

Technical Document

Niagara Enterprise Security Facility Manager's Guide

March 17, 2025



Contents

About this guide	7
Document change log	7
Related documentation	7
Chapter 1. Getting Started	9
Logging in to the system	9
Changing passwords	9
Logging out of the system	10
Browser controls	10
User interface	11
Title bar controls	12
About the view pane	14
Controller (System) Setup menu	16
NAC Network Setup Menu	16
Add NAC Controller Manually	17
Add Controller using Discover	18
Setup the NAC Network	19
Upload NAC Firmware files	19
Discover, Learn, Add, and Match	20
Discovery control buttons	21
About table views	22
Table right-click menus	22
Sorting table data by column	23
Adding columns to a table	24
Deleting table columns	26
Editing table column order	26
About filtering tables	26
Wild cards and filter properties	26
String filter functions	27
Filtering data in a table	28
Filtering using time	28
Exporting data to PDF or CSV	29
Quick editing common properties	30
Adding, discovering (learning), and matching	31
Adding remote modules and devices off-line	31
Discovering modules and devices	32
Adding discovered objects	33
Matching discovered objects	34
Finding a device to match	34
Configuring inputs and outputs	35
Assigning and unassigning items	35
Mapping cameras connected to a Supervisor PC	36
Mapping cameras connected to a remote controller	37

Chapter 2. Special event scheduling	39
Adding a special one-time event	41
Adding a special event by referencing a calendar schedule	41
Setting up holidays and other special events on a calendar schedule	43
Exporting a schedule to a CSV file	44
One way to discover and export schedules	44
Another way to discover and export schedules	46
Chapter 3. People management	47
Creating a new tenant	47
Editing an existing tenant	47
Creating a person record	48
Editing an existing person record	49
Combining person records	50
Creating a PIN for a person	50
Filtering personnel records by tenant	51
Assigning an access right to a person	51
Access rights limited by time range	52
Editing access right effective date and assigned threat level	52
Restricting available information by tenant	52
Managing occupants in an access zone	53
Monitoring door entries	54
Manually inserting an attendance record	56
Tracing a person's entry and exit activity	56
Displaying the person's photo on a history report	57
Easy Lobby visitor management	59
Visitor management with Sine	59
Prerequisites	60
Sine configuration	61
Configuring Sine and WebHook	61
Visitor integration in the Niagara station	64
Adding the VisitorIntegrationService	64
Setting up the Visitor Type and Access Right mapping	66
Adding Points to the VisitