moved to other partitions. Moving recording servers to other partitions may be useful in the case of multi-tenant facilities or varied geographic locations. It allows direct supervision of the recording server and associated cameras at a specific site, while maintaining system management at a central facility or location.

- When you move the management server, the associated recording servers are not moved to the new partition automatically. If you want to move a recording server, you must move it individually to the desired partition.
- When you move a recording server, all cameras managed by that server are moved to the new partition automatically.

The partition where the management server resides will control the registration and updating of the overall camera list and recording server list.

To move a video management system to a different partition:

1. Select **Configuration : Site Settings : Partitions**.
2. Select the partition to which the video management system is currently assigned.
The **Video Servers** table lists the video server for each video management system assigned to the selected partition. For a Milestone XProtect Corporate integration, the table lists the management server, and below it, an entry for each of its associated recording servers (listed by their hostnames).
3. On the **Move to partition** drop-down list for the server you want to move, select the name of the destination partition.
4. Click **Save**.

See also: [Setting Up Partitions](#)

[Selecting a Different Partition](#)

[Updating an NVR Integration](#)

ASSA ABLOY Remote Lockset Setup

Overview: Integrating ASSA ABLOY Remote Locksets

Once an ASSA ABLOY remote lockset has been installed and is connected to the controller, its name appears in the system as "Remote Lockset" followed by the lockset's unique identifier. For information on installing remote locksets and testing their connection to the controller, refer to [Tech Note 15: Integrating ASSA ABLOY Remote Locksets \(PDF\)](#).

CAUTION: If you are configuring a PoE-powered lockset, you MUST select "Use alternate PoE communication mode" in the ASSA ABLOY Network Configuration Tool (NCT). This switches the lock to the periodic call mode that S2 currently supports. The PoE lock requires the NCT and LCT version 2.0 or later and this setting to configure the PoE (Power Over Ethernet) communication mode compatible with S2 systems.

If you do not select this option, the PoE lock will continuously attempt to contact the controller. **If this situation continues, it will eventually cause permanent damage to the lockset hardware.**

Note: The status of a remote lockset will not be displayed on the Portal Status page or elsewhere in the user interface.

About Offline and Online Remote Locksets

When a remote lockset connects to the controller, it reports its power type, which is encoded in its serial number.

- If the lockset reports that it runs exclusively on batteries, without a backup power source, it is treated as an offline lockset.
- If the lockset reports that it runs on PoE (Power over Ethernet) or external power, with or without battery backup, it is treated as an online lockset.

You can use a lockset's serial number to determine whether it will be treated as an offline or online lockset. Serial numbers take the form XXywwBssss-MNHHPL, where P is the power source. P can be one of the following:

- A - Batteries (offline)
- B - External power
- C - PoE
- D - External power with battery backup
- E - PoE with battery backup

Configuring Remote Locksets

To configure remote locksets you can:

- [Enable the locksets and set their configuration options.](#)
- [Create remote lockset profiles](#) to make configuring and managing large numbers of remote locksets easier.
- [Configure advanced options for the locksets.](#)
- [Set up the readers associated with the locksets.](#)
- [Add the remote-lockset readers to a reader group](#) so the readers can be assigned to access levels.
- [Set up the portals associated with the locksets.](#)
- [Add the remote locksets to a portal group](#) so an unlock period can be scheduled for the locksets.
- [Assign remote lockset user types to the access cards that will be used with the locksets.](#)

Once an online or offline remote lockset has been configured, users can do the following:

Task	Procedure
View the lockset's communication status.	Viewing Remote Lockset Status
Monitor the operation of the lockset with the controller.	Monitoring the Activity Log
Reconfigure the reader and portal associated with the lockset.	Configuring Remote Lockset Advanced Options
View cached information for the lockset, for troubleshooting purposes.	Viewing Cached Information for a Remote Lockset
Run the Remote Locksets configuration report to view information about the lockset.	Configuration Reports

In addition, for an *online* remote lockset, users can do the following:

Task	Procedure
	<p>Momentarily unlock the lockset. Define a Momentary Unlock event action on the Events page.</p> <p>- or -</p> <p>Click the Momentarily Unlock Portal button on the Portal Status page or in the Portal Status or Portal Unlock widget.</p>
<p>Switch the lockset to a persistent locked or unlocked state.</p>	<p>Define an Unlock Portal or Lock Portal event action on the Events page.</p> <p>- or -</p> <p>Click the Unlock Portal or Lock Portal button on the Portal Status page or in the Portal Status or Portal Unlock widget.</p>
<p>Schedule an extended lock or unlock of the lockset.</p>	<p>Schedule an Unlock or Lock action using:</p> <ul style="list-style-type: none"> • the Schedule Action page • the Portal Status page • the Portal Status or Portal Unlock widget • a Floorplan <p>NOTE: If a lockset that has been put into a locked state by a scheduled action is unlocked by an event, it does not return to the locked state once the event ends.</p>
<p>Disable and enable the lockset.</p>	<p>Click the Disable Portal or Enable Portal button on the Portal Status page or in the Portal Status or Portal Unlock widget.</p>
<p>Use threat levels to cause the lockset to enter and exit panic mode.</p>	<p>Optionally, assign the lockset to a location, and assign a threat level group to the lockset.</p>

Enabling and Configuring ASSA ABLOY Remote Locksets

Select **Configuration : Site Settings : Network Nodes**.

On this page, a node that has been set up for an ASSA ABLOY remote lockset appears on the **Name** drop-down as "Remote Lockset" followed by the lockset's unique identifier. To configure the lockset you can:

- Enable the lockset and set its time zone for scheduling purposes.
- Configure events for the lockset.
- Swap the lockset's unique identifier with that of another lockset. *Call for support if you have any questions or problems when using this option.*
- Reload all configuration information into the lockset.

For information on configuring advanced options for a remote lockset, see [Configuring Remote Lockset Advanced Options](#). For general information on node configuration, see [Configuring Network Nodes](#).

To enable a remote lockset and set its time zone:

1. Select the name of the lockset from the **Name** drop-down list.
2. If the lockset is disabled, select the **Enabled** check box to enable it.
The **Status** drop-down list displays one of the following states for the lockset:
 - **Connection Scheduled:** The lockset has called in and the Network Controller has communicated with it and given it a regular schedule.
 - **Connection Overdue:** The lockset has not called in according to its schedule.
 - **Disconnected:** The controller has never communicated with the lockset.
3. To change the lockset's time zone, select an entry from the **Timezone** drop-down list.
4. Click **Save**.
Your changes will take effect the next time the lockset calls in.

To view network settings for a remote lockset:

1. Select the name of the lockset from the **Name** drop-down list.
2. Click the **Network** tab to view the lockset's network settings. Among the settings are:
 - **Lock AES Key:** The Lock AES Key that is used to communicate end-to-end with the controller. The key was set by the network administrator, using the ASSA ABLOY Network Configuration Tool.
 - **IP Address:** The IP address for the lockset, which is set remotely.
 - **Allow Network Controller autodiscovery:** Remote locksets always use auto-discovery to find their controllers.
 - **Network Controller IP Address:** The IP address the lockset used to contact the controller.
 - **Last Modified:** The last time the administrator modified configuration settings for the lockset.
 - **Last Connection:** The last time the lockset called in to the controller. Note that if this time is more recent than the Last Update Completed time (described below), you should check the lockset's status. If the situation persists, you will need to troubleshoot the lock.
 - **Last Update Completed:** The last time the controller had a successful session with the lockset.
 - **Firmware Version:** The version number of the lockset firmware.
 - **Battery Voltage** (applies to offline locksets only): The battery voltage output the last time it was sampled by the lockset.

To configure events for a remote lockset:

1. Select the name of the lockset from the **Name** drop-down.
2. Click the **Events** tab.
3. Select any or all of the following events for the lockset:

- A **Low Battery Event** (applies to offline locksets only) to be activated if the battery voltage drops below the **Low Voltage** setting specified in the assigned [Remote Lockset profile](#).
 - A **Tamper Alarm Event** to be activated if someone tampers with the lockset—for example, by attaching a cable to it.
 - A **Timeout Event** to be activated, for example, if the lockset becomes overdue for a scheduled call-in.
 - A **Disconnect Event** to be activate, for example, if the lockset is disconnected in the middle of a session with the controller.
4. Once you have selected an event, select its **Enabled** check box to enable it.
 5. Click **Save**.

For more information, see [Specifying Node Events](#).

To reload all configuration information into a remote lockset:

1. Select the name of the lockset from the **Name** drop-down.
2. Click the **Commands** tab.
3. Click **Reload Node** and click **OK** to confirm.

The lockset is completely reconfigured. All credentials are removed, and then a full credential download is performed. This procedure is typically used when a lockset has been tampered with or is behaving strangely.

NOTE: [Restoring the database](#) or performing an upgrade has the same effect on all ASSA ABLOY locksets as clicking Reload Node.

As of Release 4.8.01, a change to a credential anywhere in the system causes the controller to run an update session with each online lockset, bringing its configuration information and credentials into sync. This is similar to what happens when the locksets call in for their daily configuration updates.

For information on using the **Swap** button on the Commands tab to swap remote lockset unique identifiers, see [Using Node Command Buttons](#).

See also: [Overview: Integrating Remote Locksets](#)

[Configuring Remote Lockset Advanced Options](#)

[About the Remote Lockset Advanced Options](#)

[Creating Remote Lockset Profiles](#)

[Viewing Remote Lockset Status](#)

[Viewing Cached Information for a Remote Lockset](#)

[Monitoring Remote Locksets](#)

[About Remote Lockset User Types](#)

[Remote Locksets Report](#)

[Integrating ASSA ABLOY Remote Locksets \(PDF\)](#)

Configuring ASSA ABLOY Remote Lockset Advanced Options

Select **Configuration : Site Settings : Network Nodes**.

On this page, a node that has been set up for an ASSA ABLOY remote lockset appears on the **Name** drop-down as "Remote Lockset" followed by the lockset's unique identifier. When a remote lockset is selected, you can use the **Advanced** tab to:

- [Display the lockset's advanced settings.](#)
- [Assign a different lockset profile to the lockset.](#) The attributes defined in the assigned profile affect the lockset's behaviors, such as its call-in and lockout behaviors.
- [Clone an existing lockset profile, modify it, and assign the new profile to the lockset.](#)
- [Configure the reader and portal that were created automatically for the lockset.](#)
- [View cached information for the lockset, for troubleshooting purposes.](#)

For information on additional settings you can configure for a remote lockset, see [Enabling and Configuring Remote Locksets](#).

To display a lockset's advanced settings:

1. Select the name of the lockset from the **Name** drop-down list.
2. Click the **Advanced** tab.

The selected lockset's **Connection** type and **Power Source** (which is encoded in its serial number) are displayed at the top of the page. If the lockset reports having PoE (Power over Ethernet) or direct hardwired power, it is treated as an online lockset. If the lockset reports having only batteries as a power source, it is treated as an offline lockset.

Most of the other fields on this tab are read-only. They display the settings configured in the lockset profile currently assigned to the lockset.

To assign a different profile to the lockset:

1. Select the profile you want to assign to the lockset from the **Lockset Profile** drop-down list.
The settings for various options on this tab may change to reflect the settings in the new profile. For more information on these options, see [About the Remote Lockset Advanced Options](#) and [Creating and Editing Remote Lockset Profiles](#).
2. Click **Save**.

To clone a profile, modify it, and assign the new profile to the lockset:

1. Save any changes you have made on the Network Nodes page.
CAUTION: Once you clone an existing profile and save it as a new profile, all unsaved changes on the Network Nodes page will be lost.
2. Click the **clone** link next to the **Lockset Profile** drop-down list.

The Remote Lockset Profiles page opens in a new window.

3. In the **Name** field, enter a name for the new profile.
4. Change any of the settings you want. For more information, see [Creating and Editing Remote Lockset Profiles](#).
5. Click **Save**.

The new profile is applied to the lockset and saved for future use.

To configure the reader and portal for a remote lockset:

1. To change the name of the reader associated with the lockset, click the **Reader** link to open the **Readers/Keypads** page. For information on configuring readers, see [Setting Up Readers/Keypads](#).
2. To configure the portal associated with the lockset, click the **Associated Portal** link to open the **Portals** page. For information on configuring portals, see [Setting Up Portals](#).

NOTE: When you delete a remote lockset, its associated reader and portal are also deleted. You cannot delete the reader or portal directly.

The associated reader can be part of any reader group. It supports time specs but does not respond to threat level information. The associated portal can be part of a portal group, but the **Unlock Time Spec** option is not supported at this time.

See also: [Overview: Integrating Remote Locksets](#)

[Enabling and Configuring Remote Locksets](#)

[About the Remote Lockset Advanced Options](#)

[Creating and Editing Remote Lockset Profiles](#)

[Viewing Remote Lockset Status](#)

[Viewing Cached Information for a Remote Lockset](#)

[Monitoring Remote Locksets](#)

[About Remote Lockset User Types](#)

[Remote Locksets Report](#)

[Integrating ASSA ABLOY Remote Locksets \(PDF\)](#)

About the ASSA ABLOY Remote Lockset Advanced Options

When an ASSA ABLOY remote lockset is selected on the Network Nodes page, the following read-only fields on the [Advanced tab](#) show the settings in the currently selected [lockset profile](#):

- If the **Not in Node Events** check box is selected, the lockset will call in with an alarm when an access attempt is made with unknown credentials.
- The **Call-in Schedule** field shows the time range during which the lockset will call in for its scheduled configuration updates. The default time range is 1 AM to 6 AM.

- The **Call-in Keypad Code** field shows the six-digit PIN code that, when entered into the lockset's keypad, will cause the lockset to call the controller immediately.
- The **Low Voltage is under** field (applies to offline locksets only) shows the voltage level below which the lockset will go into power saving mode. If a Low Battery event is enabled for the lockset (on the [Events tab](#) of the Network Nodes page), the event will be activated.
- The **Call Required Every** field shows when the controller will raise an alert if it has not heard from the lockset. For example, if a lockset is set to call in once per day, but you set this option to **2 days**, no alarm will occur unless the lockset has not called in for two days.
- The **Remote Auth Time Limit** field shows how long the lockset will wait for acknowledgment from the system that a person is authorized for access before timing out. If **Reswipe** is selected, the lockset will time out immediately and the person will need to present the credentials again to gain access.
- The **Session Wait Timeout** field shows how long the lockset will wait to establish a connection with the Network Controller before timing out. The specified time includes the time required for powering up the lockset.
- If the **Retry on Timeout** check box is selected, the lockset will try again to establish a connection after a timeout.
- The **Daily Battery Check** field (applies to offline locksets only) shows the time of day the lockset will pulse the activator so it can read the voltage meter.
- The **Lockout Attempt Limit** field shows how many consecutive rejections of an access attempt will be allowed before a lockout occurs. If **Disable** is selected, an unlimited number of access attempts will be allowed.
- The **Lockout Duration** field shows how long a lockout will last.
- Selected check boxes for **Valid Entry**, **Access Denied**, **Door Secure**, **Door Forced**, **Door Held**, **Low Battery** (applies to offline locksets only), and **REX Held** indicate the alarm events the lockset will report when it is in passage mode and when it is not in passage mode.

NOTES: As of Release 4.8.01, a change to a credential anywhere in the system causes the controller to run an update session with each online lockset, bringing its configuration information and credentials into sync. This is similar to what happens when the locksets call in for their daily configuration updates.

Passage mode is activated either at the start of the scheduled unlock period for a portal, or when a user presents a Toggle Passage Mode card. Although the lockset is in passage mode, it is not actually unlocked until a valid card is presented.

See also: [Overview: Integrating Remote Locksets](#)

[Enabling and Configuring Remote Locksets](#)

[Configuring Remote Lockset Advanced Options](#)

[Creating Remote Lockset Profiles](#)

[Viewing Remote Lockset Status](#)

[Viewing Cached Information for a Remote Lockset](#)

[Monitoring Remote Locksets](#)

[About Remote Lockset User Types](#)

[Remote Locksets Report](#)

[Integrating ASSA ABLOY Remote Locksets \(PDF\)](#)

Viewing Cached Information for an ASSA ABLOY Remote Lockset

Select **Configuration : Site Settings : Network Nodes** and click the Advanced tab.

- or -

Select **Administration : Reports : Configuration : Remote Locksets**.

The Remote Node Cache Contents window displays cached information for an ASSA ABLOY remote lockset. This information can be used for troubleshooting purposes.

To view cached information for a remote lockset:

1. Select the lockset on the Network Nodes page, click the Advanced tab, and then click the **See information cached on node** link.

- or -

Click the Status link for the lockset in the [Remote Locksets report](#).

The Remote Node Cache Contents page opens.

2. Click the **Access Card Pending**, **Timespec Pending**, or **Holiday Pending** tab to view information on access cards, time specs, and holidays that will be sent the next time the controller has a session with the remote lockset.
3. Click the **Access Cards Sent** or **Calendar Sent** tab to view information on access cards, time specs, and holidays that have been sent to the lockset.

See also: [Overview: Integrating Remote Locksets](#)

[Enabling and Configuring Remote Locksets](#)

[About the Remote Lockset Advanced Options](#)

[Creating and Editing Remote Lockset Profiles](#)

[Viewing Remote Lockset Status](#)

[Monitoring Remote Locksets](#)

[About Remote Lockset User Types](#)

[Remote Locksets Report](#)

[Integrating ASSA ABLOY Remote Locksets \(PDF\)](#)

Creating and Editing ASSA ABLOY Remote Lockset Profiles

Select **Configuration : Site Settings : Remote Lockset Profiles**.

To make it easier to configure and manage large numbers of ASSA ABLOY remote locksets, you can create lockset profiles.

A lockset profile is a defined set of attributes that affect remote lockset behaviors, such as their call-in and lockout behaviors. Assigning a lockset profile to a remote lockset gives it the attributes defined in the profile. Any subsequent changes made to the profile are applied to the lockset automatically.

Every remote lockset profile is created in the Master partition and is available in all partitions.

NOTE: The first time a remote lockset connects to the controller, it is automatically assigned the **Default** profile. You can edit, rename, or clone this profile, but you cannot delete it.

To create or edit a remote lockset profile:

1. Select the name of the profile you want to edit from the **Name** drop-down list—or click the **add**, **rename**, or **clone** link and then enter a name for the new, renamed, or duplicate profile.
2. (optional) If there is a magnetic card format that you want all locksets created from this profile to use exclusively, select it from the **Card Format** drop-down list.

Select **None** if you do not want to force locksets created from this profile into a specific magnetic stripe card format.

3. (optional) For **Lock AES Key**, enter the 32-character hexadecimal key that will be used to for end-to-end communications with the controller. The key can be any combination of the numbers 1 through 9 and the letters a through f (uppercase or lowercase).

Once you enter and save the lock AES key, the **Encryption Type** changes to **AES** automatically.

4. For **Call-in Keypad Code**, enter a six-digit call-in keypad code that, when entered into a lockset's keypad, will cause the lockset to call the controller immediately. This call-in will be in addition to the lockset's daily call-in.

NOTE: For a magnetic stripe lockset, the system uses the first four digits of the code you enter.

5. For **Low Voltage** (applies to offline locksets only), enter the voltage level below which the lockset will go into power saving mode. If a Low Battery event is enabled for the lockset (on the [Events tab](#) of the Network Nodes page), the event will be activated. The minimum Low Voltage setting is 5.6 and the maximum setting is 7.6.

NOTE: Once the battery is replaced, the lockset will leave power saving mode only when the voltage level reaches 1.5 volts higher than its current Low Voltage setting.

6. For **Calls Per Day**, specify how many times the lockset should try to contact the controller in one day. The options are: **1** time, **2** times, **3** times, or **4** times per day.
7. For **Call Required Every**, specify when the controller should raise an alert if it has not heard from the lockset. For example, if a lockset is set to call in once per day, but you don't want an alarm to occur unless it misses its call for two days, set this option to **2 days**.

NOTE: This field is read-only in the default lockset profile and is set to **1 day**. With this setting, automatic database updates (including cardholder information and configuration changes) will occur once per day between the hours of 1 AM and 6 AM. Database updates will also occur whenever an event is sent to the controller from the lockset, a comm event is generated by the lockset, or the **Reload Node** button is clicked on the [Commands tab](#).

8. For **Remote Auth Time Limit**, specify how long the lockset should wait for the system to acknowledge that a person is authorized for access before timing out. Select **Reswipe** to have the lockset time out immediately. With this setting, the person will need to present his or her credentials again to gain access.

Select **Disable** if you do not want the lockset to call the controller when a card is presented that is not in its list of credentials.

9. For **Session Wait Timeout**, specify how long the lockset will wait to establish a connection with the controller before timing out. The time you specify will need to include the time required for powering up the lockset.
10. Select the **Retry on Timeout** check box if you want the lockset to try again to establish a connection after a timeout.

IMPORTANT: It is recommended that you select **Retry on Timeout** only for troubleshooting purposes. In the event of a power outage, for example, the lockset will continue trying to connect. Because the lockset radio will power up for each connection attempt, it may run down its battery.

11. For **Daily Battery Check** (applies to offline locksets only), specify the time of day the lockset will pulse the activator so it can read the voltage meter.

NOTE: The battery voltage is routinely checked whenever someone uses the lockset, and a low voltage warning will be raised if there is no use for 24 hours. Therefore, a daily battery check is recommended only for low-use locksets whose batteries might wear out unexpectedly after long periods of inactivity. If you do use this option, you should select a time when people are least likely to be disturbed by the sound the lockset makes when it pulses the activator.

12. For **Lockout Attempt Limit**, specify how many consecutive rejections of an access attempt will be allowed before a lockout occurs. Select **Disable** to allow an unlimited number of access attempts.
13. For **Lockout Duration**, specify how long a lockout will last.
14. Select the **Not In Node** check box to have the lockset to call in with an alarm when an access attempt is made with unknown credentials.
15. In the **Alarm Events** table, select the check boxes for the alarm events you want the lockset to report when the portal is in passage mode and when it is not in passage mode.

NOTES: As of Release 4.8.01, a change to a credential anywhere in the system causes the controller to run an update session with each online lockset, bringing its configuration information and credentials into sync. This is similar to what happens when the locksets call in for their daily configuration updates.

Passage mode is activated either at the start of the scheduled unlock period for a portal, or when a user presents a Toggle Passage Mode card. Although the lockset is in passage mode, it is not actually unlocked until a valid card is presented.

When setting profile options that affect the call-in behaviors of a remote lockset, such as the **Not in Node** and **Alarm Events** options, you will need to balance the need to conserve battery power against the need for immediate information.

See also: [Overview: Integrating Remote Locksets](#)

[Enabling and Configuring Remote Locksets](#)

[Configuring Remote Lockset Advanced Options](#)

[About the Remote Lockset Advanced Options](#)

[Viewing Remote Lockset Status](#)

[Viewing Cached Information for a Remote Lockset](#)

[Monitoring Remote Locksets](#)

[Overview: Integrating Remote Locksets](#)

[About Remote Lockset User Types](#)

[Remote Locksets Report](#)

[Integrating Remote Locksets \(PDF\)](#)

Viewing ASSA ABLOY Remote Lockset Status

Select **Configuration : Site Settings : Node Status**.

The table at the bottom of this page shows all ASSA ABLOY remote locksets in the active partition. If you have the full system setup user role, the table shows all remote locksets in the system, organized by partition.

Remote locksets whose serial numbers appear in **green** are enabled and communicating with the Network Controller. Remote locksets whose serial numbers appear in **red** are not currently communicating with the controller.

As shown in the following example, the Remote Lock column contains a link for each lockset. Clicking the link opens the Network Nodes page, where you can view and modify the lockset's configuration settings.

Partition	Remote Lock	Serial Number	Status	Call-in Time	IP Address	Last Complete Update
Master	Remote Lockset IT123J0002PA01CC	IT123J0002PA01CC	Scheduled	09:30:00	74.251.175.18	2010-01-22 15:56:09.941858
Master	Remote Lockset IT527J1851PC09AA	IT527J1851PC09AA	Connection overdue!	04:00:00	192.168.51.171	2010-01-15 14:52:26.031184
Master	Remote Lockset IT930H1487SC03AA	IT930H1487SC03AA	Scheduled	03:46:00	192.168.51.170	2010-01-22 13:02:38.01092

See also: [Overview: Integrating Remote Locksets](#)

[Enabling and Configuring Remote Locksets](#)

[Configuring Remote Lockset Advanced Options](#)

[About the Remote Lockset Advanced Options](#)

[Viewing Cached Information for a Remote Lockset](#)

[Creating Remote Lockset Profiles](#)

[Setting Up the Network Controller](#)

[Configuring Network Nodes](#)

[Monitoring Remote Locksets](#)

[About Remote Lockset User Types](#)

[Remote Locksets Report](#)

[Integrating ASSA ABLOY Remote Locksets \(PDF\)](#)

About ASSA ABLOY Remote Lockset User Types

When you are [issuing a new credential](#) to be used with ASSA ABLOY remote locksets, you can assign any of the remote lockset user types listed below. Your assignment will affect the user's access and abilities at portals currently accessible to the user based on his or her access levels.

Once a card has been assigned a remote lockset user type, it is no longer usable as an access card. The exception is **Regular Access Card**, which allows a card to function with both remote locksets and regular locks. This is the user type you will select for the majority of the users in your system.

NOTE: Users whose cards have been assigned any of the user types listed below, except **Emergency Open**, may be constrained by time specs. That is, the users may be denied access or functionality at a portal for which a time spec is in effect.

- **Regular Access Card:** By presenting this card, a user can momentarily unlock the remote lockset (or regular lock). The card gives the user no special abilities. For example, the user's credentials will not be accepted during lockout and panic modes (described below).
- **Trigger Comm Update:** By presenting this card, a user can start a communications session between the remote lockset and the controller.
- **Toggle Passage Mode:** By presenting this card, a user can toggle the remote lockset between passage mode (described below) and the locked state.
- **Relock Passage:** By presenting this card, a user can relock the lockset if it is in an unlocked state for any reason, but cannot unlock it. When passage mode ends (at the end of the scheduled unlock period for the portal), the relock request is discarded and the lock returns to normal operation. This user type is useful, for example, when a lockset must be re-locked before its scheduled lock time.
- **Panic Lockdown:** By presenting this card, a user can place the lockset into panic mode.
- **Lockout Users:** By presenting this card, a user can toggle the remote lockset between lockout mode and normal operation. Note that the door does not unlock when it goes into lockout mode; the card cannot be used to gain access. This user type is especially useful for preventing people from entering an area where a dangerous situation has been identified.
- **Master Clear Lockouts:** By presenting this card, a user is never granted access but is able to clear panic, lockout, and relock modes for the remote lockset.
- **Emergency Open:** By presenting this card, a user can unlock the remote lockset for emergencies, regardless of panic, lockout, or relock modes—and in spite of low battery situations for battery powered locksets. If passage mode is in effect when the user presents the card, the lockset returns to passage mode. Otherwise, the lockset remains unlocked for the duration of the [Extended Unlock Time](#) specified in the portal definition.
- **Supervisor Open:** By presenting this card, a user can unlock the remote lockset regardless of lockout mode, but cannot override panic mode.

NOTES: Sx locksets support all user types listed above. Px locksets support only the Regular Access Card, Trigger Comm Update, and Supervisor Open user types.

The Panic Lockdown user type observes time specs, but the Emergency Open user type ignores them.

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

About Remote Lockset Modes

- **Passage mode:** Activated either at the start of the scheduled unlock period for the portal, or when a user presents a **Toggle Passage Mode** card. Although the lockset is in passage mode, it is not actually unlocked until a valid card is presented.
- **Lockout mode:** Activated when a user presents a **Lockout Users** card. If the lockset is in passage mode, it is re-locked. Access is granted only to users who present **Master Clear Lockouts**, **Emergency Open**, or **Supervisor Open** cards. Lockout mode can be cleared by any user with a **Lockout Users** or **Master Clear Lockouts** card.
- **Panic mode:** Activated when a user presents a **Panic Lockdown** card or when a remote command is issued. It immediately cancels passage mode and locks out all users except those with **Master Clear Lockouts** and **Emergency Open** cards for the duration of the panic. Panic mode can be cleared by a user with a **Master Clear Lockouts** card or via a command from the server.

See also: [Overview: Integrating Remote Locksets](#)

[Enabling and Configuring Remote Locksets](#)

[Configuring Remote Lockset Advanced Options](#)

[About the Remote Lockset Advanced Options](#)

[Creating Remote Lockset Profiles](#)

[Creating Time Specs](#)

[Viewing Remote Lockset Status](#)

[Monitoring Remote Locksets](#)

[Remote Locksets Report](#)

[Integrating Remote Locksets \(PDF\)](#)

Using Threat Levels to Initiate ASSA ABLOY Remote Lockset Panic Mode

ASSA ABLOY [online remote locksets](#) have many of the capabilities of standard portals. This includes the ability to change their behavior based on threat level changes. The following procedure describes how to have an online remote lockset enter and exit [panic mode](#) based on changes to its location's threat level.

To have an online remote lockset enter and exit panic mode based on threat level changes:

1. (optional) Assign the lockset to a specific [location](#) in the active partition.
By default, the lockset's location is the default location in the active partition.
2. Create a [threat level group](#) that excludes any threat level under which the lockset should enter panic mode.
For example, if you want the lockset to enter panic mode when its location's threat level changes to Severe, exclude the Severe threat level from the threat level group.
3. Assign the threat level group to a new or existing [portal group](#).
4. Add the online lockset to the portal group.
The lockset will lock and unlock according to the portal group's assigned time spec. If the lockset's location changes to a threat level that is not in the threat level group you assigned at step 3, the lockset will enter panic mode. When that location's threat level returns to normal, the lockset will exit panic mode.

NOTE: If a lockset has been put into panic mode and subsequently loses power, it exits panic mode. Panic mode is not restored until the next time the lockset's location changes to a threat level under which it should enter panic mode.

See also: [Overview: Integrating Remote Locksets](#)

[Setting Up Threat Level Groups](#)

[Using Threat Levels to Change System Behavior](#)

[Setting Up Portal Groups](#)

[Setting Up Locations](#)

[Integrating ASSA ABLOY Remote Locksets](#)

Creating Partial-Match Card Formats for ASSA ABLOY Remote Locksets

Select **Configuration : Access Control : Card/Keypad Formats**.

If the magnetic stripe access cards you will use with ASSA ABLOY remote locksets include encoded data you do not want sent to the controller, you can create a partial-match card format and assign it to the locksets via a [lockset profile](#). The partial-match format will instruct the locksets to match only a part of the encoded data—such as the card ID number—when validating a card read, and to send only the matched data to the controller.

NOTE: The encoded data to be matched must be a contiguous set of bytes; variable-length fields are not supported.

To create a partial-match magnetic stripe ABA Track 2 format:

1. Click the **add** link under the **Name** drop-down list.

NOTE: If you are adding a card format that is substantially similar to an existing format, you can save time by selecting that format from the drop-down list, clicking the **clone** link, entering a new **Name**, and making any needed changes to the new format.

2. Enter a **Name** for the new card format. This is a required entry.
3. Enter a **Description** for the card format.
4. From the **Data Format** drop-down list, select **Magstripe Track 2**.
5. In the **Length** text box, enter the number of **bytes** in this card format. This is a required entry. The number entered here determines the number of byte definition drop-down lists provided below.
6. Check the card manufacturer's documentation for the facility code of the card batch you are using. Enter this number in the **Facility Code** field.

NOTE: Make sure the facility code for keypads differs from the facility codes used in the card population. It is important that the system recognize keypad input as separate from card reads. For instructions on setting keypad facility codes, refer to the keypad manufacturer's documentation.

7. Enter in the following four fields the correct start byte and byte length values for the format you are creating:
 - **Facility Code Start:** The first byte of the facility code number.
 - **Facility Code Length:** The number of bytes used to indicate the facility code.
 - **Encoded # Start:** The first byte of the card ID number.
 - **Encoded # Length:** The number of bytes used to indicate the card ID number.

NOTE: If you want your system to ignore the facility code when validating card reads, enter a zero (0) in each of the following fields: **Facility Code**, **Facility Code Start**, and **Facility Code Length**.

8. Select the **Hot Stamp and encoded numbers default identical** check box if the number printed on the card is the same as the encoded number. If this box is checked, whenever you enroll a card using a reader or manually enter a number in the **Hot Stamp #** field, the system populates both **Hot Stamp #** and **Encoded #** fields with the same value.
9. To ensure that the new card format will be recognized by remote locksets with magnetic stripe card readers, select the **Magnetic Stripe Remote Lockset supported** check box.
10. **Byte definitions in card format:** These drop-down lists will fill in automatically when you complete step 7 above. The number of byte drop-down lists will match the number you entered in the **Length** box at step 5.
 - F is for a facility code byte.
 - N is for a card number byte.
 - ? is for an unmatched character.
 - SS is a Start Sentinel byte with the ASCII value ";".
 - ES is an End Sentinel byte with the ASCII value "?".
 - LRC is a checksum character.
11. Click **Save**.

See also: [Handling Lost Cards](#)

[Changing a Person's Access](#)

[Decoding Cards](#)

[Access Card Formats](#)

[Setting Up Readers and Keypads](#)

[About Remote Lockset User Types](#)

[Entering PINs at ASSA ABLOY Sx and Px Locksets](#)

Entering PINs at ASSA ABLOY Sx and Px Locksets

The following table summarizes the steps for entering PINs at ASSA ABLOY Sx and Px remote locksets. A lockset can be configured to require entry of one or both of the following PINs (which appear on the Access Control tab of a person record):

- **Credential PIN:** This is the six-digit PIN entered in the **Hot stamp #** field for a *Remote Lockset PIN Only* credential assigned to the person record.
- **Person PIN:** This is the four-digit or 6-digit PIN entered in the **PIN** field for the person.

Sx locksets require six-digit person PINs. Px locksets require four-digit person PINs.

Lockset Type	Reader/Keypad Type	Person PIN?	Steps for Entering PINs
Sx	PIN-only	No	<ol style="list-style-type: none"> 1. Enter six-digit credential PIN 2. Enter *
Sx	PIN-only	Yes	<ol style="list-style-type: none"> 1. Enter six-digit credential PIN 2. Enter * 3. Enter six-digit person PIN 4. Enter *
Sx	Non-magnetic card	Yes	<ol style="list-style-type: none"> 1. Present card 2. Enter * 3. Enter six-digit person PIN 4. Enter *
Px	PIN-only	No	<ol style="list-style-type: none"> 1. Enter # 2. Enter six-digit credential PIN
Px	PIN-only	Yes	<ol style="list-style-type: none"> 1. Enter # 2. Enter six-digit credential PIN 3. Enter four-digit person PIN

Px	Magnetic stripe card	Yes	<ol style="list-style-type: none"> 1. Present card 2. Enter four-digit person PIN
----	----------------------	-----	---

NOTE: To require the entry of a person PIN at a lockset, a keypad must be configured for the lockset on the Portals page (*Configuration : Access Control : Portals*).

See also: [Overview: Integrating Remote Locksets](#)

[Configuring Remote Lockset Advanced Options](#)

[About the Remote Lockset Advanced Options](#)

[Creating Remote Lockset Profiles](#)

[Viewing Remote Lockset Status](#)

[Viewing Cached Information for a Remote Lockset](#)

[Monitoring Remote Locksets](#)

[About Remote Lockset User Types](#)

[Remote Locksets Report](#)

[Integrating ASSA ABLOY Remote Locksets \(PDF\)](#)

Reports

Creating Report Groups

Select **Configuration : Site Settings : Report Groups**.

With this page you can create, edit, and delete report groups containing one or more predefined and custom reports. When such a report group is assigned to a user role, users holding that role will be able to run, and possibly edit, the reports in the group.

To create a report group:

1. Click the **add** link under the **Name** drop-down list.
2. Enter a **Name** for the new report group and, optionally, a **Description** that explains its use.
3. In the **Reports Available** list, select each report you want to add to the group, then click the right-arrow button to move it to the **Selected** list.
4. Click **Save**.

To delete a report group:

1. Select the report group from the **Name** drop-down list.
2. Click **Delete**.

See also: [Administration : Reports Menu](#)

[How Groups are Used in the System](#)

Configuring Custom Report Settings

Select **Configuration : Site Settings : Report Groups**.

On this page you can configure system-wide default settings for Custom History and Custom People reports.

To configure default report settings:

1. For **Storage Budget**, enter the default storage space to be reserved for custom reports, in days.
2. For **Minimum Space for New Report**, enter the minimum available space, in megabytes, that must be available for a report to run.
3. For **Retention Time**, enter the number of days the system will retain a report.
4. For **Schedule Start Time**, enter the time (in the format HH:MM) scheduled reports will be run.
5. Click **Save**.

See also: [Creating Custom History Reports](#)

[Creating Custom People Reports](#)

Activating a Software License File

Select **Configuration : Site Settings : Software License**.

With this page you can activate the system licensing.

New Systems

If this is a new system the fields will be pre-filled with the appropriate keys.

Upgrades and Renewals

If this is an license upgrade or license renewal, you must obtain an **Activation Key**, and a **Product Key** specific to your system's license identifier. Contact your system installer. They will need the license identifier for your system, which can be found on the **About** page.

- The **License Identifier** comes from your system hardware.
- The **Product Key** contains the licensed system features and limits. To upgrade your system license to enable additional cameras or doors, you will need a new Product Key.
- The **Activation Key** contains the warranty expiration date.
The keys are locked to the license identifier and will only be valid for one system.

To activate the software license:

1. Ensure that the **License Identifier** is entered in the license text box.
2. Enter the **Activation Key** and the **Product Key** into the appropriate text boxes if needed.
3. Click the link to **View End User License Agreement** and select the check box to indicate acceptance of the license agreement.
4. Click **Apply**.

See also: [The About Dialog Box](#)

[Managing System Health](#)

Creating Rules to Change System Behavior

Select **Configuration : Site Settings : System Rules**.

With this page you can create or delete a First-in Unlock system rule. This rule is used to modify the automatic locking and unlocking behavior of a [portal group](#) that has an [unlock time spec](#). A system can have up to 64 system rules at one time.

Example

The main entrance to a facility should be unlocked between 9 a.m. and 5 p.m., as long as the receptionist is on duty. The receptionist normally arrives at around 8:30 a.m. and unlocks the main entrance temporarily to gain access to the facility.

- Place the "main entrance" portal into a portal group and assign it an unlock time spec of 9:00 a.m. to 5:00 p.m.
- Create an access level called "Receptionist In" and another called "Receptionist Out." Assign the reader for the "main entrance" portal to each of these access levels.
- Create a First-in Unlock rule that requires a valid read of the "Receptionist In" access level before the portal group will unlock according to its unlock time spec. The rule should also specify that the portal group will re-lock when the system sees a read of the "Receptionist Out" access level. Set a daily reset time of 8 a.m. for the rule.
- Assign the "Receptionist In" and "Receptionist Out" access levels to the receptionist.
- Issue an access card to the receptionist if he or she does not already have one.
- The main entrance will unlock each day only if the system sees a valid card read with the access level "Receptionist In" before or after 9 a.m.

NOTE: The portals in a group to which a First-in Unlock rule is assigned will unlock only when the rule is satisfied **and** the portal group's unlock time spec is valid.

- The main entrance will re-lock at 5 p.m. (when the portal group's unlock time spec becomes invalid) **or** when the system has seen a card read with the access level "Receptionist Out."

To create a First-in Unlock rule:

1. Click the **add** link under the **Name** drop-down list.
2. Enter a **Name** for the First-in Unlock rule, such as "weekday unlock rule."
3. Select an **unlock access level** for the rule.

4. Select a **relock access level** for the rule.
5. Select a daily reset time for the rule.
Unless the system sees a valid read of the rule's **relock access level** beforehand, the First-in Unlock rule will reset at the time you specify and its **unlock access level** will become invalid.
6. Click **Save**.
7. Assign the rule to a [portal group](#) that has an [unlock time spec](#).

NOTE: Although you can save a First-in Unlock rule without completing step 5, you should specify a daily reset time to ensure that someone is present when the portals unlock each day. The reset time should be before the start time of the portal group's unlock time spec, and close to the time a person with the unlock access level will normally want to gain access.

In the example above, suppose that no reset time is specified and the receptionist needs to enter the facility after normal business hours to retrieve something. The following day, the main entrance will automatically unlock at 9 a.m., even if the receptionist is not there. This is because the system saw a valid read of the unlock access level the previous evening, and because that access level was still valid at 9 a.m., all of the rule's conditions were satisfied.

To delete a system rule:

1. Select the rule you want to delete from the **Name** drop-down list.
2. Click **Delete**.

See also: [Using the First-in Unlock System Rule \(PDF\)](#)

[Setting Up Portal Groups](#)

[Creating Time Specs](#)

[Creating Custom User Roles](#)

Creating User Roles

Select **Configuration : Site Settings : User Roles**.

With this page you can create user roles. Users to whom the role is assigned (via the Login tab of their [person records](#)) will be able to log into the partition where the role was created and will have the specific set of permissions defined for the role.

NOTE: For descriptions of the default user roles, see [Editing Person Records](#).

To create a user role:

1. Enter a **Name** for the new user role and, optionally, a **Description** that explains its use.
2. To assign a threat level group, select it from the **Threat Level Group** drop-down list. This user role will function only if the threat level of the default location in the active partition is a member of the assigned threat level group.
Select <not applicable> if the threat level should *not* affect the behavior of this user role.
4. To give users with this role abilities for viewing and working with resources such as cameras or readers, select resource groups from the Available lists and click the right-arrow buttons to

move them to the Selected lists. Select one or more of the check boxes next to a Selected list to set specific permissions for resources in the selected groups. For more information, see [Permissions You Can Set for User Roles](#).

CAUTION: Floorplan permissions are a special case. Allowing a user access to a floorplan gives that user access to all resources placed on the floorplan, regardless of the permissions otherwise granted by the user role. Before assigning a user a role that grants access to floorplans, be sure that none of those floorplans include resources to which the person should not have access.

5. To give users with this role permissions for viewing and working with the information in person records, select any of the available entries under **Personal Information** and click the right-arrow button to move them to the Selected list.
6. To assign a [custom menu](#) to users with this role, select it from the **Custom Menu** drop-down list. The list shows all available custom menus in the active partition.

This setting takes precedence over the Custom Menu setting on the [Admin tab](#) of the Network Controller page. It will be the custom menu for all users with this role who do not have individually assigned custom menus (via the [Login tab](#) of their person records).

If you also select the **Restrict to Custom Menu** check box, this custom menu will be the only menu available to users with this role. Icons for the Monitor, Administration, and Setup menus will not be displayed in the [page bar](#) when these users are logged in.

7. Click **Save**.

See also: [Permissions You Can Set for User Roles](#)

[Using Threat Levels to Change System Behavior](#)

[Creating Camera Groups](#)

[Creating Elevator Groups](#)

[Creating Floorplan Groups](#)

[Grouping Widget Desktop Layouts](#)

[Editing Person Records](#)

[Setting Up Portal Groups](#)

[Creating Event Groups](#)

[Creating Report Groups](#)

[Setting Up Reader Groups](#)

[Setting Up Access Levels](#)

Permissions You Can Set for User Roles

When creating a [user role](#), you can set specific permissions for viewing and working with:

- Members of [resource groups](#), such as the cameras in selected camera groups.

- [Access levels](#).
- [Data Operations features](#).
- [Personal information](#), such as credentials, access levels, and other types of information in person records.

Resource Group, Access Level, and Data Operations Permissions

The table below describes permissions you can set for viewing and working with members of selected resource groups, access levels, custom menus, and Data Operations features.

Resource Group or Feature	Available Permissions
Access levels	Assign: Ability to assign the selected access levels to person records
Camera groups	<p>View: Ability to view camera images for the cameras in selected groups (non-NetVR cameras and NetVR cameras)</p> <p>Go to presets: Ability to select available presets, for PTZ cameras that support presets</p> <p>PTZ: Ability to display PTZ controls and use them to pan, tilt, and zoom the camera views</p> <p>Edit presets: Ability to add, remove, and edit camera presets</p> <p>Forensic Desktop: For sites with NetVR integrations, the ability to open and use the Forensic Desktop.</p>
Custom Menus	<p>Custom Menu List: Select a custom menu to assign it to all users with this role.</p> <p>Restrict to Custom Menu: Select to restrict users with this role to pages that can be accessed via controls in the selected custom menu.</p>
Data Operations	<p>View: Ability to view the results of data operations on the Data Operations page.</p> <p>Delete: Ability to delete existing person records.</p> <p>Upload: Ability to upload import files (tab-separated or comma-separated (CSV) text files) to your security management system.</p> <p>Export: Ability to create export files containing all person record data and download the files from the security management system.</p> <p>Configure NAS: Ability to configure a NAS storage location for scheduled import operations.</p> <p>Schedule: Ability to schedule automatic data operations.</p>
Elevator groups	<p>View: Ability to monitor the elevators in selected groups</p> <p>Free Access: Ability to manually override controlled access to the elevators by enabling free access for their floor-select buttons</p>
Event groups	<p>View: Ability to view the events in selected groups</p> <p>Acknowledge: Ability to acknowledge the events' alarms</p> <p>Clear actions: Ability to clear actions for the events' alarms</p>

Floorplan groups **View:** Ability to [monitor the floorplans](#) in selected groups

Portal groups **View:** Ability to [monitor the portals](#) in selected groups
Momentary unlock: Ability to momentarily unlock the portals
Extended unlock: Ability to schedule extended portal unlocks
Extended lock: Ability to schedule extended portal locks
UI lock/unlock: Ability to switch the portals to a [persistent locked or unlocked state](#)
Disable: Ability to disable the portals, temporarily removing them from the system's control.

Reader groups **View photo IDs:** Ability to view a recent history of cardholders who have presented their credentials at the readers in the selected groups, using the [Photo ID History widget](#)

Report groups **Run:** Ability to [run the reports](#) in selected groups
Edit: Ability to edit the reports

Widget Desktop groups **Run:** Ability to view the layouts in selected groups on the [Widget Desktop](#) and select them on the person record Login tab as the [default Widget Desktop layout](#).

Personal Information Permissions

The table below describes permissions you can set for viewing and working with selected types of information in person records, such as peoples' credentials, access levels, and ability to change the system threat level.

Personal Information	Available Permissions
Person	<p>Add: Ability to add a person to the system by creating a person record</p> <p>Edit/Delete: Ability to edit and delete a person record, respectively</p> <p>Personal Info. View: Ability to view a person's name, activation/expiration dates and times, notes, and ID# in fields at the top of a person record</p> <p>Personal Info. Assign: Ability to enter information into the fields at the top of a person record</p> <p>Login Assign: Ability to assign a user name and password on the Login tab of a person record</p> <p>Login View: Ability to view information on the Login tab of a person record</p> <p>View: Ability to see a person record—for example in person search results</p>
Card	<p>Assign: Ability to issue a credential in a person record</p> <p>Lookup: Ability to scan a credential to find person records with matching hot stamp numbers</p> <p>Temp: Ability to set expiration dates for credentials</p>

	View: Ability to view a person's credentials
Access Levels	<p>Assign: Ability to assign, edit, and remove access levels on the Access Levels tab of a person record</p> <p>View: Ability to view a person's assigned access levels</p>
Photo	Assign: Ability to upload, save, and delete photo ID images on the Photo ID tab of a person record
Photo ID	<p>Assign: Ability to capture and save ID Photos, if the system is licensed for photo ID badging</p> <p>Print: Ability to print ID photos, if the system is licensed for photo ID badging</p>
PIN	<p>Assign: Ability to assign a PIN in a person record</p> <p>View: Ability to view a PIN in a person record</p>
Extended Unlock	Assign: Ability to assign an extended unlock period in a person record
Company ID	<p>Assign: Ability to add a person ID number to a person record</p> <p>View: Ability to view a person ID number in a person record</p>
User-defined Fields 1-20	<p>Assign: Ability to add a UDF to the User-defined field tab of a person record</p> <p>View: Ability to view the User-defined Fields tab of a person record</p>
Other Contact	<p>Assign: Ability to add information to the Other Contact tab of a person record</p> <p>View: Ability to view the Other Contact tab of a person record</p>
Contact	<p>Assign: Ability to add information to the Contact tab of a person record</p> <p>View: Ability to view the Contact tab of a person record</p>
Vehicle	<p>Assign: Ability to add information to the Vehicles tab of a person record</p> <p>View: Ability to view the Vehicles tab of a person record</p>
Recent Activity	View: Ability to view the Recent Activity tab of a person record
Threat Level	Set: Ability to change the threat level for all locations or for selected locations in the active partition

See also: [Creating User Roles](#)

[Editing Person Records](#)

NetVR Appliances

Configuring a NetVR Appliance

Select **Configuration : Video : NetVR Appliances**.

For a more complete treatment of this topic, see the [NetVR Setup and Configuration Guide \(PDF\)](#).

On this page you can add a NetVR appliance to the system.

NOTE: Click the **Install NetVR Setup Tool** link on this page to download, install, and open the NetVR setup and configuration application.

To set up a NetVR embedded appliance:

1. The **NetVR IP Address** for the appliance is displayed as an internal connection between the controller and the embedded NetVR appliance.
2. Use your custom login or the default entries in the **NetVR Username** and **NetVR Password** fields with the secure login name and password you entered when configuring the appliance.

NOTE: The username and password you enter here must exactly match the username and password you entered when you configured the NetVR appliance through the NetVR Setup Tool. The name and password are case sensitive.

3. Click **Check connection**.
In the **Discovered Information** section that appears, the serial number, vendor, model, and camera count are filled in automatically.
4. Click **Save**.
5. In the **Discovered Information** section, click the **List VMS Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NetVR appliance through its own web interface.
6. To rename the NetVR appliance, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

To set up the NetVR freestanding appliance:

NOTE 1: Before configuring the NetVR appliance on the network controller, ensure that the appliance and cameras have been set up and verified through the NetVR Client, installed by using the **NetVR Setup Tool**.

NOTE 2: We recommend the use of a static IP address for a NetVR appliance. If the IP address of the appliance changes, the connection between it and the network controller will be lost. The static IP address must be set using the NetVR Client / System Setup / Network Tab.

NOTE 3: Using live streaming video consumes considerable network bandwidth.

1. Enter the **NetVR IP Address** for the appliance.
2. Replace the default entries in the **NetVR Username** and **NetVR Password** fields with the secure login name and password you entered when configuring the appliance.

NOTE: The username and password you enter here must exactly match the username and password you entered when you configured the NetVR appliance through its own web interface. The name and password are case sensitive.

3. Click **Check connection**.

In the **Discovered Information** section that appears, the serial number, vendor, model, and camera count are filled in automatically.

4. Click **Save**.
5. In the **Discovered Information** section, click the **List VMS Cameras** link and verify that the list of cameras is correct and complete. These cameras were set up during the configuration of the NetVR appliance through its own web interface.
6. To rename the NetVR appliance, click the **rename** link below the **Name** field, enter a new name, and then click **Save**.

To configure public settings:

1. **NetVR Public IP Address:** This IP address fills in automatically when you save a new NetVR appliance configuration.

NOTE: If this address is on another subnet or behind a firewall, you may have to change this to the external public address of the router or firewall. The network administrator will have to set up the port translation for communications and video to and from this address.

2. **NetVR Public Service Port:** This port number defaults to 80.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

Example: If you set this field to 60 seconds, additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. Click **Save**.

See also: [Setting Up Virtual Inputs for VMS Cameras](#)

[Updating an NVR Integration](#)

[Changing the Default IP Address for a NetVR System \(PDF\)](#)

[Moving Video Management Systems Between Partitions](#)

[Setting Up Camera Types](#)

[Creating Camera Definitions](#)

[Setting Up Multi-Camera Views](#)

[Setting Up Camera Tours](#)

[Configuring the NetVR Web Service \(PDF\)](#)

Setting the Network Connection for a NetVR Appliance

Following the NetVR hardware setup, while the NetVR appliance it is still connected directly to a local PC or laptop (not on the corporate network), you can set the network connection.

To set the network connection for a NetVR appliance:

1. Set the local PC or laptop to a static IP address of 192.168.0.X (where X is a number other than 251, 250, and 249).
2. Set the Subnet Mask to **255.255.255.0**.
3. Set the Gateway to **192.168.0.1**.
4. Browse to the NetVR at 192.168.0.249.
The Software License page opens.
5. Accept the terms and click **Apply**.
6. Log in:
 - Enter the username: **admin**.
 - Enter and confirm the password: **admin**.
7. On the S2 NetVR Downloads page, download, install, and open the S2 NetVR Setup Tool.
8. Select **Add System** in the menu and do the following:
 - Click **New**.
 - Enter the default NetVR IP address: **192.168.0.249**.
 - Enter the username: **admin**.
 - Enter and confirm the password: **admin**.
 - Click **Apply**.

The screen indicates "Connected" when the NetVR server has been added.

9. Select **System Setup** and click the **Network** tab.
 - Enter your preferred **IP address** and **Netmask** for the NetVR server.
 - Enter the **Gateway** and, optionally, the **Primary DNS**.
 - Click **Apply**.
10. Set the PC or laptop back to an IP address on your network.
11. Browse to NetVR at the new NetVR server IP address.
12. Return to the NetVR Setup Tool's Add System page to register the new IP address.
13. On the **Users** menu, create a new Admin password (recommended) to use for logging in to NetVR.
14. Use the NetVR Setup Tool to configure cameras and the NetVR appliance.

See [Configuring a NetVR Appliance](#) and the [NetVR Setup and Configuration Guide \(PDF\)](#) for detailed camera setup and configuration instructions.

See also: [Beginning a Forensic Search](#)

[Using the Forensic Desktop Activity Log](#)

[Using the Forensic Desktop Video Player](#)

[Creating and Saving Clips](#)

[Using the Forensic Desktop Timeline](#)

[Composing Forensic Cases](#)

[Printing and Exporting Forensic Cases](#)

[Accessing Recorded Video from a Person Record](#)

[Monitoring the Activity Log](#)

[Monitoring NetVR Cameras](#)

[Monitoring NetVR Multi-Camera Views](#)

System Maintenance

Select **Configuration : System Maintenance** to display the following options.

Choose this	To see information on
Backup System	Performing an immediate security database backup to the network controller or downloading an existing backup to off-controller storage.
Restore System	Performing an immediate restore of the on-controller security database backup or uploading an existing backup from a network storage location.
System Health and Maintenance	Viewing the status of the system's Software Upgrade and Support (SUSP) license, acknowledging a license expiration to disable the blinking icon in the page bar, and exporting system information to obtain a new license.
Storage	Monitoring disk usage, configuring disk usage thresholds and specifying events to be activated when they are reached, and enabling automatic remediation.
Update Software	Updating the security management system to the latest revision.
Utility	Refreshing security database and system configuration data to nodes, cleaning up images and backups, shutting down and rebooting the system, and disabling node communication.

See also: [Setting Up the Network Storage Location](#)

[FTP Backup Settings](#)

[Activating a Software License File](#)

[About Archive Files](#)

Backing Up the System Data

Select **Configuration : System Maintenance : Backup System**.

- or -

Select **Administration : Utility : Backup System**.

With this page you can:

- Back up the security database to the network controller.
- Back up the security database to a network attached storage (NAS) if one is configured using [Setting Up the Network Storage Location](#) or [FTP Backup Settings](#).
- Download a backup of the security database to off-controller storage.

The system data is regularly backed up to the network controller each night at 00:15 hours. The Sunday backup is a full backup. The Monday through Saturday backups 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 off-controller system backups. Backups delivered to a configured FTP server or NAS drive will not be overwritten.

You can perform additional backups whenever you want.

NOTE: The system will also automatically create [archive files](#) of all data required for [General Event History reports](#), [Custom History reports](#), [Custom People reports](#) and [Audit Trail Reports](#). Each Sunday, after the full backup at 00:15 hours, the system checks the number of Activity Log records. If this number exceeds 150,000 then all records in excess of 100,000 are zipped into an archive file. This file is stored on the controller and on any configured NAS or FTP servers.

NOTE

To back up system data:

1. Enter a **Comment** to explain the purpose of this backup.
2. Click **Full Backup**.
3. Once 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.

To download a backup to off-controller storage:

1. In the **Existing Backups** table, click **get** for the backup you wish to save to off-controller storage.
2. In the **File Download** dialog, click **Save**.
3. In the **Save As** dialog, browse to the location where you wish to save this backup.
4. Click **Save**.

See also: [Restoring the System Data](#)

[Setting Up the Network Storage Location](#)

[FTP Backup Settings](#)

[About Archive Files](#)

[Setting Up the Network Controller](#)

[System Maintenance Utilities](#)

About Archive Files

The system automatically creates archive files of all data required for [General Event History Reports](#), [Custom History Reports](#), and [Custom People Reports](#).

Each Sunday, after the full backup at 00:15 hours, the system checks the number of Activity Log records. If this number exceeds 150,000 then all records in excess of 100,000 are zipped into an archive file. Only full days of data are included.

This file is stored on the controller and on any configured NAS or FTP servers.

The archive files are named:

arch_YYYYMMDD_YYYYMMDD.zip

where the first date is the oldest day of records, and the second date is the most recent day of records contained within the archive.

If the inclusive dates of your custom reports are weeks or months in the past, it is likely that some of the relevant data is in archive files. The report will still run correctly. The appropriate data will be retrieved from the archive files. This will take a few moments.

See also: [Backing Up the System Data](#)

Restoring the System Data

Select **Configuration : System Maintenance : Restore System**.

You can use this page to restore the security database from online backups located on the controller or offline backups located on an FTP server or NAS drive.

NOTE: The system data is backed up daily at 00:15 hours. The Sunday backup is a full backup. The Monday through Saturday backups 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 board.

To restore the security database from backup:

1. Select **Configuration : System Maintenance : Restore System**.

In the list of backups, the Status column indicates whether a backup is online or offline.

3. Select the button in the **Restore?** column for the backup you want to restore. The system will be completely restored to its condition as of the date and time of the backup you selected. If the backup is offline, the system will retrieve it and then perform the restore.

If you select a **Differential** backup, the system will automatically restore the full backup and then the differential backup.

- Click **Restore Now** and click **OK** to confirm.
The selected backup security database is restored.

See also: [Setting Up the Network Storage Location](#)

[Backing Up the System Data](#)

[FTP Backup Settings](#)

[About Archive Files](#)

[System Maintenance Utilities](#)


Managing System Health


Select **Configuration : System Maintenance : System Health and Maintenance**.

Maintaining an active Software Upgrade and Support (SUSP) license ensures that you will be able to upgrade to newer software versions and that S2 diagnostic support will be available should issues arise. To assist you, the system monitors the status of your SUSP license and alerts you (via Activity Log messages and icons in the page bar) 60 days prior and then 30 days prior to the license expiration date, and again if your license expires.

You can use the System Health and Maintenance page to check the expiration date and current status of your SUSP license at any time. If the license status is Active but the expiration date is fewer than 90 days away, you can avoid receiving alerts by obtaining a new license as soon as possible.

If you receive an alert indicating that your license is about to expire, or that it has already expired, you should obtain a new license immediately. If you have setup privileges, you can acknowledge the alert to disable the blinking icon in the page bar:

 Warning icon indicating your license is about to expire

 Error icon indicating the license has expired

To acknowledge an alert:

- Click the warning or error icon in the page bar to open the System Health page, or navigate to the page using the navigation palette.
- (optional) If the license has already expired, specify when you want to be reminded (in 30, 60, or 90 days).
- Click **Acknowledge**.

In the page bar, the warning or error icon stops blinking.

To obtain a new license:

- Click **Export System Information**.
Information about your system is exported to a CSV file.
- Share the CSV file with your integrator to obtain a quote and complete the purchase.
- When you receive a new license, follow the instructions in [Activating a Software License File](#).

If there is a warning or error icon in the page bar, it is removed once the new license is activated.

See also: [The Page Bar](#)

[The Navigation Palette](#)

Managing Storage

Select **Configuration : System Maintenance : Storage**.

The Storage page provides options for monitoring and managing disk usage:

- [Configuring disk usage thresholds](#): Configure Caution and Warning disk usage thresholds.
- [Configuring disk usage events](#): Configure events that will be activated when specific disk usage thresholds are met or exceeded.
- [Configuring disk usage remediation](#): Configure manual and automatic remediation by the security management system.
- [Viewing disk usage status](#): View disk usage status information.

See also: [Monitoring the Activity Log](#)

[Setting Up Events](#)

[System Maintenance Utilities](#)

[Using the Monitoring Desktop](#)

Configuring Disk Usage Thresholds

Select **Configuration : System Maintenance : Storage**.

Over time, as a result of normal security operations, video capture and retrieval, downloads of new software versions, backup and restore operations, expansion of the S2 database, and so on, you will accumulate files on your system and use up disk space.

The system will automatically initiate remediation procedures when the Warning thresholds have been reached and delete unnecessary files if you have enabled automatic remediation. (See [Configuring Disk Usage Remediation](#) for details).

Even when remediation is enabled, at some point, as disk usage reaches capacity, you may have to take action to remove files. (See [System Maintenance Utilities](#) for information on managing files).

Use the System Storage Monitor to define Caution and Warning thresholds that generate alerts to indicate that disk space usage has reached critical levels. When a threshold is reached, the system generates an Activity Log message and, if configured, activates an optional user-defined event for the Caution High Limit or Warning High Limit threshold. Events for the Caution Low Limit and Warning Low Limit thresholds are not supported. (See [Configuring Disk Usage Events](#) for details.)

The Activity Log messages appear in the Activity Log and on the Monitoring Desktop.

You can set the following disk usage thresholds:

- **Caution High Limit:** the point at which the system state changes from Normal (**green**) to Caution (**yellow**) as disk usage increases. (range: 50% to 95% disk capacity utilized; the default is 70%)
- **Caution Low Limit:** the point at which the system state changes from Caution (**yellow**) back to Normal (**green**) as disk usage decreases (range: 40% to 95% disk capacity utilized; the default is 65%)
- **Warning High Limit:** the point at which the system state changes from Caution (**yellow**) to Warning (**red**) as disk usage increases (range: 50% to 95% disk capacity utilized: the default is 95%)
- **Warning Low Limit:** the point at which the system state changes from Warning (**red**) back to Caution (**yellow**) as disk usage decreases (range: 40% to 95% disk capacity utilized; the default is 90%)

Use the four thresholds as a barometer of the health of disk space usage. You can modify them or leave the Caution or Warning thresholds at the default values.

Examples

For example, suppose you set the disk space usage thresholds to values shown in the sample table below and select the System Storage Monitor check box. When *increasing* disk usage *meets or exceeds* the Caution High Limit or Warning High Limit configured threshold, the appropriate Activity Log message is generated. However, when increasing disk usage meets or exceeds the Caution Low Limit or Warning Low Limit threshold, no Activity Log message is generated. Only when disk usage *falls below* a Low Limit threshold is an Activity Log message generated to inform the user that system disk usage has returned to a less critical state.

Threshold Type	Threshold % (User-Defined)	Activity Log Message When Threshold is Exceeded
Caution Low Limit	70	No message generated for increasing disk usage
Caution High Limit	75	System Health: Total Disk Usage exceeded caution monitor level
Warning Low Limit	85	No message generated for increasing disk usage
Warning High Limit	90	System Health: Total Disk Usage exceeded warning monitor level

When the disk usage threat *recedes* and disk usage percentages fall below the Warning Low Limit and Caution Low Limit thresholds, the appropriate Activity Log messages are generated (as shown in the table below). The Warning High Limit and Caution High Limit thresholds when reached during *decreasing* disk usage do not generate an Activity Log message.

Threshold Type	Threshold % Actually Reached	Activity Log Message When Usage Recedes Below Threshold
Warning High Limit	90	No message generated for decreasing

disk usage		
Warning Low Limit	84	System Health: Total Disk Usage returned to caution monitor level
Caution High Limit	75	No message generated for decreasing disk usage
Below Caution Low Limit (Acceptable Operating Range)	69	System Health: Total Disk Usage acceptable operating level

To set the Caution and Warning disk usage thresholds:

1. **Select Configuration : System Maintenance : Storage.**
2. In the Configuration section, select the **Caution High Limit** from the drop-down list to set the high threshold for Caution state disk usage.
3. In the Configuration section, select the **Caution Low Limit** from the drop-down list to set the low threshold for Caution state disk usage.
4. In the Configuration section, select the **Warning High Limit** from the drop-down list to set the high threshold for Caution state disk usage.
5. In the Configuration section, select the **Warning Low Limit** from the drop-down list to set the low threshold for Caution state disk usage.
6. Select the **Enable System Storage Monitor** check box to turn on the System Storage Monitor feature and to start logging caution and warning messages.
7. Select the **Enable Remediation** check box to engage disk usage remediation (See [Configuring Disk Usage Remediation](#)).
8. Click **Save**.

The system responds with the message: The System Storage settings have been saved.

See also: [configuring disk usage events](#)

[Configuring Disk Usage Remediation](#)

[Viewing Disk Usage Status](#)

[system maintenance utilities](#)

Configuring Disk Usage Events

Select **Configuration : System Maintenance : Storage**.

You can configure the System Storage Monitor to activate an event when increasing disk usage meets or exceeds the Caution High Limit or Warning High Limit threshold. You must [set up a new event](#) if the event you want to activate is not currently configured.

Once an alarm becomes active for a disk usage event, it will remain active until it is acknowledged (if acknowledgement is required according to the event definition) and the system changes to a more critical or less critical state.

To configure events to be activated when disk usage thresholds are reached:

1. Select **Configuration : System Maintenance : Storage**.
2. In the Configuration section, select an event from the **Caution High Limit : Event** drop-down list.
3. In the Configuration section, select an event from the **Warning High Limit : Event** drop-down list.
4. Select the **Enable System Storage Monitor** check box to turn on the System Storage Monitor feature and start logging caution and warning messages.
5. Select the **Enable Remediation** check box to engage disk usage remediation (See [Configuring Disk Usage Remediation](#) for details).
6. Click **Save**.

The system responds with the message: The System Storage settings have been saved.

NOTE: If the event you want activated is not available in the drop-down list, you must go to the [Events](#) page to set up a new event.

Example

If you want a specific email message to be sent to the Administrator email account when a Caution or Warning disk usage threshold is met or exceeded, select an event for the threshold that has the **Send Email** action defined. (See [Defining Event Actions](#) for details on how to define an action for an event.)

The following table provides a sample configuration setup for events that generate emails when High Limit disk usage thresholds are reached.

NOTE: The Caution High Limit and the Warning High Limit thresholds are used by the S2 system as barometers of increasing disk usage.

Threshold Type	Threshold % (User-Defined)	Current State of Disk Usage	Event Name (User-Defined)	Message Sent to Admin Email Account (User-Defined)
Caution High Limit	75	Increasing	Increasing disk usage has met or exceeded Caution High Limit	CAUTION HIGH LIMIT disk usage level reached: remove unnecessary files to free up disk space !!!!
Warning High Limit	90	Increasing	Increasing disk usage has met or exceeded Warning High Limit	WARNING HIGH LIMIT disk usage level has reached critical level: remove unnecessary files to free up disk space immediately !!!!

See also: [Configuring Disk Usage Thresholds](#)

[Configuring Disk Usage Remediation](#)

[System Maintenance Utilities](#)

[Viewing Disk Usage Status](#)

Configuring Disk Usage Remediation

Select **Configuration : System Maintenance : Storage**.

When the Warning threshold is reached and the **Enable Remediation** check box is selected, the System Storage Monitor automatically deletes the following files to make disk space available:

- **Upgrade/installation artifacts** – software installation files that were unpacked from an upgrade and left on a system. There is no need to keep these files on your system.
- **System log files** – compressed system log files (files with the .gz extension).

To configure disk usage remediation:

1. Select **Configuration : System Maintenance : Storage**.
2. Click the **Enable Remediation** check box to engage disk usage remediation.
3. Click **Save**.

The system responds with the message: The System Storage settings have been saved.

Performing Manual Remediation of Disk Usage

If, after automatic system remediation occurs, disk usage remains above Caution or Warning thresholds, you need to take action by manually deleting files to clear storage on your disk. Use the [System Maintenance : Utility](#) page to review and delete system backups, Photo ID layouts and Photo IDs, floorplan images, sound files, and system updates.

To delete system backups:

1. Select **Configuration : System Maintenance : Utility**.
2. Select the **Delete?** check box for each backup you want to delete.
3. Click **Delete File(s)**.

To delete floorplan images, Photo IDs, sound files, and system updates:

1. Click the appropriate link for the type of file you want to delete.
2. Select the **Delete?** check box for each item you want to delete.
3. Click **Delete File(s)**.

If deleting unwanted and unnecessary files from your S2 system does not reduce disk usage to acceptable levels, call S2 Support.

See also: [Configuring Disk Usage Events](#)

[Configuring Disk Usage Thresholds](#)

[System Maintenance Utilities](#)

[Viewing Disk Usage Status](#)

Viewing Disk Usage Status

Select **Configuration : System Maintenance : Storage**.

Storage Status

The Storage Status section of the Storage page displays general disk usage information:

- **Filesystem:** The filesystem the Storage Monitor will monitor. If the system has the /var filesystem mounted on its own disk partition or device, /var will be monitored. Otherwise, the root filesystem ("/"), which includes /var, will be monitored.
- **State:** The overall disk usage state (normal, caution, or warning)
- **Total Space:** the total disk space (not including video stores) available
- **Used:** The percent of disk space used

Storage Details

The Storage Details section of the Storage page displays detailed disk usage information for the system drives and video storage:

- **Name:** The name of the system drive or video storage device
- **Resource:** The location
- **Capacity:** The total capacity of the storage resource
- **Used:** The storage space used
- **Available:** The storage space available (free)
- **Use%:** The percentage of total storage space used

See also: [Configuring Disk Usage Events](#)

[Configuring Disk Usage Remediation](#)

[Configuring Disk Usage Thresholds](#)

Updating the System Software

Select **Configuration : System Maintenance : Update Software**.

Updating the security management system software is a three-step process.

1. Click the **Backup System** link and [back up the security database](#).
2. To return to the Software Update page select **Configuration : System Maintenance : Update Software**.
3. Click the **Upload System Update (*.upg)** link, and from the Upload page browse to the appropriate file and click **Save**. This copies the update file to the Network Controller.
4. Click the **Apply System Update** link to display all available software update files on the controller.

5. Select the software update you want to apply by clicking the appropriate button in the **Apply?** column.
6. Click **Apply Update Now**. This may take several minutes to apply, and then you will hear a double-beep. It will then take several more minutes to reboot and reload services and you will then hear a single beep.
7. Log back in to the security management system.

See also: [Backing Up the System Data](#)

System Maintenance Utilities

Select **Configuration : System Maintenance : Utility**.

Performing File Management

You can review and delete system backups, Photo ID layouts and Photo IDs, floorplan images, sound files, and system updates. You can also upload sound files and update the disk usage statistics displayed on the About page.

Deleting Unneeded Files

To delete system backups:

1. Click the **System backups** link.
2. Select the **Delete?** check box for each backup you want to delete.
Note that all database backup file names contain date and time stamps.

File name	Date & Time	Comment	Delete?
diff_20100512_001503.1.dar	2010-05-12 00:15:03	nightly	<input type="checkbox"/>
full_20100511_001504.1.dar	2010-05-11 00:15:04	nightly	<input type="checkbox"/>

3. Click the **Delete File(s)** button.

To delete floorplan images, photo IDs, photo ID layouts, sound files, and system updates:

1. Click the appropriate link for the type of file you want to delete.
2. Select the **Delete?** checkbox for each item you want to delete.
3. Click the **Delete File(s)** button.

See also: [Updating the Security Management System Software](#)

[Backing Up the System Data](#)

[About Archive Files](#)

[Uploading Floorplan Background Images](#)

Uploading Sound Files

You can upload sound files to use in announcing alarms. To set up the use of a sound file to announce an event, use [Setup : Alarms : Events](#).

NOTE: You can upload a sound file (.wav) that is up to 100K in size, and you can store up to 256 sound files on the controller.

To upload a sound file:

1. Click the **Upload Sound file** link.
2. Click the **Browse** button to browse to the location of your .wav file.
3. Click **Save**. The selected file is saved to the controller.

Updating Disk Usage

Clicking the **Update Disk Usage** button refreshes the ROM, RAM disk, and Flash Card usage statistics that are displayed on the [About page](#).

See also: [Backing Up the System Data](#)

[FTP Backup Settings](#)

[Setting Up the Network Storage Location](#)

[About Archive Files](#)

Downloading nnconfig

Click the [nnconfig.exe](#) link in this section to download the Network Node Configurator utility (nnconfig.exe), which you can use to point a node to the specific controller to which it should connect. For more information, see [Tech Note 4: Connecting Nodes and Controllers Across Subnets \(PDF\)](#).

Resetting the Event Tables

You can reset all events and event actions by clicking **Reset Events**. Normally this should not be necessary. If an event persistently reappears, the inputs involved should be investigated because they may have wiring problems.

Performing Diagnostics

Testing Network Connectivity

You can ping a known network IP address to check for connectivity between the controller and other network devices.

To test a network connection:

1. Click the **Test Network Connection** link. The Test Network Connection page displays.
2. Enter the **IP address or DNS name** into the text box and click **Check Connection**.
3. Within a few seconds the PING results display on the page.

Getting the Controller Messages File, Authorizations File, Last System Update Log, and System Diagnostics

These files may be requested by system support for diagnostic purposes.

Refreshing Nodes

You can refresh the security database and configuration data to all system nodes by clicking the **Refresh Now** button. Nodes will normally be refreshed automatically whenever the controller has new data. However, you may wish to force an immediate refresh of node data after changes have been made to the security database or configurations.

Displaying Portal Status

Clicking the **Portal Status Display** link displays in table form all configured nodes, portals, readers, inputs, and outputs. Slot and position number, status and/or state for each resource is shown.

This is a very useful report for diagnosing system configuration issues.

Performing System Functions

Shutting Down the System

You can stop the system by clicking the **Shutdown Now** button. Before the system shuts down it will store the current security database in ROM. The system will remain stopped until power is removed and reconnected.

This function is intended for use when physically moving the system or performing hardware service requiring the disconnection of power.

Restarting the System

You can restart the system by clicking the **Reboot** button. Before the system shuts down it will store the current security database in ROM.

Starting and Stopping Communication with Devices

Click the appropriate **Disable** toggle button to disable communication between the controller and all:

- Standard nodes
- ASSA ABLOY remote locksets
- DMP intrusion panels
- Mercury panels

Communication will remain disabled, even after a reboot, until the button (which is now labeled **Enable**) is clicked again.

This function is intended for use in some upgrade scenarios. When the upgrade is complete, communication between the controller and the devices can be re-enabled one node at a time.

See also: [Configuring Network Nodes](#)

[Integrating ASSA ABLOY Remote Locksets](#)

[Configuring DMP Intrusion Panels](#)

[Configuring Mercury Panels](#)

Enabling The S2 Video Streamer Service

To allow the system to stream video to mobile devices running S2 Mobile Security Officer, click the **Enable** toggle button to enable the Video Streamer service. It will remain enabled, even after a reboot, until the button (which is now labeled **Disable**) is clicked.

See also: [Tech Note 33: S2 Mobile Security Officer Video Streaming Modes \(PDF\)](#)

[S2 Mobile Security Officer User Guide \(PDF\)](#)

Threat Levels

Select **Configuration : Threat Levels** to display the following options.

Choose	To see information on
Definitions	Naming, setting the color code, and entering descriptions for threat levels.
Menu Order	Setting the order of threat levels in menus and lists.
Settings	Requiring passwords for changing threat levels and uploading images to use as threat level colors.
Threat Level App	Set up and enable the Threat Level App on mobile devices.
Threat Level Groups	Creating and editing threat level groups, which can be assigned to portal groups, access levels, portals, event actions, and user roles to change system behavior.

See also: [Using Threat Levels to Change System Behavior](#)

[Setting Up Portal Groups](#)

[Setting Up Portals](#)

[Access Levels](#)

[Setting Up Events](#)

[Configuration Reports](#)

[Setting Threat Levels](#)

Adding, Changing, and Deleting Threat Levels

Select **Configuration : Threat Levels : Definitions**.

On this page you can:

- Add new threat levels to the system.
- Edit and delete existing threat levels.

You can configure up to eight threat levels. By default the system contains six threat levels: Default, Low, Guarded, Elevated, High, Severe.

Levels Low through Severe are named and color-coded to follow the United States Department of Homeland Security threat level designations. These can be edited or deleted.

The threat level named "Default" cannot be edited or deleted.

To add new threat levels to the system:

1. Click the **add** link under the **Name** drop-down list.
2. Enter a name for the threat level in the **Name** text box. It is recommended that the name be descriptive of the threat, e.g. Unauthorized Entry, or Fire Alarm. (These are conditions under which you may wish to alter the system behavior.)
3. Enter a **Description** for this threat level.
4. Select from the **Color code** drop-down list the color to associate with this threat level.
5. Click **Save**.

To edit a threat level:

1. Select a threat level from the **Name** drop-down list. The remaining fields on the page fill with the settings for this threat level.
2. Edit any part of the threat level definition.
NOTE: Editing a threat level that is assigned to [threat level groups](#) will NOT cause a change in system behavior. The threat level ID is used to determine system behaviors. Changing the threat level name, description, or color will not change this ID.
3. Click **Save**.

To delete a threat level:

1. Select from the **Name** drop-down list the threat level you wish to delete.
2. If this threat level is defined as part of any threat level group then these groups will be listed next to **Part of group(s)**. You cannot delete a threat level while it is part of a threat level group.
3. Click **Delete**.

See also: [Using Threat Levels to Change System Behavior](#)

[Setting Up Threat Level Groups](#)

[Threat Level Settings](#)

[Setting the Threat Levels Menu Order](#)

[Setting Threat Levels](#)

Setting the Threat Levels Menu Order

Select **Configuration : Threat Levels : Menu Order**.

On this page you can set the order in which the threat levels appear in menus and lists.

To change the threat levels menu order:

1. Select a threat level in the list box by clicking on it. It will highlight to show that it is selected.
2. Click the **Move up** or **Move down** arrow to move the selected threat level up or down the list.
3. Click **Save**.

See also: [Using Threat Levels to Change System Behavior](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Setting Up Threat Level Groups](#)

[Threat Level Settings](#)

Threat Level Settings

Select **Configuration : Threat Levels : Settings**.

On this page you can:

- Require password entry to change the current system threat level.
- Upload an image to the network controller to use as a threat level color or icon.

To require password entry to change the system threat level:

1. Select the **Require Password** check box.
2. Click **Save**.

To upload images to use for threat level colors or icons:

1. Click the **Upload Threat Level Image** link.
2. In the **Select file** text box enter the directory and file name or click the **Browse** button and select the file.

NOTE: The image file must be less than 20KB and must be named one of the following names: green.jpg, blue.jpg, yellow.jpg, orange.jpg, red.jpg, color1.jpg, color2.jpg, color3.jpg.

3. Click **Save**.

See also: [Using Threat Levels to Change System Behavior](#)

[Setting Threat Levels](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Setting Up Threat Level Groups](#)

[The Threat Level Widget](#)

[Threat Level Reports](#)

Setting Up the Threat Level Escalator App

Select **Configuration : Threat Levels : Threat Level App**.

The Threat Level Escalator is an App that runs on any iOS enabled Apple device. Setting up the App on the device is a two-step process. First a user installs the App and registers the device with the controller. Then a system administrator configures the App for that device.

Once the setup process is complete, the user will be able to press a "panic button" in an emergency to set a specific threat level at the devices configured location. If the device is capable of placing phone calls, the App may also assist the user in placing an emergency call.

For Users: Installing the Threat Level Escalator and Registering the Device

To install the Threat Level Escalator:

1. Check for previous versions of the App on the device and remove any that you find.
2. Open the App Store on the device.
3. Search for **S2 Threat Level Escalator**.
4. Install the App from the iTunes App Store.

To create a secret PIN:

1. Start the Threat Level Escalator.
2. On the **Enter PIN** screen, enter a four-digit PIN.
3. On the **Re-Enter PIN** screen, re-enter the four-digit PIN to save it on your device.

To register the device with the controller:

1. Start the Threat Level Escalator.
2. On the **Enter PIN** screen, enter your secret PIN.
3. On the **Register Device** screen, do the following:
 - Enter the IP address of the controller.
 - Enter the user name and password that make up your login credentials on the controller.

An access request is sent to the controller and you are returned to the **Enter PIN** screen.

For Administrators: Configuring the Threat Level Escalator for a Device

Each time a user registers a device for access to the Threat Level Escalator, an access request is sent to the S2 controller and recorded in the Activity Log. The device is added to the Threat Level App page, where an administrator can configure the App for that device.

To configure the Threat Level Escalator for a device:

1. Log into the security management system and select **Configuration : Threat Levels : Threat Level App**.

2. Locate the device in the list. You can look for the user in the **Person** column or for the device in the **Device Name** column.
3. In the row for the device, do the following:
 - Select the check box in the **Registered Device** column.
 - Select the **Location** whose threat level should change when the panic button is pressed.
 - Select the **Threat Level** to which the selected location should be set when the panic button is pressed.
 - Select the **Device Enabled** check box to enable the Threat Level App on the device.
4. (optional) Enter the **Phone Number** to be called in an emergency, and select a **Phone Option**:
 - **No Phone** (the default): The App will provide no assistance with placing an emergency phone call.
 - **Auto Dial**: The App will automatically dial the emergency phone number.
 - **Manual Call**: The App will display an **Emergency Call** button. When the user presses this button, the App will dial the emergency phone number.

If you do not enter a phone number and select a phone option, the defaults shown at the top of the page will be applied to the device automatically.

NOTE: If the device does not support phone dialing or the user does not subscribe to phone service, the App will ignore the emergency-call feature.

6. Click **Save**.
7. To disable the Threat Level App on the device, clear the **Device Enabled** check box and click **Save**.

To set emergency-call defaults for registered devices:

1. To set a default emergency phone number for registered devices, enter it in the **Phone Number** text box at the top of the page.
2. To set a default phone option for registered devices, select it from the **Phone Option** drop-down list at the top of the page. The available options are described in the previous procedure.
3. Click **Save**.

These defaults will be applied to any registered device for which a specific emergency phone number and phone option have not been configured.

To test the Threat Level Escalator:

1. Start the Threat Level Escalator on a device.
2. Enter the secret PIN established for the App on the device.
3. In the security management system, make sure you are in the partition containing the device's configured location, and select **Administration : Set Threat Level**.
4. If necessary, select the device's configured location from the **Applies to location** drop-down list.
5. Click the panic button on the device.

6. If the Threat Level Escalator is working correctly, the **Threat Level** setting for the selected location will change to reflect the new threat level.
7. If a password is required to change the threat level, enter it in the **Password** box.
8. Reset the selected location's threat level to the default setting.

See also: [Using Threat Levels to Change System Behavior](#)

[Setting Up Threat Level Groups](#)

[Threat Level Settings](#)

[Setting the Threat Levels Menu Order](#)

[Setting Threat Levels](#)

Setting Up Threat Level Groups

Select **Configuration : Threat Levels : Threat Level Groups**.

You can use this page to create, edit, and delete threat level groups. Each group will include one or more of the threat levels currently defined in the system.

By including certain threat levels and excluding others, you can determine the group's effect on any portal, portal group, access level, user role, or event action to which it is applied. For more information, see [Using Threat Levels to Change System Behavior](#).

To create a threat level group:

1. Click the **add** link under the **Name** field.
2. Enter a **Name** for the new group and, optionally, a **Description** that describes its use.
3. In the **Threat Levels Available** list, select each threat level you want to include in the group and click the right-arrow button to move it to the **Selected** list.
4. Click **Save**.

To edit a threat level group:

1. Select an existing threat level group from the **Name** drop-down list.
2. Edit any part of the threat level group definition.
NOTE: Editing a threat level group that is assigned to [portal groups](#), [access levels](#), [portals](#), [user roles](#), or [event actions](#) will cause a change in system behavior.
3. Click **Save**.

To delete a threat level group:

1. Select an existing threat level group from the **Name** drop-down list.
NOTE: Deleting a threat level group that is assigned to [portal groups](#), [access levels](#), [portals](#), [user roles](#), or [event actions](#) will cause a change in system behavior.
2. Click **Delete**.

See also: [Using Threat Levels to Change System Behavior](#)

[Adding, Changing, and Deleting Threat Levels](#)

[Threat Level Settings](#)

[Threat Level Reports](#)

[Setting Threat Levels](#)

[Setting Up Portal Groups](#)

[Setting Up Access Levels](#)

[Enabling Double Card Presentation Mode for Portals](#)

[Creating Custom User Roles](#)

[Defining Event Actions](#)

[How Groups are Used in the System](#)

Using Threat Levels to Change System Behavior

To have system behavior change in response to changes in the current threat level, you can apply a threat level group to any of the following:

- [A portal group](#) to change the effect of the group's unlock time spec on each member portal based on threat level changes at the portal's location. If the portal group includes online remote locksets, threat level changes at each lockset's location can cause it to [enter and exit panic mode](#).
- [An access level](#) to change its validity at a particular reader based on threat level changes at the reader's location.
- An [event action](#) or [user role](#) to change its validity based on threat level changes at the default location in the active partition.

Example: [Effects of Applying a Threat Level Group](#)

Threat level changes can be made manually using the [Set Threat Level](#) page or the [Threat Level widget](#), or automatically using the [Set Threat Level event action](#).

You can also use portal policies to change a portal's behavior based on threat level changes. See [Setting Up Portals](#) for more information.

To make a portal group's unlock time spec invalid under certain threat levels:

1. [Create a threat level group](#) containing only the threat levels under which a portal group's unlock time spec should be considered valid.
2. On the [Portal Groups page](#), select a portal group.
3. Assign the new threat level group to the portal group and click **Save**.

When the portal group's unlock time spec is valid and its first-in unlock rule (if one is specified) is satisfied, an individual portal in the group will unlock at the start of the time spec period *only*

if its location is currently under one of the threat levels in the assigned threat level group. Note that the assigned threat level group will have no effect on any remote lockset in the portal group.

CAUTION: For any portal that is assigned to multiple portal groups, the most permissive portal group will determine when the portal unlocks and relocks. For this reason, it might be necessary to either remove the portal from the additional portal groups, or assign the threat level group to all of the portal groups.

Example: An administrator who uses a portal group to unlock a building's portals during normal business hours may want the portals to remain locked on snow days, requiring card reads for access. To accomplish this, he could create a threat level group containing all defined threat levels except one named Snow Day, and then apply the group to his portal group. On days when the building's threat level changes to Snow Day, its portals will remain locked.

To cause online remote locksets to enter and exit panic mode under certain threat levels:

1. [Create a threat level group](#) containing only the threat levels under which a remote lockset should *not* be in panic mode.
2. On the [Portal Groups page](#), select a portal group that includes one or more online remote locksets.
3. Assign the new threat level group to the portal group and click **Save**.

An individual lockset in the group will enter panic mode only if its location changes to a threat level that is not included in the assigned threat level group. Once the lockset has entered panic mode, it will exit that mode only if its location changes to one of the threat levels in the assigned threat level group.

To make an access level invalid under certain threat levels:

1. Create a [threat level group](#) containing only the threat levels under which an access level should be considered valid.
2. On the [Access Levels page](#), select an access level.
3. Assign the new threat level group to the access level and click **Save**.

When a user with this access level presents valid credentials to a reader, access will be granted *only* if the reader's location is currently under one of the threat levels in the assigned threat level group.

CAUTION: If a person is assigned multiple access levels, the most permissive access level will determine whether access is granted or denied. For this reason, it might be necessary to either eliminate additional access levels in the person's record, or assign the threat level group to all of the person's access levels.

To make Double Card Presentation mode invalid for a portal under certain threat levels:

1. Create a [threat level group](#) containing only the threat levels under which [Double Card Presentation mode](#) should be considered valid.
2. On the [Portals page](#), select a portal for which Double Card Presentation Mode is enabled.
3. In the Double Card Presentation section, select the new threat level group and click **Save**.
When a [qualified user](#) performs a double read at the portal, the portal will switch to the unlocked or locked state *only* if its location is currently under one of the threat levels in the assigned threat level group.

To make an event action invalid under certain threat levels:

1. Create a [threat level group](#) containing only the threat levels under which an [event action](#) should be considered valid.
2. On the [Events page](#), select an event or define a new event.
3. Select an action or [define a new action](#) for the event.
4. Under **action details**, assign the new threat level group to the action and click **Save**.
When the event is activated, the action will be performed *only* if the default location in the active partition is currently under one of the threat levels in the assigned threat level group.

To make a user role invalid under certain threat levels:

1. Create a [threat level group](#) containing only the threat levels under which a custom [user role](#) should be considered valid.
2. On the [User Roles page](#), select a user role or define a new user role.
3. Assign the new threat level group to the user role and click **Save**.
When a user with this user role attempts to log in, the login will be allowed *only* if the default location in the active partition is currently under one of the threat levels in the assigned threat level group.

To change a location's threat level using an event action:

1. On the [Events page](#), select an event or define a new event.
2. [Add an action](#) to the event, selecting "Set Threat Level" from the **Action** drop-down list and one of the available threat levels from the **Change to Threat Level** drop-down list.
When the event is activated, the selected threat level will be applied to the default location in the active partition—unless you select a different location from the **At Location** drop-down list. To apply the threat level to all sub-locations of the selected location, select the **Apply to Sublocations** check box.

Tip: To apply the selected threat level to the entire system, select **Master location** and then select **Also apply to sublocations**.

3. Click **Save**.

See also: [Setting Up Threat Level Groups](#)

[Effects of Applying a Threat Level Group: Example](#)

[Setting the Threat Level](#)

[Setting Up Portal Groups](#)

[Enabling Double Card Presentation Mode for Portals](#)

[Creating User Roles](#)

[Defining Event Actions](#)

Effects of Applying a Threat Level Group: Example

For each portal or other entity to which a threat level group is applied, the group defines which threat levels should be considered valid (those included in the group) and which should be considered invalid (those excluded from the group).

Threat level groups can be used to raise the level of protection for a location when its threat level changes to one considered insecure or dangerous, and to lower the level of protection when the threat level returns to normal.

For example, suppose you have defined separate [locations](#) for individual buildings at your site. You have created a threat level group named Low-to-High, which includes all defined threat levels except Severe. You have applied the new group to various portals, portal groups, access levels, event actions, and user roles.

(1) If the threat level for the Building A location changes to Severe, the change will affect:

- Any **portal** in Building A that is a member of a **portal group** to which the Low-to-High threat level group is assigned.
The portal will fail to unlock and relock even if the portal group's Unlock time spec is valid and its First-in Unlock rule (if one is defined) is satisfied.
- Any reader in Building A that is presented with an **access level** to which the Low-to-High threat level group is assigned.
When a cardholder with this access level presents valid credentials to the reader, access will be denied.
- Any **portal** in Building A that is using [Double Card Presentation mode](#) and to which the Low-to-High threat level group is assigned.
The portal will unlock and relock on a valid card read, but it will not honor a double read.

These behaviors will return to normal once Building A returns to a valid threat level (one that is a member of the Low-to-High group).

(2) If the threat level for the default location in the active partition changes to Severe, the change will affect:

- Any **event action** to which the Low-to-High group is applied.
When an event for which the action is defined is activated, the system will fail to perform the action.
- Any **user role** to which the Low-to-High group is applied.
A user with such a role will be unable to log into the system. If the user is already logged in, the session will end and the user will be logged out.

These behaviors will return to normal once the default location in the active partition returns to a valid threat level (one that is a member of the Low-to-High threat level group).

Time

Select **Configuration : Time** to display the following options.

Choose this	To see information on
Holidays	Creating, editing, and deleting holidays, which act as exclusions to time specs that do not include them.
Network Controller	Setting the system time and time server.
Time Specs	Creating, editing, renaming, and deleting time specs.
Time Spec Groups	Grouping individual time specs to create more complicated schedules.

See also: [Changing a Person's Access](#)

[Setting the Network Controller Time](#)

[Setting the Time Zone Using Initmode](#)

Creating Holidays

Select **Configuration : Time : Holidays**.

Holidays let you override time specs for specific periods of time. For example, suppose you use a time spec to unlock your building's doors on weekdays, but you want the doors to remain locked on New Year's Day—even if it falls on a weekday. To do this, you can define a holiday that starts and ends on January 1. By adding the holiday to a holiday group and excluding the group from your time spec, you can ensure that the doors will never unlock on New Year's Day.

Each holiday must be assigned to at least one holiday group, and it can be assigned to up to three groups. When defining a [time spec](#) and selecting the days of the week and holiday groups to be included, you will select only the holiday groups containing holidays on which you want the time spec to work. The holidays in all other holiday groups will override the time spec.

Example: You have assigned a *Weekends* time spec to the access level of each employee who should be allowed access to your facility on Saturdays and Sundays. To deny access to these employees on a particular Sunday, you can create a holiday that starts and ends on that day, include it in Holiday group 1, and exclude Holiday group 1 from the "Weekends" time spec. If managers require access on that Sunday, you can assign a different time spec to their access levels that includes Holiday Group 1.

To create a holiday:

1. Click the **add** link under the **Name** drop-down list.
2. Enter a **Name** for the new holiday and, optionally, a **Description** that explains its use.
3. Select one or more holiday groups in which this holiday should be included.

4. Enter a **Start Date** and **End Date** for the holiday. You can click the calendar icons to select these dates from a calendar.

When entering these times, use a 24-hour time format. For a one-day holiday, the normal start time is 00:00 and the normal end time is 23:59 on the same day.

5. Click **Save**.

NOTE: Mercury panels recognize the start and end dates you specify when creating a holiday, but not the start and end times. For a Mercury panel, a holiday always begins at 00:00:00 on the specified start date and ends at 23:59:59 on the specified end date. See [Configuring Partial-Day Holidays for Mercury Panels](#) for information on a procedure you can use to work around this limitation.

To edit a holiday definition:

1. Select an existing holiday from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this holiday.
2. Edit any of the fields.
3. Click **Save**.

CAUTION: Changing a holiday definition will change valid access times for any time spec that does NOT include the holiday. This is because holidays act as exclusions to all time specs that do not include them.

To delete a holiday:

1. Select an existing holiday from the **Name** drop-down list.
2. Click **Delete**.

See also: [Creating Time Specs](#)

[Setting Up Access Levels](#)

Setting the Network Controller Time

Select **Configuration : Time : Network Controller**.

With this page you can:

- Set the current time on the network controller.
- Enter network time server DNS names.
- Set the time zone for your controller.

Use of an NTP network time server ensures that the Network Controller will be regularly synchronized with the exact time used by all other network resources. At least one time server must be designated for the Network Controller to synchronize its own time. If no timeserver is available the Network Controller time will drift.

NOTE: Time changes required for **Daylight Saving Time** will be automatic as long as the controller is configured with a valid time server. The controller re-synchronizes its time four times each day at 12 AM, 6 AM, 12 PM, and 6 PM.

Current Network Controller Time displays the current time of the Network Controller clock.

Setting the Network controller time:

1. Select from the **Manually Set Date/Time** drop-down lists the correct current time.
2. In the **Timeserver 1** field the default preset name is **ntp.ubuntu.com**. If the network controller is installed on a network with Internet access then this setting need not be changed.

If there is no Internet access:

- The network administrator can supply you with a local network timeserver name and you can enter that name here.
 - If there is no timeserver, remove the timeserver name from this field or the network controller will spend several minutes searching for this server.
3. (optional) Change the **Timeserver 2** and **Timeserver 3** fields as appropriate.
 4. Select from the **Timezone** drop-down the correct time zone for your area.

See also: Configuring Network Nodes

[IP Setup Using Initmode](#)

About Time Specs

A time spec defines a period of time during which any feature to which it is applied will be in effect. For example, a time spec can define an automatic unlock period for the portals in a portal group, an automatic arming period for an alarm panel or input group, or valid access times for a user's access level.

NOTE: For a complete list of the features to which time specs can be applied, see [Creating Time Specs](#).

When creating a time spec, you must specify when it will be valid. To do this, you select:

- [A start time and end time](#), to define the time of the day when the time spec will be valid.
- [Days of the week](#), to define the combination of days of the week when the time spec will be valid.
- [One or more holiday groups](#), to define the holidays on which the time spec will be valid.

Selecting Start and End Times

To define the time of the day included in a time spec, you enter a start time and end time, using a 24-hour format. Any feature to which the time spec is applied will be in effect during this time (assuming that all other rules governing the feature's availability are also valid).

The time spec period will begin on the first second of the start time you enter. For example:

- If you enter a start time of **08:00**, the time spec period will begin at 8 AM—or more precisely, at 08:00:01.
- If you enter a start time of **15:15**, the time spec period will begin at 3:15 PM—or more precisely, at 15:15:01.

The time spec period will end on the *last* second of the end time you enter. For example:

- If you enter an end time of **12:59**, the time spec period will end at 1 PM—or more precisely, at 12:59:59.

- If you enter an end time of **17:29**, the time spec period will end at 5:30 PM—or more precisely, at 17:29:59.

When defining start and end times, keep these guidelines in mind:

- The time spec period will end almost a minute after the end time you enter. For example, if you enter an end time of 10:30, the time spec period will actually end closer to 10:31.
- If the start time you enter is after the end time—for example, if the start time is 10 PM (22:00) and the end time is 2 AM (01:59)—the time spec period will span a day boundary. This means that it will start on each of the selected days of the week and will end on the following day, even if that day is not selected. See the following section for more information.

Selecting Days of the Week

When creating a time spec, you can select any combination of days of the week. Any feature to which the time spec is applied will be in effect on those days (assuming that all other rules governing the feature's availability are also valid).

The time spec period will begin on each of the days of the week you select and will end on the same day. An exception is a time spec period that spans a day boundary. In this case, the time spec period will begin on each of the selected days of the week and will end on the following day, even if that day is not selected.

For example, to create a time spec for employees whose work week begins at 10 PM on Monday and ends at 6 AM on Saturday, you would:

- Enter a start time of 10 PM (22:00)
- Enter an end time of 6 AM (05:59)
- Select the days Monday, Tuesday, Wednesday, Thursday, and Friday

Saturday is not selected; however, because the time spec period starts on Friday and spans a day boundary, it will end on Saturday.

	Sun	Mon	Tues	Wed	Thurs	Fri	Sat	H1	H2	H3
12 ^{am}										
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12 ^{pm}										
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										

Selecting Holiday Groups

By default, [holidays](#) provide exceptions to time specs. If a holiday occurs on a day of the week when a time spec would normally be valid, the time spec will be invalid on that day.

To override this default behavior for an individual time spec, you can include one or more holiday groups in its definition. If any of the holidays contained in these groups occurs on a day of the week that is included in the time spec definition, the time spec will be valid on that holiday.

Suppose, for example, that the Labor Day holiday (a U.S. holiday that always occurs on a Monday) is defined in your system and is a member of Holiday Group 1. To allow certain employees to access your facility on that day, include Holiday Group 1 in a time spec that also includes Monday, and assign that time spec to the employees' access levels.

Note that including a holiday group in a time spec does not make the time spec valid on a holiday in that group if it occurs on a day of the week when the time spec would normally be invalid. For example, if a time spec that includes only the days Wednesday and Thursday also includes a holiday group containing a Monday holiday, the time spec will not be valid on that holiday.

See also: [Creating Time Specs](#)

[Creating Time Spec Groups](#)

[Creating Holidays](#)

Creating Time Specs

Select **Configuration : Time : Time Specs**.

With this page you can create, change, and delete [time specs](#). A time spec can be applied to:

- An [access level](#), to specify valid access times for users.
Depending on your needs, you might want to define a variety of time specs for different users. For example, you could create a time spec named "Weekdays 8 AM to 6 PM" for employees requiring access during the standard work week, and a time spec named "Weekdays 7 PM to 10 PM" for members of the cleaning crew.
- A [portal group](#), to specify an automatic unlock period for its portals.
- An elevator [floor group](#), to specify a free-access period for secure floors.
- An [alarm panel](#) or [input group](#), to specify an automatic arming period for the alarm panel or the group's inputs.
- An [output group](#), to specify an automatic activation period for its outputs.
- A [portal](#), to specify periods when use of its keypad and outgoing reader will be required, when its two-man access restriction will be in effect, or when [Double Card Presentation mode](#) will be in effect.

NOTE: The default time specs, **Always** and **Never**, cannot be edited or deleted. The **Always** time spec allows access at all times—including defined [holidays](#), which normally act as exclusions to time specs.

To create a time spec:

1. Click the **add** link under the **Name** drop-down list.
2. Enter a **Name** for the new time spec and, optionally, a description that explains its use.
3. Enter a **Start Time** and an **End Time** in 24 hour format: for example, enter **09:00** for 9 AM.
The time spec will be in effect from the first second of the start time through the last second of the end time. For example, if you enter 09:00 for the start time and 17:59 for the end time, the time spec will be in effect from 9 AM to 6 PM—or more precisely, from 09:00:01 to 17:59:59.
4. Select the check box for each day of the week you want to include in the time spec.
IMPORTANT: For a time spec whose start time is later than its end time, the time spec period will end on the day *following* the last day of the week you select. For example, suppose that when setting up a "Weekdays 8 PM to 7 AM" time spec, you select the days Monday through Friday. The time spec period will start at 8 PM on Monday and will end at 7 AM on Saturday, even though Saturday was not one of the days you selected. To have the time spec period end at 7 AM on Friday, you would need to select only the days Monday through Thursday.
5. Select any [holiday group](#) containing holidays you want to include in the time spec.
Any holiday that is not included in the time spec will override it. For example, unless a particular holiday is included in the time spec assigned to an access level, users with that access level will be denied access on that holiday—even if it falls on a day of the week included in the time spec.
6. Click **Save**.

To edit a time spec:

1. Select an existing time spec from the **Name** drop-down list.
The remaining fields on the page fill with the settings for this time spec.
2. Edit the fields that require changes.
3. Click **Save**.
CAUTION: Time specs are part of [access level definitions](#). When you change a time spec you are changing any access level that uses the time spec as part of its definition.

To delete a time spec:

1. Select an existing time spec from the **Name** drop-down list.
If the time spec is defined as part of one or more access levels, these access levels will be listed next to **In Access Level(s)**. Before you can delete this time spec, you will need to remove it from these access level definitions.
2. Click **Delete**.

To rename a time spec:

1. Click the **rename** link under the **Name** drop-down list, then enter a new name into the field.
2. Click **Save**.

See also: [About Time Specs](#)

[Creating Holidays](#)

[Enabling Double Card Presentation Mode for Portals](#)

Creating Time Spec Groups

Select **Configuration : Time : Time Spec Groups**.

With this page you can create, edit, rename, and delete time spec groups. These groups can be used to create complex schedules covering non-contiguous hours on the same day.

You can use time spec groups in the same ways as individual [time specs](#). For example, you can apply them to [access levels](#) to specify valid access times, to [portal groups](#) to specify automatic unlock periods, and to [alarm panels](#) to specify automatic arming periods.

To create a time spec group:

1. Click the **add** link under the **Name** field.
2. Enter a **Name** for the new time spec group and, optionally, a **Description** that explains its use.
3. In the **Time Specs Available** list, select each time spec you want to add to the group and click the right-arrow button to move it into the **Selected** list. There is a limit of eight time specs per group.

Each time you select an available time spec, the hours affected by that spec appear in blue on the time schedule matrix to the right. When you move the time spec to the Selected list, the matching whole hours appear in yellow, and the matching partial hours appear in red.

TIP: You can click an hour on the time spec map to display the names of the matching time specs and/or holiday groups.

4. Click **Save**.

To delete a time spec group:

1. Select an existing time spec group from the **Name** drop-down list.
2. Click **Delete**.

See also: [Creating Holidays](#)

[Creating Time Specs](#)

[How Groups are Used in the System](#)

Widget Desktops

Select **Configuration : Widget Desktop** to display the following options.

Choose this	To see information on
Compose	Composing, editing, and saving custom Widget Desktop layouts.
Group	Creating groups of Widget Desktop layouts for assignment to specific

user roles.

See also: [Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[Using the Monitoring Desktop](#)

Composing Widget Desktop Layouts



Select **Configuration : Widget Desktops : Compose**.

The default Widget Desktop layout provides a starting point for creating custom, real-time displays for monitoring the system. To compose a new layout, you can make various changes to the default layout and then save it as a new layout.

On this page you can:

- [Compose and edit Widget Desktop layouts](#).
- [Set properties that determine the available options on the Desktop menu for a layout](#).
- [Set default widget properties for a layout](#).


To compose or edit a Widget Desktop layout:

1. Select **Configuration : Widget Desktops : Compose**.
2. In the **Load Layout** dialog box, select the layout you want to modify—or select **Default** to create an entirely new layout—and then click **OK**.
3. To change the desktop background, right-click anywhere on the background, select a number from the **Background** drop-down, and then click **OK**.
4. Change the selected layout by doing any of the following:
 - To move a widget, click its title bar and drag it to a different location in the layout.
 - To resize a widget, drag any of its edges or corners until it is the size you want.
 - To minimize a widget, click the minimize button  in its upper right corner
 - To add a new widget to the layout, select it from the **Desktop** menu in the lower left corner of the page.
 - To remove a widget from the layout, click the close box  in its upper right corner.

NOTE: You can configure various properties for the widgets that will appear in the layout. See [Configuring a Widget's Common Properties](#), [Configuring a Widget's Scope Properties](#), and [Configuring a Widget's Unique Widget Properties](#).

6. When the layout is complete do either of the following:
 - To save the modified layout, select **Save Layout** from the **Desktop** menu and then click **OK**.
 - To save the modified layout as a new layout, select **Save Layout As....** , enter a new layout name, and then click **OK**.

To set properties for the current layout:

1. Click this button  in the lower left corner of the page to open the Layout Properties dialog box.

2. To turn on the snap to grid feature, select the **Snap to Grid** check box.

A grid overlay appears on the desktop background. Whenever you move or resize a widget in the current layout, the widget will align to the nearest intersection of lines in the grid.

NOTE: If this check box is selected when you save the layout, the grid will appear when a user views the layout in monitor mode. There will be no way for the user to turn off the grid.

3. To increase or decrease the number of pixels between the grid lines, select a different number from the **Grid size** drop-down list. The default grid size is 5 pixels, and you can increase it to 10, 25, or 50 pixels.
4. If the layout will be displayed on an Apple iPad or MacBook Air, select one of the following from the **Show layout guide** drop-down list:
 - **iPad Landscape Viewable Area (1024 x 586)**
 - **iPad Portrait Viewable Area (768 x 1160)**
 - **MacBook Air 13" (1440 x 900)**

Vertical and horizontal red lines appear on the desktop background, representing the right and bottom edges of the iPad or MacBook Air screen. Positioning all widgets within these lines ensures that the layout will fit the screen display.

5. Select or clear the **Load Layout** check box to determine whether users will be able to load other layouts.

The **Load Layout** option will be available on the Desktop menu only if this check box is selected.

6. Select or clear the check box for each widget in the list to determine whether users will be able to add it to the layout.

A widget will be available on the Desktop menu only if its check box is selected.

7. Select or clear the **Logoff** check box to determine whether users will be able to log off from the system.


The **Logoff** option will be available on the Desktop menu only if this check box is selected.

8. Select or clear the **Exit** check box to determine whether users will be able to exit the Widget Desktop.

The **Exit** option will be available on the Desktop menu only if this check box is selected.

9. Click **OK**.

To set default widget properties for the current layout:

1. Click this button  in the lower left corner of the page.
2. Select the check box for each widget property that should be selected by default in new widgets that are added to the layout.
3. To apply the selected properties to existing widgets in the layout, select the **Apply properties to existing widgets** check box.
4. Click **OK**.

To exit the Compose page:

- Make a new menu selection to navigate to a different page.

See also: [Setting Up Multi-Camera Views](#)

[Summary of the Available Widgets](#)

[The Camera View Widget](#)

[About Widget Properties](#)

[Using the Widget Desktop](#)

Grouping Widget Desktop Layouts

Select **Configuration : Widget Desktops : Group**.

On this page you can create, change, rename, or delete Widget Desktop layout groups. When a layout group is included in a user role, users holding that role will be able to monitor layouts in the group and select them as users' default layouts.

To create a Widget Desktop layout group:

1. Enter a name for the group in the **Name** text box. You might need to click the add link if groups have already been created.
2. In the Layouts Available list, click to select a specific layout needed for this group.
3. Click the right arrow button to move the selected layout from the Available list to the Selected list. Repeat this process until all layouts needed for this group appear in the Selected list.
4. Click **Save**.

To delete a Widget Desktop layout group:

1. Select the group you want to delete from the **Name** drop-down list.
2. Click **Delete**.

See also: [Creating User Roles](#)

[Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Using the Monitoring Desktop](#)

[How Groups are Used in the System](#)

Summary of the Available Widgets

Select **Configuration : Widget Desktops : Compose**.

As part of the process of composing or editing a Widget Desktop layout, you can add widgets by selecting them from the **Desktop** menu in the lower left corner of the page. The widgets that may be available on the menu are:

- **Activity Log:** See [Monitoring the Activity Log](#).
- **Alarm Workflow:** See [The Alarm Workflow Widget](#).
- **Auto-Monitor:** See [The Auto-Monitor Widget](#).
- **Camera View:** See [The Camera View Widget](#).
- **Clock:** See [The Clock Widget](#).
- **DMP Intrusion Panels:** See [The DMP Intrusion Panel Widget](#).
- **Duty Log Entry:** See [Entering Duty Log Messages into the Activity Log](#).
- **Elevator Status:** See [The Elevator Status Widget](#).
- **Events:** See [Using the Monitoring Desktop](#).
- **Explorer:** See [The Explorer Widget](#).
- **Floorplans:** See [Monitoring Floorplans](#).
- **Passback Grace:** See [The Passback Grace Widget](#).
- **Photo ID History:** See [The Photo ID History Widget](#).
- **Portal Status** and **Portal Unlock:** See [The Portal Status and Portal Unlock Widgets](#).
- **Statistics Block:** See [The Statistics Block Widget](#).
- **Status:** See [The Status Widget](#).
- **Threat Level:** See [The Threat Level Widget](#).

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[About Widget Properties](#)

[The Home Page](#)

Widget Properties You Can Configure



Select **Configuration : Widget Desktop : Compose**.

You can configure the following types of properties for the widgets that will appear in a Widget Desktop layout:

- **Common properties** are shared by all widgets. By setting these properties for a widget, you can determine whether the widget will appear on the Widget Desktop when the layout is loaded; the initial position, size, and state (either open or minimized) of the widget; and whether users will be able to move, size, minimize, and close the widget for individual monitoring sessions.
For more information, see [Configuring a Widget's Common Properties](#).
- **Scope properties** are shared by most widgets. By setting these properties for a widget, you can determine which partitions the widget displays data from, the types of data displayed in the

widget, and whether users will be able to expand or narrow the scope of the data for individual monitoring sessions.

For more information, see [Configuring a Widget's Scope Properties](#).

- **Unique properties** are particular to a given widget. Unique widget properties that cannot be made configurable by users are available by clicking this icon  in the upper left corner of the widget. (These properties appear in the bottom section of the dialog box.) Unique properties that users will be able to change if you make the widget configurable are available by clicking this icon  in the upper left corner of the widget.

For more information, see [Configuring a Widget's Unique Properties](#).

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)




[Grouping Widget Desktop Layouts](#)

Configuring a Widget's Common Properties

Select **Configuration : Widget Desktops : Compose**.


When composing or editing a Widget Desktop layout, you can configure various properties for the widgets that will appear in the layout. Many of these properties are common to all widgets. They determine the extent to which users will be able to modify the widgets for individual monitoring sessions. You can configure these properties for individual widgets in a Widget Desktop layout, or as the defaults for a layout.

The common widget properties are:

- **Closable:** Users will be able to click this icon  to close the widget.
- **Minimizable:** Users will be able to click this icon  to minimize the widget.
- **Movable:** Users will be able to drag the widget to different locations on the Widget Desktop.
- **Resizable:** Users will be able to drag any corner of the widget to resize it.
- **Configurable:** Users will be able to click this icon  to change the widget's properties for individual monitoring sessions.

NOTE: Many widgets have unique properties you can configure. For more information, see [Configuring a Widget's Unique Properties](#).


To configure common properties for an individual widget:

1. Select **Configuration : Widget Desktops : Compose**, select the layout you want to modify—or select **Default** to create an entirely new layout—and then click **OK**.
2. Click this icon  in the upper left corner of the widget you want to modify.
3. To change the name that will appear in the widget's title bar, enter a new name in the **Name** box.
4. Select the check box for each of the properties described above that you want to set for the widget.

NOTE: Many widgets have two additional properties: **Allow multiple partition viewing** and **Allow filtering**. For information on these properties, see [Configuring a Widget's Scope Properties](#).

6. Click **OK**.
7. To preview the modified widget, click **Preview** on the **Desktop** menu in the lower left corner of the page. Click **End Preview** when you want to return to Compose mode.

To configure common properties as the defaults for a layout:

1. Select **Configuration : Widget Desktops : Compose**, select the layout you want to modify—or select **Default** to create an entirely new layout—and then click **OK**.
2. Click this icon  in the lower left corner of the page to open the **Default Widget Properties** dialog box.
3. Select the check box for each property you want to set as a default for the layout.
4. For the **Apply properties to existing widgets** option, do one of the following:
 - Clear the check box if you want the selected properties to be applied only to widgets you add to the layout. This is the default setting.
 - Select the check box if you want the selected properties to be applied both to widgets you add to the layout and to widgets currently displayed in the layout.
6. Click **OK**.
7. To preview the modified widgets, click **Preview** on the **Desktop** menu in the lower left corner of the page. Click **End Preview** when you want to return to Compose mode.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)


[About Widget Properties](#)


Configuring a Widget's Unique Properties

Select **Configuration : Widget Desktop : Compose**.

When composing or editing a Widget Desktop layout, you can configure properties for the widgets that will appear in the layout. In addition to configuring properties that are common to all widgets, you can configure unique properties for certain widgets.

To configure a widget's unique properties:

1. In the Load Layout dialog box, select the layout you want to modify—or select **Default** to create an entirely new layout—and then click **OK**.
2. Do either of the following in the upper left corner of any of the widgets listed below: Click this icon  to configure unique properties of the widget that cannot be made configurable by users. (These properties appear in the bottom section of the Properties dialog box.) Click this

icon  to configure properties that users will be able to change if you make the widget configurable.

- **Auto-Monitor:** See [The Auto-Monitor Widget](#).
- **Alarm Workflow:** See [The Alarm Workflow widget](#).
- **Camera View:** See [The Camera View Widget](#).
- **Clock:** See [The Clock Widget](#).
- **Explorer:** See [The Explorer Widget](#).
- **Passback Grace:** See [The Passback Grace Widget](#).
- **Photo ID History:** See [The Photo ID History Widget](#).
- **Portal Status:** See [The Portal Status and Portal Unlock Widgets](#).
- **Statistics Block:** See [The Statistics Block Widget](#).
- **Status:** See [The Status Widget](#).
- **Threat Level:** See [The Threat Level Widget](#).

3. Click **OK**.

See also: [Composing Widget Desktop Layouts](#)

[Summary of the Available Widgets](#)

[Using the Widget Desktop](#)

[Configuring a Widget's Common Properties](#)

[Configuring a Widget's Scope Properties](#)

Configuring a Widget's Scope Properties

Select **Configuration : Widget Desktops : Compose**.


By default, widgets display all available data from the active partition. However, many widgets have scope properties you can configure to customize the data they will display. Depending on the widget, you may be able to configure it to display:

- Data from all partitions to which a user has access.
- Data from one or more selected partitions.
- Specific types of data only.
- Data matching specific text only.

For details on which widgets have scope properties you can configure, see [Summary of the Widget Scope Properties](#).


Before you can configure the scope of the data displayed in a widget, and/or allow users to configure its scope for individual monitoring sessions, you must enable the widget's scope properties.

To enable a widget's scope properties:

1. Select **Configuration : Widget Desktops : Compose**, select the layout you want to modify—or select **Default** to create an entirely new layout—and then click **OK**.
2. Click this icon  in the upper left corner of the widget you want to modify.
3. Select **Allow multiple partition viewing** to enable the widget to display data from multiple partitions rather than from the active partition only.
4. Select **Allow filtering** to enable the widget to display data that has been filtered according to specific criteria.
5. If you want users to be able to change the widget's scope to suit their needs, make sure the **Configurable** check box is selected.
6. Click **OK**.
7. To change the widget's scope for the current layout, use the procedure below.

NOTE: The procedure below assumes that both **Allow multiple partition viewing** and **Allow filtering** have been enabled for the widget.

To change a widget's scope properties:

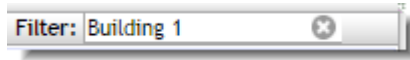
1. Click this icon  in the upper left corner of the widget.
2. To have the widget display data from all partitions to which a user has access, select the **Show multiple partitions** check box.
When you select the check box, a Partition filter appears below it.
3. To narrow down the data to specific partitions, use the Partition filter's right-arrow button to move those partitions from the Available list to the Selected list.
4. For any additional filter that is available for the widget, use the right-arrow button to move the criteria you want from the Available list to the Selected list.
5. If a **Text filter** is available for the widget, enter any text you want to further narrow down the data.
6. Click **OK**.

When a user views the layout during a monitoring session, the widget will display data from any of the partitions you specified to which he or she has access. The data from these partitions will be filtered to include only information matching the criteria and/or text you specified.

To preview your changes:

1. Click **Preview** on the **Desktop** menu in the lower left corner of the page to see the widget as it will appear to users who view the current layout. The changes you made are indicated in the widget's title bar:
 - If you specified that the widget should display data from multiple partitions, the note "(multi-partition)" appears in the title bar.
 - Any filtering criteria you selected are also listed in the title bar. For example, if you applied all available filters, you will see a list similar to this: "(filter by partition, type, text)".

- If you specified a text filter, the text you entered appears in the Filter box on the right side of the widget's title bar, as shown below.



Note that if you made the widget user-configurable, the Filter box will be enabled in the current layout. Users will be able to enter text to filter the data according to their needs, and they will be able clear all text filters by clicking the Clear Filters icon

- If you made the widget user-configurable, this icon appears on the left side of the widget's title bar. Users will be able to click the icon to open the widget's Properties dialog box, where they can configure the widget for individual monitoring sessions.
3. Click **End Preview** to return to Compose mode.

See also: [Composing Widget Desktop Layouts](#)

[Configuring a Widget's Common Properties](#)

[Configuring a Widget's Unique Properties](#)

[Summary of the Widget Scope Properties](#)

[Summary of the Available Widgets](#)

[Using the Widget Desktop](#)

Summary of the Widget Scope Properties

Select **Configuration : Widget Desktop : Compose**.

The following table lists all available widgets and indicates which ones have the ability to display data from multiple partitions and/or filtered data. For each widget that can display filtered data, the table lists the filters you can apply when configuring it for a Widget Desktop layout.

Widget	Multiple Partition Viewing	Filtering	Available Filters
Activity Log	X	X	Partition Log entry type Reader group Text
Alarm Workflow	X	X	Partition Priority filtering level Priority filtering method Text
Auto-Monitor			
Clock			
DMP Intrusion Panel	X	X	Partition

Duty Log Entry			
Elevator Status	X	X	Partition Text
Events	X	X	Partition Priority filtering level Priority filtering method Text
Explorer			
Floorplans			
Passback Grace	X	X	Partition
Photo ID History	X	X	See note below
Portal Status/Portal Unlock	X	X	Partition Text
Statistics Block	X		Partition
Status	X		
Threat Level	X	X	Partition
Video	X	X	Partition View type Text

NOTE: Although you cannot explicitly set scope properties for the Photo ID History widget, you can have it display data from multiple partitions and/or filtered data by anchoring it to an Activity Log widget that has the scope properties you want. The scope of the data displayed in the Photo ID History widget will always match that of the Activity Log widget selected as its **Source Activity Log**. For more information, see [The Photo ID History Widget](#).

See also: [Composing Widget Desktop Layouts](#)

[Configuring a Widget's Scope Properties](#)

[Configuring a Widget's Common Properties](#)

[Configuring a Widget's Unique Properties](#)

[Summary of the Available Widgets](#)

[Using the Widget Desktop](#)

More On Configuring Specific Widgets

The Alarm Workflow Widget

If you configure the Alarm Workflow widget for a Widget Desktop layout, operators will be able to use it to [monitor and resolve alarms](#). The Alarm Workflow widget includes two views:

- The **Offered Alarms** view displays up to 10 of the oldest alarms that are either unowned or are owned by an operator other than the one who is currently logged in. Once an alarm has been resolved, the list is refreshed and if there are 10 or more alarms remaining, you will see 10 again.
- The **My Alarms** view displays all alarms owned by the operator who is currently logged in.

Columns in each view show for each alarm:

- **Priority/Color:** The priority and color specified in the associated 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 became active.
- **Partition:** The partition in which the alarm became active. This column will not appear if the widget is configured to show only alarms from the active partition.
- **Name:** The **Operator short msg**, if one was entered in the associated event definition.
- **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.
- **State:** The current state of the alarm: Active, Escalated, or Urgent.
- **Owner:** (Offered Alarms view only) The name of the user who has adopted the alarm and currently owns it.

Configuring the Alarm Workflow Widget

To configure the Alarm Workflow widget for a Widget Desktop layout, you can set its [common properties](#), its [scope properties](#), and the following unique properties:

- **Priority sorting method:**
 - **Sort by priority:** With this setting, alarms are sorted according to the priority numbers specified in their associated event definitions.
 - **Sort by color:** With this setting, alarms are sorted according to the display colors defined in their associated event definitions.
- **Update progress bar every:** You can select 1, 2, 5, or 10 seconds to determine how often the system will update the progress bars displayed for alarms in the State column.

See also: [Monitoring and Resolving Alarms](#)

[About the Alarm Workflow Widget](#)

[Setting Up Events](#)

[Creating Alarm Workflow Policies](#)

[Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)


[About Widget Properties](#)

The Auto-Monitor Widget

The Auto-Monitor widget provides a quick view of issues that might require attention, such as process failures or access control issues. It is available in selected versions of the security management system, both on the [Home page](#) and on the [Widget Desktop](#) when you are composing new layouts.






For each type of event that has occurred, the Auto-Monitor widget displays a notification indicating the number of such events that are currently active—or in the case of Recent Access Denied Activity notifications, the number that have occurred within a specific time period. Once an active event is resolved, the notification disappears.

You can point to a notification to display an informational tooltip. As shown in the example below, the tooltip shows details about each event, such as the date and time it occurred and the name of the affected device.

 **4 Device(s) have lost communication**

```
0000002410300001 at 11/05/2010 15:20:33
0000002469012740 at 11/05/2010 15:20:33
260000000C054A27 at 11/05/2010 15:20:33
4A000000131EAF27 at 11/05/2010 15:20:33
```

The icon and font color displayed for a notification indicates the event type, as described in the following table.



Notification	Color	Meaning
 Unacknowledged Events	Red	One or more events requiring acknowledgement have not yet been acknowledged.
 Node Communication Loss	Red	One or more Network Nodes or MicroNodes have lost communication.
 Door Forced Open	Red	One or more portals are in the forced open state.
 Door Held Open	Yellow	One or more portals are in the held open state.
 Recent Access Denied Activity	Yellow	One or more of the Invalid Access types configured for the widget have occurred within the Invalid Access History time period configured for the widget. NOTE: Clicking a NOT IN NODE or BIT

MISMATCH message opens the [Card Decoder](#) window.

Configuring the Auto-Monitor Widget

The Auto-Monitor widget has unique properties that you can configure for the current Widget Desktop layout and allow users to configure for individual monitoring sessions.

To configure the Auto-Monitor widget:

1. Click this icon  in the upper left corner of the widget.
2. In the **Tip placement** drop-down list, select the location where you want the informational window to appear when users point to notifications.
3. Select the check box for any of the event types that should be displayed in the widget.
4. If you select any of the **Invalid Access** types, select a time period on the **Invalid Access History** drop-down list.
Invalid accesses of the selected types will be displayed in the widget for the specified time period.
5. Click **OK**.
6. If you want Widget Desktop users to be able to configure these settings for individual monitoring sessions, click this icon  in the upper left corner of the widget, and make sure the **Configurable** check box is selected.


See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)


[About Widget Properties](#)

The Camera View Widget


When [composing a Widget Desktop layout](#), the layout creator can click this icon  in a specific Camera View widget to configure its properties and behaviors. The following options are available:

- **Allow multiple partition viewing** and **Allow filtering**: For information on setting these properties, see [Configuring a Widget's Scope Properties](#).
- **Allow camera to be manually changed**: Displays a drop-down that allows users to select a specific camera or camera view for the widget.
- **System sets widget title**: Allows the system to display the camera name in the title bar of the widget, rather than a name entered in the **Title** text box above. This ensures that if the camera changes, the widget title will reflect the change.
- **Is a camera monitor**: Sets the widget as a camera monitor, which can accept camera views and recorded video from other video widgets. A camera monitor 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.

- **Is the default camera monitor:** Sets the widget as the default camera monitor. Unless another monitor is specified for receiving a video stream, this widget will receive it.
- **Switch to linked camera on an event:** When events are configured, specific cameras can be linked to the event. With this setting, the widget will automatically switch to the event-linked camera when the event is activated.
- **Show person photo ID on access at location:** Sets the live Camera View widget to automatically display (fade in and out) the person's stored photo ID upon "valid access" Activity Log entry, within camera view linked to a reader portal. Both the Activity Log and Camera View widgets must be open on the Widget Desktop for the stored Photo ID to be displayed upon an associated "valid access" reader entry.
- **Photo ID display duration in seconds:** When Auto Display (fade in and out) is configured, this setting determines the duration of the photo ID display.
- **Play video event when activity log icon is clicked:** If an event is configured to record video, the Activity Log displays a camera icon. When this property is set, the widget will display the event-recorded video when the activity log camera icon is clicked.
- **Monitor to which to send video:** Specifies the camera monitor to which the widget will send video when you click the camera-to-monitor icon, if there are multiple camera monitors. If this property is not set, the default camera monitor will receive the images.

In addition, the layout creator can click this icon  in the upper left corner of a specific Camera View widget to set the following properties as its defaults in the current layout:

- **Show multiple partitions:** When selected, specifies that the widget will display data from all partitions to which a user has access. To narrow down the data to specific partitions, the layout creator can select from a list of available partitions.
- **View Type:** Specifies whether the camera will show a single-camera view or a four-camera (Quad) view.
- **Text Filter:** Specifies the text that will be used to filter the data displayed in the widget.
- **Selection:** Specifies a camera for the widget.
- **Show multiple partitions:** When selected, specifies that the widget will display data from all partitions to which a user has access. To narrow down the data to specific partitions, the layout creator can select from a list of available partitions.
- **Aspect Ratio:** The available NetVR options are **Standard-def 4:3 / Wide Screen 16:9**
- **Variable View Type:** The available NetVR options are **Single Camera / Quad View / NetVR 2x2 / NetVR 1+7**
- **Selection:** The available NetVR options appear in a list of defined views.

If the layout creator has made the Camera View widget configurable, monitors will be able to click the same icon  to change these default properties.

NOTE: Once a Camera View widget is set as a camera monitor, as the camera to which an event-linked camera switches, or as the camera that plays event-recorded video, only the **Single Camera** view type can be selected for the widget.

TIP: On a monitor that is too small to display all four cameras in a quad view, increasing the size of the widget and then using its scroll bars may cause the display to begin flashing. If this happens, press F11 on the keyboard.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)


[About Widget Properties](#)

[Configuring a Widget's Common Properties](#)

[Using the Forensic Desktop](#)

The Clock Widget

When the Clock widget is displayed on the Widget Desktop, it shows the current Network Controller time in digital or analog format. If an alarm is set for the clock, the widget plays the configured sound and displays any configured text message at the scheduled time.

If the creator of the Widget Desktop layout has allowed the Clock widget to be configured, monitors can click this icon  in the widget's upper left corner to change its unique properties:

- **Format:** Determines whether the clock has an analog or digital display.
- **Number Style (Analog):** For an analog display, determines the number style. The choices are arabic numerals, uppercase roman numerals, lowercase roman numerals, and tick marks.
- **Hour Color, Minute Color, and Second Color:** Determine the color used to display hours, minutes, and seconds, respectively. Clicking the box for any of these properties displays a color wheel for entering RGB values automatically.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The DMP Intrusion Panel Widget

When the Intrusion Panel widget is open on the Widget Desktop, it displays a tile for each DMP intrusion panel in the system. Monitors can use the widget to view configuration and status information for the panels. Administrators with setup privileges can use the widget to:






- [Arm or disarm an area associated with a panel.](#)
- [Bypass a faulted zone in an area associated with a panel.](#)
- [Activate or deactivate an output associated with a panel.](#)

NOTE: For information about integrating a Digital Monitoring Products (DMP) XR500 Series or XR550 Series control panel into a security management system (SMS), including important information about the ports that must be available for communications between the DMP panel and the SMS, see [Tech Note 18: DMP Intrusion Panel Integration](#).

To view available DMP intrusion panels:

1. If the Intrusion Panel widget is not open on the Widget Desktop, select it from the **Desktop** menu in the lower left corner of the page.
 If the widget is not listed on the menu and you have setup privileges, switch to Compose mode and add the widget to your current layout. Otherwise, ask someone who has setup privileges to add the widget for you.

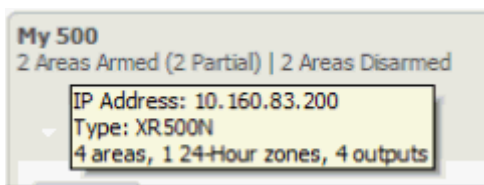
The tile for each panel indicates how many of the associated areas are fully armed, partially armed (containing faulted zones), and disarmed. If there is an error condition on a panel, one or more of the panel status icons will appear on the panel's tile:

Panel Status Icon Meaning	
AC Power 	Panel power is low
Alarm 	Panel is in alarm The panel tile will be red.
Battery 	Panel battery is low
Communications 	Panel has a communications problem
Tamper 	Panel tamper alert

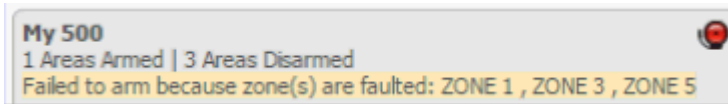
2. Click the tile for a panel to open the associated Panel Detail widget.
 The Panel Detail widget displays detailed status information for the panel. It also includes options for controlling the panel by arming and disarming areas, bypassing and resetting zones, and activating and deactivating outputs. These procedures are described below.

To view the areas associated with a DMP intrusion panel:

1. In the Intrusion Panel widget, click the tile for a panel to open the associated Panel Detail widget.
 The panel name and a summary of its fully armed, partially armed, and disarmed areas are displayed at the top of the widget.
2. Hover over the panel name to view the panel type and configuration:



Below the panel name, you might see a message reporting one or more execution errors. This message is in addition to information reported in the Activity Log. For example, if an area fails to arm, a message with a yellow background will appear:



The message will disappear once other activity occurs.

The areas associated with the panel are shown on a collapsible menu. The menu entry for each area shows the total number of faults for that area. If the area is in alarm, its name and fault count are shown in bold red: **AREA 1 [1 fault]**

Status icons displayed for each area indicate its current state:

Area Status Icon Meaning

Armed



Area is armed

Disarmed



Area is disarmed

In-Schedule



Area is armed due to a schedule

NOTE: If an area is partially armed, a text label indicates the number of areas armed over the total number of areas.

- The first entry on the collapsible menu is expanded to show a list of the zones in that area. To see the zones in a different area, click its entry.

Each zone's name indicates its current alarm status: If a zone is in alarm, its name is shown in bold red.




For zones that have errors, status icons indicate their current states:

Zone Status Icon Meaning

Battery



Zone battery is low

Missing	Zone is missing
	
<hr/>	
Open or Short	Zone circuit is in the open or short state
	
<hr/>	
Trouble	Undefined zone problem
	
<hr/>	

To arm or disarm an area associated with a DMP intrusion panel:

1. In the Panel Detail widget, click the menu entry for the area you want to change.
2. Select one of the following options from the drop-down menu:
 - **Normal:** (default) The area will fail to arm if any zones are faulted.
 - **Bypass Faulted Zones:** Faulted zones will be bypassed automatically, allowing the area to be armed. Each of the bypassed zones will display the label *Bypassed*.
 - **Force Arm:** Faulted zones will be switched to a "ready to be armed" state and each will be armed as soon as it is no longer faulted.
3. Click **Arm**.
Once the change takes effect on the panel, the area's Arm button changes to Disarm.
4. To disarm an area, click its **Disarm** button.

To bypass a faulted zone in an unarmed area:

1. In the Panel Detail widget, click the menu entry for the unarmed area. You cannot bypass a faulted zone in an area that is armed.
 2. Click the **Bypass** button for a faulted zone to switch it to the bypassed state. The Bypass button changes to Reset.
- NOTE:** You cannot bypass a 24-hour zone.

To activate or deactivate an output associated with a DMP intrusion panel:

1. In the Panel Detail widget, click the output you want to change.
2. Click the **Activate** or **Deactivate** button for the output.
Once the change takes effect on the panel, the button toggles to the opposite state, indicating that the output is now activated or deactivated. This may take a few minutes.

See also: [Configuring DMP Intrusion Panels](#)

[Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Elevator Status Widget

If you configure the Elevator Status widget for a Widget Desktop layout, users monitoring that layout will be able to see the current status and unlock schedule for floor-select buttons in the elevators they have permission to view. A user whose [user role](#) gives him or her Free Access privileges for an elevator group will also be able to [manage access to floors](#) from the elevators in that group. The user will be able to:

- Momentarily enable free access for a floor-select button. This will allow temporary access to the floor without the normal access control constraints such as card reads.
- Schedule an extended period of free access or controlled access for a floor-select button. This will allow either free access to the floor, or access controlled by constraints such as card reads, for a specified period of time.

Scheduled actions for elevator floor-select buttons are available only for elevators associated with standard nodes. They are not supported on Mercury panels.

To configure the Elevator Status widget for a Widget Desktop layout, you can set its [common properties](#) and its [scope properties](#).

See also: [Managing Floor Access Using the Elevator Status Widget](#)

[Composing Widget Desktop Layouts](#)


[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Explorer Widget

When the Explorer widget is displayed on the Widget Desktop, it acts essentially as a browser window, delivering content from a web site in real time. For example, the widget can display content from a corporate web site or a local weather site.

If the creator of the Widget Desktop layout has allowed the Explorer widget to be configured, monitors can click this icon  in the widget's upper left corner to change its unique properties:

- **Type:** The type of web site displayed in the widget. The choices are: **Web**, **Secure Web**, **FTP site**, or **about** (to use an internal URI scheme, such as about:blank, rather than a URL).
- **URL:** The URL for the web site displayed in the widget.
- **Refresh Time:** The interval at which the widget will attempt to reload the web page. The choices are: **Never**, **1 minute**, **5 minutes**, **15 minutes**, or **1 hour**.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Passback Grace Widget

When the Passback Grace widget is displayed on the Widget Desktop, monitors can use it to grace card holders from passback and tailgate violations. Once an individual is "graced," his or her next card read will be allowed and no violations will be triggered. For subsequent card reads, all previous anti-passback rules will be in effect for the individual.

To allow monitors to find specific card holders to be graced, the widget includes fields for specifying search criteria, such as **First Name**, **Last Name**, and **Access Level**. When a monitor runs a search, the search results are listed at the bottom of the widget. The monitor can either click any of the **Grace** buttons within the list to grace individual card holders, or click the **Grace all shown** button to grace all card holders in the list.

The creator of a Widget Desktop layout can specify the following unique properties for the Passback Grace widget:

- **Number of search fields:** The specified number determines how many search fields are available on the widget for entering search criteria.
- **Allow user to select search fields:** When selected, monitors can change individual search fields by selecting different search criteria from their drop-downs. For example, a monitor who wants to search for card holders by access level rather than ID number can select **Access level** from the **ID#** field's drop-down.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)


[Summary of the Available Widgets](#)

[System Monitors and Passback Grace](#)

[About Widget Properties](#)

The Photo ID History Widget

When the Photo ID History widget is displayed on the Widget Desktop, it provides a recent history of cardholders who have presented their credentials to readers in the system. For each new access request, a box is added to the upper left corner of the widget. The box shows the cardholder's name and ID photo, the name of the reader, and the date and time the credentials were read. Depending on how the widget was configured for the selected layout, the box might also display information from one of the user-defined fields displayed in the cardholder's [person record](#).

Clicking the cardholder's name for a particular access request opens a Personal Information widget in which his or her person record is displayed. Clicking the icon to the right of the cardholder's name  opens a Duty Log Entry widget, which can be used to enter [duty log comment](#) into the Activity Log.


The boxes displayed in the Photo ID History widget are color coded:

- A blue box indicates that access was granted.
- A red box indicates that access was denied.
- A gray box indicates that access was denied and the cardholder is unknown.
- A box in the color selected for **Trace person log color** on the Network Controller page indicates that the cardholder's activity is currently being [traced](#).


Each instance of the Photo ID History widget is anchored to an Activity Log widget, which is the source of its access data. When the widget for the source Activity Log is added to the current layout, the information in the Photo ID History widget is updated automatically.

NOTE: Just as in the Activity Log, a monitor can click the **PASSBACK** or **TAILGATE** message displayed for a cardholder in the Photo ID History widget to grace that person from passback and tailgate violations.

About the Widget's Unique Properties

For any instance of the Photo ID History widget, the layout creator can click this icon  in its upper left corner and configure the following properties:

- **Cache size:** Specifies the number of cardholders to be displayed. The cache size can be set to any number from 100 to 2500. Whenever there are more cardholders displayed than can be shown in the widget, a scroll bar appears so a monitor can scroll through the list.
- **Note field:** Specifies a user-defined field whose value should appear for an access request, if that field is filled in on the cardholder's person record.
- **Show incomplete accesses:** Specifies whether incomplete access requests will appear in the widget.

In addition, the layout creator—or a monitor if the widget has been made configurable—can click this icon  and configure the following properties:

- **Source Activity Log:** Anchors this instance of the widget to a particular Activity Log widget, which will be the source of its access data.
- **Show only most recent access request:** Replaces the widget's current view showing a history of recent access requests with a new view showing only the most recent access request. In this view, the cardholder's ID photo is displayed in a larger size, to make identification easier.

See also: [Monitoring the Activity Log](#)

[Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Portal Status and Portal Unlock Widgets

When the Portal Status and Portal Unlock widgets are displayed on the Widget Desktop, you can use them to work with portals in the following ways:

- View a portal's current location, state, and unlock schedule. Note that you cannot view the current state of an [ASSA ABLOY online remote lockset](#).
- View the current threat level for any portal whose [location](#) has a different threat level than the partition's default location.
- [Momentarily unlock a portal](#). (You can also do this using [the Portal Status page](#) or the **Unlock Portal** command in the [command palette](#).)
- [Switch a portal to a locked or unlocked state](#). This removes the portal from the automatic control of any [scheduled action](#), [double card read](#), or [portal group](#) time spec currently in effect for the portal. It also suspends any [event action](#) defined for the portal.
- [Disable or enable a portal](#). Disabling a portal locks it and temporarily removes it from the system's control.
- [Schedule an extended lock or unlock of a portal](#). (You can also do this using the [Portal Status page](#) or the [Schedule Action page](#).)

If an ASSA ABLOY online remote lockset that has been put into a locked state by a scheduled action is unlocked by an event, it does not return to the locked state once the event ends.

NOTE: If [Allow filtering](#) is enabled for either widget and the widget is configurable, you can enter text in the **Filter** box to narrow down the list of portals, making it easier to find the one you want.

To momentarily unlock a portal:

1. Do either of the following:
 - In the Portal Status widget, locate the portal in the table.
 - In the Portal Unlock widget, select the portal from the drop-down list.


To make it easier to find a portal in the drop-down list, you can narrow down the list by changing the **All Portals** setting to **Favorites** or **Recent**.

2. Click **Momentarily Unlock Portal** .

The portal will unlock for its configured unlock duration.

NOTE: An online remote lockset will be taken out of panic mode if necessary, then returned to panic mode at the end of the unlock duration.

To switch a portal to a locked or unlocked state:

1. Do either of the following:
 - In the Portal Status widget, locate the portal in the table.
 - In the Portal Unlock widget, select the portal from the drop-down list.
2. To switch the portal to a locked state, click **Lock Portal** .


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. To switch the portal to an unlocked state, click **Unlock Portal** .


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.

To disable or enable a portal:

1. Do either of the following:
 - In the Portal Status widget, locate the portal in the table.
 - In the Portal Unlock widget, select the portal from the drop-down list.

2. To disable the portal, click **Disable Portal** .



The portal is temporarily removed from the system's control.

3. To enable the portal, click **Enable Portal** .

The portal is returned to the system's control.

NOTE: It may take several minutes to enable an [online remote lockset](#). This is because all of its credentials and time specs, which were removed when it was disabled, must be restored.



To schedule an extended unlock of a portal:

1. Do either of the following:
 - In the Portal Status widget, locate the portal in the table.
 - In the Portal Unlock widget, select the portal from the drop-down list.
2. Click **Edit Schedule**  to display a list of scheduled actions for the selected portal.
3. To add a scheduled action, click add .
4. In the dialog box that appears, select **Lock** or **Unlock** from the **Action** drop-down list.
5. For the **Uses Time** setting:
 - Select **System Time** if you want the start and end times to be based on the time zone set for the controller.
 - Select **Local Site Time** if you want the start and end times to be based on the time zone set for the local node.

For example, suppose that the controller is in the Eastern time zone and the node is in the Central time zone (one hour earlier). To have the action start at 9 a.m. you can either enter the start time as 09:00:00 and select Local Site Time, or enter the start time as 10:00:00 and select System Time.

6. 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.
7. 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 Date/Time.
 - **After:** The action will end once the number of specified hours and minutes past the action's start time have elapsed.
 8. In the **Comment** box, enter any comments you want to appear in the list of scheduled actions for the portal.
 9. 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.
 10. To remove a scheduled action, repeat step 2, select the action, click delete , and click **OK**.
 11. 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**.

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 customize the Portal Unlock widget:

1. To limit the number of portals displayed on the portal selection drop-down list, do either of the following:
 - Select **Favorites** from the leftmost drop-down to display only the portals on the Favorites list
 - Select **Recent** from the leftmost drop-down to display only the portals you have selected most recently.

Your changes will remain in effect until you change the selection from the drop-down list, or close the widget or the selected layout.
2. To modify the Favorites list, select a portal and do either of the following:
 - Click this icon  to add the portal to the Favorites list.
 - Click this icon  to remove the portal from the Favorites list.

Your changes to the Favorites list are permanent.

To customize the Portal Status widget:

1. Click this icon  in the upper left corner of the widget.
2. Select the **Always Show Threat Level** check box.

For every portal shown, the widget will now display the current threat level at the portal's location.

See also: [Monitoring the Activity Log](#)

[Unlocking Portals and Viewing Their Status](#)

[Composing Widget Desktop Layouts](#)


[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Statistics Block Widget

When the Statistics Block widget is displayed on the Widget Desktop, monitors can use it to view various system information. For example, they can view statistics on unacknowledged alarms and devices in communication failure.

If the creator of the Widget Desktop layout has made the Statistics Block widget configurable, monitors can also click this icon  in the widget's upper left corner to specify which of the following are displayed in the widget:

- **Local Time:** The current Network Controller time.
- **System Uptime:** How long the system has been powered up.
- **User:** The current monitor's user name.
- **Logged In:** The time the current monitor logged in.
- **Unacknowledged Alarms:** How many of the active alarms are unacknowledged. For example, 1/5 means that one out of five alarms requires acknowledgement; the rest go away automatically when the underlying condition is fixed.
- **Devices in Communication Failure:** How many of the configured devices are currently in communication failure. For example, 2/9 means that two out of nine devices are in communication failure.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)


[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Status Widget

When the Status widget is displayed on the Widget Desktop, monitors can use it to view the status of all configured nodes and system resources. This information is presented in an expandable, hierarchical format.

Within the hierarchy, the icons displayed for a given resource and its node change depending on the current status of the resource. For example, when a blade needs attention, its icon and the icon for its node change from green balls to yellow triangles. If the blade fails, both icons change to red triangles.

If the creator of the Widget Desktop layout has made the Status widget configurable, monitors can click this icon  in the widget's upper left corner to specify the style it uses to display status information. The available **Style** settings are:

- **Node | Portal/Alarm Panel/Elevator | Resources:** With this setting, the widget display is based on each node's logical resources, such as its portals and their configured resources.
- **Node | Blade | Resources:** With this setting, the widget display is based on each node's physical resources, such its blades and their configured resources.

See also: [Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

The Threat Level Widget

The Threat Level widget is displayed on the Monitoring Desktop and in the default Widget Desktop layout. Monitors can use the widget to view the current threat level for the default location in the active partition. Administrators can also use the widget to change the threat level for any or all locations in the active partition.

In a Widget Desktop layout that includes the Threat Level widget, the information it displays depends on how it was configured for that layout. The widget might show the current threat level for:

- The default location in the active partition
- The default location and all of its sub-locations in the active partition
- The default location in selected partitions
- The default location and all of its sub-locations in selected partitions.

To use the Threat Level widget to change the current threat level:



1. Open the **Monitoring Desktop** or **Widget Desktop**.
2. In the **Threat Level** widget, click the button for the location whose threat level you want to change.
The Set Threat Level dialog box appears.
3. If a password is required to change the current threat level, enter it in the **Password** text box.
4. Select the threat level you want to apply.
5. Make sure the correct location is selected in the **Applies to location** drop-down list.
6. To apply the change to all sub-locations of the selected location, select the **Also apply to sublocations** check box.

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

7. Click **OK**.

In the Threat Level widget, the buttons for all affected locations change to reflect their new threat level.

To configure the Threat Level widget for a Widget Desktop layout:

1. Select **Configuration : Widget Desktops : Compose**.
2. In the **Load Layout** dialog box, select the layout you want to configure.
3. Click this icon  in the upper left corner of the **Threat Level** widget.
4. In the Properties dialog box, select the check box for any of the [common widget properties](#) you want the widget to have. If you want users to be able to configure the widget, be sure to select the **Configurable** check box.
5. To allow users to view threat level information for multiple partitions, select the **Allow multiple partition viewing** check box.
6. Click **OK**.
7. Click this icon  in the upper left corner of the widget.
8. If you want the widget to display threat level information for multiple partitions, select the **Show multiple partitions** check box.
9. In the Partition filter that appears below the check box, move the partitions you want the widget to display from the Available list to the Selected list.
10. To have the widget display all sub-locations of the selected partitions, select the **Show Locations** check box.
11. Click **OK**.

TIP: To see the way the widget will look when viewed in the current layout, click **Desktop** in the lower left corner of the Widget Desktop and click **Preview** to switch to Preview mode. To return to Compose mode, click **End Preview**.

See also: [Setting Threat Levels](#)

[Composing Widget Desktop Layouts](#)

[Using the Widget Desktop](#)

[Summary of the Available Widgets](#)

[About Widget Properties](#)

[Setting Up Partitions](#)

[Setting Up Locations](#)

How Groups are Used in the System

Various resource groups can be created in the security management system. Each is used for one or both of the following purposes:

- **Functional** - affects the functionality of group members and/or other resources to which it is assigned.
- **Permissions** - included in user roles to give users access to group members.

Group	Operations	Role-Based Permissions
Alarm Filter group	The group's filters can be used to determine which alarms individual users see in the Alarm Workflow widget.	-
Camera group	The group's cameras can be displayed on the NetVR Forensic Desktop.	Users can monitor cameras in the group and may be able to: <ul style="list-style-type: none"> • Select available presets. • Display and use PTZ controls. • Add, remove, and edit presets. • Work with the cameras on the Forensic Desktop.
Elevator group	-	Users can monitor elevators in the group and may be able to: <ul style="list-style-type: none"> • Enable momentary free access for floor-select buttons. • Schedule extended free-access periods for floor-select buttons.
Email distribution group	The group's email addresses can be used to: <ul style="list-style-type: none"> • Distribute scheduled custom reports. • Notify people when person records, credentials, and access levels expire. 	-
Event group	-	Users can monitor events in the group and may be able to: <ul style="list-style-type: none"> • Acknowledge alarms. • Clear event actions.
Floor group	The group's floors can be: <ul style="list-style-type: none"> • Made freely accessible for a specific period of time via the group's Free-access time spec. • Secured via access levels. 	-
Floorplan group	-	Users can monitor floorplans in the group.
Input group	The group's inputs can be armed and disarmed via event actions.	-

Magic Monitor group	The group's Magic Monitors can receive a request to display a NetVR camera stream or a Magic View that has been pushed to the group by an event action.	-
Output group	The group's outputs can be: <ul style="list-style-type: none"> Activated for a specific period of time via the group's Auto-activate time spec. Pulsed automatically by event actions. 	-
Portal group	The group's portals can be: <ul style="list-style-type: none"> Locked and unlocked automatically. Made to enter and exit panic mode (online remote locksets only). 	Users can monitor portals in the group and may be able to: <ul style="list-style-type: none"> Unlock and lock portals. Disable portals.
Reader group	The group's readers can be used to: <ul style="list-style-type: none"> Grant or deny access to cardholders based on their access levels. Disarm an alarm panel upon valid credential reads, or always deny access when the alarm panel is armed. <p>NOTE: The group can be used to bulk change the Facility Code Mode of Mercury readers/keypads.</p>	Users can view recent access requests (with ID photos) made at readers in the group.
Report group	-	Users can run reports in the group and may be able to edit them.
Threat level group	The group's threat levels can be used to determine the conditions under which: <ul style="list-style-type: none"> An action defined for an event will be performed. A portal in Double Card Presentation mode will honor double reads. A portal's scheduled unlocks will apply. Floors in a floor group will be freely accessible. Inputs in an input group will be armed. Outputs in an output group will be energized. Portals in a portal group will lock or unlock based on their locations. Readers in a specific location will grant or 	-

	<p>deny access to cardholders based on their access levels.</p> <ul style="list-style-type: none"> • Users with a specific role will be able to log into the system. 	
<p>Time spec group</p>	<p>The group's time specs can be used to specify:</p> <ul style="list-style-type: none"> • An automatic arming period for an alarm panel. • An automatic activation period for outputs in an output group. • An automatic arming period for inputs in an input group. • An automatic unlock period for portals in a portal group. • A free access period for floors in a floor group. • Valid access times for cardholders based on their access levels. • Valid times for Double Card Presentation mode to be enabled for a portal. 	<p>-</p>
<p>Widget Desktop group</p>	<p>-</p>	<p>Users can monitor layouts in the group and select them as peoples' default layouts.</p>

Index

NOTE: Some features described in help may be unavailable in certain product variants.

Access cards, *See* [Credentials](#).

[Access, changing for a person](#)

[Access History reports](#)

Access levels:

[assigning an email distribution list for notification of expiration](#)

[assigning to people](#)

[assigning escort types to](#)

[associating with floor groups](#)

[associating with threat level groups](#)

[creating](#)

[enabling Double Card Presentation mode for](#)

[granting in a partition](#)

[ACM fault event, configuring for a MicroNode Plus](#)

Actions:

[available for events](#)

[defining for events](#)

[scheduling](#)

[specifying for standard nodes](#)

[specifying for Mercury panels](#)

Activation dates, setting:

[for access levels](#)

[for person records](#)

[Activity for a person, tracing](#)

Activity Log:

[adding duty log messages](#)

[displaying device and controller times in messages](#)

[filtering log entries](#)

[Forensic Desktop](#)

[including device and controller times in messages](#)

[monitoring](#)

[navigating to a person record from](#)

[ADA setting](#) (extended unlock time)

Alarm:

[alarm status button in the page bar](#)

- [duration, reporting on](#)
- [filters, setting up](#)
- [filter groups, creating](#)
- [inputs, setting up](#)
- [outputs, setting up](#)
- [setting up events that define alarm behavior](#)

Alarm panel:

- [automatic arming](#)
- [events](#)
- [setting up](#)

[Alarm state, delaying for inputs](#)

Alarm workflow:

- [about the Alarm Workflow widget](#)
- [configuring the Alarm Workflow widget](#)
- [monitoring and resolving alarms](#)
- [policies for, creating](#)

Allegion AD-400 Lockset Modes:

- [bulk changing](#)
- [setting for individual locksets](#)
- [restrictions associated with](#)

Anti-passback:

- [gracing individual cardholders](#)
- [gracing all cardholders at a specific time](#)
- [privileges](#)
- [regional, configuring](#)

[API, enabling](#)

Apps for mobile devices:

- [Threat Level Escalator](#)
- [S2 Mobile Security Officer User Guide \(PDF\)](#)

[Appropriate use statement, adding to login page](#)

[Archive files](#)

ASSA ABLOY remote locksets:

- [about](#)
- [adding to floorplans](#)
- [adding to portal groups](#)
- [assigning to locations](#)
- [card formats for](#)
- [creating profiles for](#)
- [enabling and configuring](#)

- [entering PINs at Sx and Px locksets](#)
 - [initiating panic mode](#)
 - [issuing credentials for](#)
 - [reporting on](#)
 - [unlocking](#)
- [Audit Trail report](#)
- [Authentication](#)
 - [of API messages using SHA](#)
 - [of user login passwords using LDAP](#)
- [Auto-arming of inputs](#)
- [Auto-fill of ID# field in person records, configuring](#)
- [Auto-incrementing of encoded credential numbers, enabling](#)
- [Automatic data operations](#)
- [Avigilon NVR:](#)
 - [configuring](#)
 - [Avigilon NVR Integration Guide \(PDF\)](#)
- [Backups:](#)
 - [backing up system data](#)
 - [FTP backup settings](#)
 - [network storage location, setting](#)
 - [restoring system data](#)
- [Badges, *See* \[Photo ID badges\]\(#\).](#)
- [Banner, adding to login page](#)
- [Binary-Coded Decimal \(BCD\) credential format, defining](#)
- [Bit burst keypads, setting up](#)
- [Burglar panels, setting up](#)
- [Camera monitor, defining default](#)
- [Camera streams, pushing to Magic Monitors](#)
- [Camera View widgets:](#)
 - [configuring](#)
 - [setting unique properties for](#)
- [Cameras:](#)
 - [configuration options](#)
 - [controls for](#)
 - [camera groups, creating](#)
 - [monitoring multi-camera views](#)
 - [presets, creating](#)
- [Cards, *See* \[Credentials\]\(#\).](#)
- [Category filters, using in the Activity Log](#)

Cases:

[video](#)[Case Inspector](#)[composing](#)

Cisco VSM integrations

[configuring](#)[Cisco Video Surveillance Manager Setup and Integration Guide \(PDF\)](#)[Clock widget](#)

Cloning:

[Events](#)[ASSA ABLOY remote lockset profiles](#)

Command buttons:

[for Network Nodes](#)[for Mercury panels](#)[Command palette](#)[Command mode, for keypads](#)

Compose mode in the Widget Desktop:

[creating and editing layouts](#)[switching to when in Monitor mode](#)[Configuring disk usage](#)

Controls on the page bar

[top-level navigation controls](#)[command palette control](#)

Controller

[setting up](#)[setting up an email server for](#)[Copy to clipboard button, enabling in Mozilla Firefox](#)[Credential Audit report](#)

Credentials:

[assigning an email distribution list for notification of expiration](#)[automatic expiration of](#)[creating profiles for](#)[customizing status settings for](#)[decoding](#)[disabling after "n" days of non-use](#)[disabling after failed accesses](#)[enabling auto-incrementing of encoded numbers](#)[formats, enabling and disabling](#)[formats, specifying](#)

- [format examples](#)
- [issuing, revoking, and disabling](#)
- [lost, handling](#)
- [maximum number of active cards per person, specifying](#)
- [PIN-only, issuing for use with ASSA ABLOY remote locksets](#)
- [scanning to search for person records](#)
- [specifying remote lockset user types for](#)
- [temporary, handling](#)
- [temporary, policy for](#)
- [Cross-partition person searches](#)
- [CSV Export report, automatically generating nightly](#)
- [Custom BCD credential formats, defining](#)
- [Custom History reports, using totals in](#)
- [Custom menus, creating](#)
- [Customizing credential attributes](#)
- [Data filtering, configuring for a widget](#)
- [Data exchange using API](#)
- Data Operations
 - [Data Operations Guide \(PDF\)](#)
 - [export files](#)
 - [import files](#)
 - [overview](#)
 - [results](#)
- [Date and time, setting for the Network Controller](#)
- [Daylight Saving Time](#)
- [Decoding a card format](#)
- [Defaults, factory](#)
- [Delaying the Alarm state for inputs](#)
- Digital Monitoring Products (DMP) intrusion panels:
 - [configuring](#)
 - [monitoring from the Widget Desktop](#)
- [Directory Services](#)
- Disabling
 - [access cards](#)
 - [credential formats](#)
 - [credentials after "n" days of non-use](#)
 - [credentials after failed access](#)
- [Disk usage](#)
- [Domain Name Server \(DNS\), setting up](#)

Doors:

[portal setup](#)[unlocking](#)

Double Card Presentation Mode:

[about](#)[enabling for access levels](#)[enabling for portals](#)[DSM inputs, assigning to portals](#)[Disabling access cards](#)[Distribution groups, for email](#)[Duration of alarms, reporting on](#)

Duress:

[access, using to activate events](#)[PINS, enabling for a partition](#)

Duty log messages:

[adding to the Activity Log](#)[Generating Duty Log reports](#)[preset, configuring](#)[Electronic locksets, integrating](#)

Elevators:

[access control overview](#)[defining](#)[grouping](#)[managing access using the Elevator Status widget](#)[managing access using the Scheduled Actions page](#)[naming floors](#)[reporting on access](#)[reporting on configuration](#)[scheduling actions for floors](#)[Wiring Elevator Controls \(PDF\)](#)

Email:

[distribution groups, managing](#)[server, setting up for the controller](#)[emergency call button, configuring for an elevator](#)

Enabling

[credential formats](#)[disk usage monitoring](#)[disk usage remediation](#)[expiration notification](#)

[standard nodes](#)

[Encoded credential numbers, auto-incrementing](#)

[Encrypted connections, using for outgoing email from the controller](#)

[End User License Agreement](#)

[Enrolling people](#)

[Escalation of alarms, creating policies for](#)

[Escort type, assigning to an access level](#)

Evacuation plans:

[creating](#)

[starting and ending](#)

[S2 Mobile Security Officer User Guide \(PDF\)](#)

Events:

[assigning to DMP intrusion panels](#)

[available actions for](#)

[configuring in a Compass™ system](#)

[Controller Failed Login event, configuring](#)

[defining actions for](#)

[duration](#)

[event groups](#)

[notification](#)

[setting up](#)

[using to set the threat level](#)

exacqVision NVR:

[configuring](#)

[exacqVision \(v5.10 and 6.0\) NVR Integration Guide \(PDF\)](#)

[exacqVision \(v4.5\) NVR Integration Guide \(PDF\)](#)

[exacqVision \(v3.6\) NVR Integration Guide \(PDF\)](#)

Exempting users:

[from credential non-use rules](#)

[from PIN entry at portals with keypads](#)

[Exempt from PIN attribute, setting in a person record](#)

Expiration dates, setting:

[for access levels](#)

[for credentials](#)

[for person records](#)

[for temporary credentials](#)

[Expiration notification, enabling](#)

[Explorer widget](#)

[Export files, creating](#)

[Extended unlock](#)

Facility Code Mode for Mercury readers/keypads:

[setting for individual readers/keypads](#)

[setting for multiple readers/keypads at once](#)

[Factory defaults, resetting](#)

Failed login attempts:

[limiting via login throttling](#)

[using to activate events](#)

Filtering:

[Activity Log entries](#)

[alarms](#)

[configuring for a widget](#)

[portals on Portal Status page](#)

[FIPS 201 card formats](#)

First-in unlock rule:

[Creating](#)

[Using the First-in Unlock System Rule \(PDF\)](#)

Floors:

[creating names for](#)

[elevator buttons for, configuring](#)

[grouping](#)

[managing access using the Elevator Status widget](#)

[managing access using the Scheduled Actions page](#)

Floorplans:

[composing](#)

[creating floorplan groups](#)

[monitoring](#)

[Floor maps, configuring for a Compass™ integration](#)

Forensic cases:

[composing](#)

[exporting](#)

[printing](#)

[saving](#)

Forensic Desktop:

[camera inspector](#)

[Case Inspector](#)

[searching](#)

[thumbnails](#)

[using](#)

[video tutorials](#)

Free access, enabling

[for elevator floor-select buttons](#)

[for floors in an elevator floor group](#)

[FTP backup settings](#)

[Gateway, for Network Controller](#)

[Grace, passback](#)

[granting user roles and access levels in a partition](#)

[Grid, displaying in Widget Desktop layouts](#)

[groups, use in the system](#)

grouping:

[alarm filters](#)

[cameras](#)

[elevators](#)

[events](#)

[floors](#)

[floorplans](#)

[inputs](#)

[outputs](#)

[portals](#)

[readers](#)

[reports](#)

[time specs](#)

[Widget Desktop layouts](#)

High Availability (HA) implementation:

[Avance IP address for HA server pair](#)

[monitoring HA status](#)

[High limit disk usage threshold caution and warning](#)

Holidays:

[creating](#)

[configuring partial-day holidays for Mercury panels](#)

Home page

[default Home page](#)

[setting a different Home page](#)

Honeywell:

[card format](#)

[configuring PW-Series access control hardware](#)

[Integrating Mercury-Powered Honeywell Access Control Hardware \(PDF\)](#)

[ID numbers, managing in person records](#)

[ID photos, including in Custom People reports](#)

Images:

[setting photo ID size limit](#)[uploading ID photos](#)

Import files, Data Operations

[adding to NAS storage location](#)[editing and deleting](#)[uploading](#)[Incrementing of encoded credential numbers, enabling](#)

Initmode:

[Email settings](#)[Network Controller Time settings](#)[Web Server settings](#)[Initially populating the system with data records](#)

Inputs:

[creating](#)[input groups, creating](#)[scheduling actions for](#)[temperature](#)[using to monitor elevator buttons](#)[virtual, setting up for VMS cameras](#)

Installation guides and technical notes, links to

Intrusion panels:

[configuring DMP panels](#)[DMP Intrusion Panel Integration \(PDF\)](#)[monitoring DMP panels from the Widget Desktop](#)

IP addresses:

[Network Controller](#)[static, assigning to a node](#)

IP settings:

[changing for Network Nodes](#)[changing for Mercury panels](#)

JPEG:

[motion files](#)[photo ID images](#)[Keypad timed unlock feature](#)[Keypads, setting up](#)

Keypad command mode:

[about](#)

- [defining keypad commands](#)
- [Language and date format, selecting](#)
- Layouts, for the Widget Desktop:
 - [composing](#)
 - [using to monitor the system](#)
 - [grouping](#)
- [LDAP server, setting up](#)
- License agreement, end user
- License file
 - [activating](#)
 - [checking status and expiration date](#)
- Links to technical documentation
- Locations:
 - [Creating](#)
 - [Setting threat level for, using an event](#)
 - [Setting threat level for, using the Set Threat Level page](#)
 - [Setting threat level for, using the Threat Level widget](#)
 - [Using threat levels to change the level of protection for](#)
- Locksets, see [ASSA ABLOY remote locksets](#).
- [Log messages, forwarding to a remote host](#)
- [Login attempts, limiting via login throttling](#)
- [Lost credentials, handling](#)
- [Low battery events, configuring for a node](#)
- [Low limit disk usage threshold caution and warning](#)
- Magic Monitors
 - [configuring](#)
 - [creating Magic Monitor groups](#)
 - [event actions for](#)
- Magnetic stripe:
 - [card format](#)
 - [photo IDs, printing](#)
- [Master \(default\) partition](#)
- [menus, custom](#)
- Mercury hardware:
 - [configuring Mercury panels](#)
 - [configuring resources for Mercury SIOs](#)
 - [bulk changing the Facility Code Mode for reader/keypads](#)
 - [Integrating Mercury EP-Series Access Control Hardware \(PDF\)](#)
 - [Integrating Mercury M5 Bridge Access Control Hardware \(PDF\)](#)

[Integrating Mercury-Powered Honeywell Access Control Hardware \(PDF\)](#)

[Integrating Mercury-Powered Allegion Schlage Wireless Devices \(PDF\)](#)

[special requirements for configuring Mercury M5 Bridge Panels](#)

[special requirements for configuring Schlage wireless devices](#)

[Wiring Elevator Controls \(PDF\)](#)

[Maximum number of active cards per person](#)

[MicroNode Installation Guide \(PDF\)](#)

[MicroNode Plus Installation Guide \(PDF\)](#)

Milestone Systems NVR:

[configuring](#)

[Milestone XProtect Enterprise/Professional 2014 \(8.6d\) NVR Integration Guide \(PDF\)](#) (Release 4.7)

[Milestone XProtect Enterprise/Professional \(v7.0b/c/d, 8.0/8.1a\) NVR Integration Guide \(PDF\)](#)
(Release 4.5)

[Milestone XProtect Enterprise/Professional \(v7.0b/c/d, 8.0\) NVR Integration Guide \(PDF\)](#) (up to
Release 4.4)

[Milestone XProtect Corporate 2014 \(v7.0c/d\) NVR Integration Guide](#) (Release 4.8)

[Milestone XProtect Corporate \(v3.1a/4.0a/4.1a/5.0a\) NVR Integration Guide \(PDF\)](#) (Release 4.5)

[Milestone XProtect Corporate \(v3.1a/4.0a/4.1a/5.0a\) NVR Integration Guide](#) (up to Release 4.4)

[Milestone Systems \(v6.5\) NVR Integration Guide \(PDF\)](#)

[Missing credentials, handling](#)

[Mobile device, setting up the Threat Level Escalator App](#)

Mobile evacuation management:

[starting and ending evacuation plans](#)

[S2 Mobile Security Officer User Guide \(PDF\)](#)

[Momentary portal unlock](#)

Monitoring the system:

[disk usage](#)

[from the Home page](#)

[HA status](#)

[Monitor menu](#)

[from the Monitoring Desktop](#)

[from the Widget Desktop](#)

[Motion JPEG](#)

Mustering

[during an evacuation](#)

[S2 Mobile Security Officer User Guide \(PDF\)](#)

NAS storage for Data Operations

[adding import files](#)

[setting up](#)

[Navigation bar](#)

NetVR:

- [cameras](#)
- [camera views](#)
- [configuring](#)
- [Forensic Desktop](#)
- [searching video](#)
- [Web Service, configuring \(PDF\)](#)

Network settings:

- [changing for standard Nodes](#)
- [changing for Mercury panels](#)

[Network storage location, setting up](#)[Netmask, for Network Controller](#)[Nightly CSV Export reports, generating](#)

Network Node Configuration utility (nnconfig.exe):

- [Connecting Nodes and Controllers Across Subnets \(PDF\)](#)
- [downloading](#)

Nodes:

- configuring standard nodes
- [configuring Mercury panels](#)
- [configuring in an Otis Compass system](#)
- [configuring ASSA ABLOY remote locksets](#)
- [new, moving to a named partition](#)
- [refreshing](#)
- [viewing current status](#)

[Node time, including in Activity Log messages](#)[Notifications, defining for events](#)[Notification on expiration](#)

NVR integrations:

- setup guides, links to
- [updating](#)

[Occupancy violation](#)[Online and offline remote locksets, defined](#)

OnSSI NVR:

- [configuring](#)
- [OnSSI Ocularis CS/IS \(2.0\) NVR Integration Guide \(PDF\)](#) (Release 4.4)
- [OnSSI Ocularis CS/IS \(2.0\) NVR Integration Guide \(PDF\)](#) (up to Release 4.3)
- [OnSSI NetDVMS \(6.5\) NVR Integration Guide](#) (Release 4.4)
- [OnSSI NetDVMS \(6.5\) NVR Integration Guide \(PDF\)](#) (up to Release 4.3)

[OTIS Elevator Compass™ integration, configuring](#)

Outputs:

- [creating](#)
- [associated with a DMP intrusion panel](#)
- [output groups, creating](#)
- [pulsing](#)
- [scheduling actions for](#)
- [using to control elevator buttons](#)

Palettes

- [command palette](#)
- [navigation palette](#)

Panels, intrusion:

- [configuring](#)
- monitoring from the Widget Desktop

Panic mode for ASSA ABLOY remote locksets:

- [described](#)
- [initiating](#)

Partitions:

- [creating](#)
- [granting limited access to person records in](#)
- [granting user roles and access levels in](#)
- [making all person records visible in](#)
- [making visible to all administrators in other partitions](#)
- [moving new nodes to](#)
- [moving video management systems to](#)
- [overview of setup](#)
- [searching for people across](#)
- [selecting](#)
- [viewing multiple in widgets](#)
- [viewing status of the nodes in](#)

Page bar:

- [about](#)
- [command palette, opening from](#)
- [navigation pane, opening from](#)

Passback grace:

- [granting to individual cardholders](#)
- [granting to all cardholders at a specific time each day](#)

[Passback Grace widget](#)[Passback violations](#)

Passwords:

- [changing](#)
- [setting strength requirements for system users](#)
- [using LDAP directory services to authenticate](#)

[People search](#)[Permissions](#)

Person records:

- [accessing recorded video from](#)
- [assigning access levels](#)
- [assigning credentials](#)
- [assigning email distribution lists for notification of expiration](#)
- [creating templates for](#)
- [editing](#)
- [configuring the display of](#)
- [initially populating system with data records](#)
- [managing person data in](#)
- [navigating to from an Activity Log entry](#)
- [making all records visible in all partitions](#)
- [searching for](#)

[Photos, including in Custom People reports](#)

Photo ID badges:

- [batch printing photo IDs](#)
- [capturing and saving digital signatures](#)
- [capturing and saving ID photos](#)
- [deleting photo ID layouts](#)
- [Photo ID Requests report](#)
- [printing photo IDs](#)
- [system data for photo ID layouts](#)
- [uploading photo ID layouts](#)

[Photo ID History widget](#)

PINs:

- [assigning](#)
- [duress PINs, enabling for a partition](#)
- [entering at ASSA ABLOY Sx and Px locksets](#)
- [for keypads](#)

[PIN-only credentials, issuing for use with ASSA ABLOY remote locksets](#)

Policies:

- [for alarm workflow](#)
- [for portals](#)

[for temporary credentials](#)

Portal unlocks:

[from a floorplan](#)

[from the Monitoring Desktop](#)

[from the Portal Status page](#)

[from the Widget Desktop](#)

[using a portal group unlock time spec](#)

[using an event action](#)

[using threat level changes](#)

Portals:

[adding to a portal group](#)

[assigning to a location](#)

[creating](#)

[enabling Double Card Presentation mode](#)

[enabling Keypad timed unlock feature](#)

[requiring two valid card reads for access](#)

[scheduling actions for](#)

[unlock behavior](#)

[using threat levels to change behavior](#)

[unlocking and viewing current state](#)

[Portal Status and Portal Unlock widgets](#)

[Power off](#)

Precision administration:

[granting access to person records in the active partition](#)

[making the active partition's name visible in other partitions](#)

[Previewing changes to a widget's scope properties](#)

Printing:

[help topics](#)

[Photo IDs](#)

[Photo IDs in batches](#)

Profiles:

[creating for credentials](#)

[creating for ASSA ABLOY remote locksets](#)

[Pulsing outputs and output groups](#)

[Pushing camera streams and Magic Views to Magic Monitors](#)

Readers:

[creating](#)

[enrollment, for issuing access cards](#)

[setting up](#)

- [reader groups](#)
- [Refreshing nodes](#)
- [Regional anti-passback, configuring](#)
- Regional evacuations:
 - [creating plans for](#)
 - [starting and ending](#)
 - [S2 Mobile Security Officer User Guide \(PDF\)](#)
- [Remote logging, setting up](#)
- Reports:
 - [adding to report groups](#)
 - [CSV Export reports, generating nightly](#)
 - [Custom People reports](#)
 - [Custom History reports](#)
 - [Configuration reports](#)
 - [History reports](#)
 - [People reports](#)
 - [Using totals in](#)
- [Resetting factory defaults](#)
- [Resetting failed accesses non a valid access](#)
- [Resistor configurations for inputs](#)
- [Resolution of alarms, reporting on](#)
- [Resources, scheduling actions for](#)
- [Resource groups, how they are used in the system](#)
- [Restoring the system data](#)
- [REX behavior, defining for a portal](#)
- [Roles, default](#)
- [Rsyslog messages, forwarding to a remote host](#)
- [Rules for changing system behavior, creating](#)
- S2 node types
- Salient Systems CompleteView NVR:
 - [configuring](#)
 - [Salient Systems NVR Integration Guide \(PDF\)](#)
- Scheduled actions:
 - [for extended portal unlocks](#)
 - [for resources and resource groups](#)
 - [reporting on changes to](#)
- Schlage wireless devices:
 - [bulk changing the Allegion AD-400 Lockset Mode for AD-400 locksets](#)
 - [Integrating Mercury-Powered Allegion Schlage Wireless Devices \(PDF\)](#)

[special considerations for configuring](#)

Scope properties of widgets:

[Changing for a monitoring session](#)

[Configuring for a Widget Desktop layout](#)

[ScratchPad](#)

[Search Clock](#)

[Searching for person records](#)

[Secondary output, selecting for a portal](#)

Secure

[FTP transfers, configuring](#)

[LDAP traffic, configuring](#)

[Securing a portal](#)

[Setting the Network Controller time](#)

[Set IP address settings](#)

Setup guides, links to

[SHA authentication for API](#)

[Shunt time](#)

[Signatures](#)

[SIOs, configuring for a Mercury panel](#)

[SMTP login password, setting for the email server](#)

[Snap to Grid feature in Widget Desktop layouts](#)

[Software, updating](#)

[Software license, activating](#)

Sound file:

[uploading](#)

[selecting for event notification](#)

[SSH protocol, using to secure FTP transfers](#)

SSL certificates

[configuring](#)

[SSL connections, using for outgoing email from the controller](#)

[State of a portal, viewing](#)

[Statistics Block widget](#)

[Status settings for credentials, customizing](#)

[Status widget](#)

[Storage management](#)

[Summer \(Daylight Saving\) Time](#)

[Supervised inputs](#)

SUSP License file

[activating](#)

- [checking status and expiration date](#)
- [System health, managing](#)
- [System messages, forwarding to a remote host](#)
- System rules:
 - [Creating](#)
 - [Using the First-in Unlock System Rule \(PDF\)](#)
- [Tabs, hiding and showing in person records](#)
- [Tailgate violations](#)
- [Tamper event, enabling for an Extreme system](#)
- [Tamper event, specifying for a node](#)
- Technical documentation, links to
- Temperature:
 - [inputs, setting up](#)
 - [scale, setting for temperature inputs](#)
- Temporary
 - [access levels, assigning](#)
 - [credentials, automatic expiration of](#)
 - [credentials, managing](#)
 - [credentials, creating a policy for](#)
- [Templates, creating for person records](#)
- [Text filter, previewing for a widget](#)
- [Text filtering, enabling on the Monitoring Desktop](#)
- Threat levels:
 - [adding, changing, and deleting](#)
 - [configuring settings for](#)
 - [selecting for portal policies](#)
 - [setting the menu order for](#)
 - [setting, using the Set Threat Level page](#)
 - [setting, using the Threat Level widget](#)
 - [setting, using an event](#)
 - [Threat level App, setting up on a mobile device](#)
 - [threat level groups, creating](#)
 - [using to change system behavior](#)
- [Throttling login attempts](#)
- [Timeline](#)
- [Time server, network](#)
- Time specs:
 - [about](#)
 - [creating](#)

[automatic activation](#)

[automatic arming](#)

[free-access](#)

[specifying local or system time spec for scheduled unlocks](#)

[time spec groups, creating](#)

[unlock](#)

[Timed anti-passback](#)

[Timed unlock feature for portals](#)

[Time zone, setting](#)

Top-level controls on the page bar

[navigation controls](#)

[command palette control](#)

[Totals, using in Custom History reports](#)

[Tracing a person's activity](#)

[Turnstile portal type, configuring](#)

[Tutorials, video](#)

[Two-man entry restriction, specifying for portals](#)

[Unique ID numbers, enforcing in person records](#)

Unlocking portals:

[from a floorplan](#)

[from the Monitoring Desktop](#)

[from the Portal Status page](#)

[from the Widget Desktop](#)

[using a portal group unlock time spec](#)

[using an event action](#)

[using threat level changes](#)

Updating

[an NVR or DVR integration](#)

[the software](#)

[your person records](#)

[Uploading Data Operations import files](#)

[Users, adding to the system](#)

User-defined fields (UDFs)

[configuring](#)

[defining value lists for](#)

User roles:

[creating](#)

[default user roles](#)

[granting in a partition](#)

[User tasks, on the Home page](#)

[Video Accelerator](#)

Video Insight NVR:

[configuring](#)

[Video Insight NVR Integration Guide \(PDF\)](#)

Video, recorded:

[cases](#)

[clips](#)

[exporting](#)

[printing](#)

[searching](#)

[viewing from a person record](#)

Video management systems:

[a NetVR appliance, configuring](#)

[Avigilon NVR, configuring](#)

[Avigilon NVR Integration Guide \(PDF\)](#)

[Cisco VSM, configuring](#)

[Cisco Video Surveillance Manager Setup and Integration Guide \(PDF\)](#)

[exacqVision NVR, configuring](#)

[exacqVision \(v5.10 and 6.0\) NVR Integration Guide \(PDF\)](#)

[exacqVision \(v4.5\) NVR Integration Guide \(PDF\)](#)

[exacqVision \(v3.6\) NVR Integration Guide \(PDF\)](#)

[Milestone NVR, configuring](#)

[Milestone XProtect Enterprise/Professional 2014 \(8.6d\) NVR Integration Guide \(PDF\)](#) (Release 4.7)

[Milestone XProtect Enterprise/Professional \(v7.0b/c/d, 8.0/8.1a\) NVR Integration Guide \(PDF\)](#) (Release 4.5)

[Milestone XProtect Enterprise/Professional \(v7.0b/c/d, 8.0\) NVR Integration Guide \(PDF\)](#) (up to Release 4.4)

[Milestone XProtect Corporate 2014 \(v7.0c/d\) NVR Integration Guide](#) (Release 4.8)

[Milestone XProtect Corporate \(v3.1a/4.0a/4.1a/5.0a\) NVR Integration Guide \(PDF\)](#) (Release 4.5)

[Milestone XProtect Corporate \(v3.1a/4.0a/4.1a/5.0a\) NVR Integration Guide](#) (up to Release 4.4)

[Milestone Systems \(v6.5\) NVR Integration Guide \(PDF\)](#)

[moving between partitions](#)

[OnSSI NVR, configuring](#)

[OnSSI Ocularis CS/IS \(2.0\) NVR Integration Guide \(PDF\)](#) (Release 4.5)

[OnSSI Ocularis CS/IS \(2.0\) NVR Integration Guide \(PDF\)](#) (up to Release 4.4)

[OnSSI NetDVMS \(6.5\) NVR Integration Guide](#) (Release 4.4)

[OnSSI NetDVMS \(6.5\) NVR Integration Guide \(PDF\)](#) (up to Release 4.4)

[Salient Systems NVR, configuring](#)

[Salient Systems NVR Integration Guide \(PDF\)](#)

[ViconNet Nucleus, configuring](#)

[Video Insight NVR, configuring](#)

[Video Insight NVR Integration Guide \(PDF\)](#)

[video tutorials, playing](#)

[Views, pushing to Magic Monitors](#)

[Viewing disk usage information](#)

[Viewing import file text, errors, and results](#)

[violations, passback and tailgate](#)

[virtual inputs, setting up for VMS cameras](#)

[Web server settings](#)

Widget Desktop:

[available widgets](#)

[composing layouts for](#)

[switching between Monitor and Compose modes](#)

[using to monitor the system](#)

[Wiegand format](#)

[Wi-Fi enabled ASSA ABLOY remote locksets, integrating](#)

[Wiring Elevator Controls \(PDF\)](#)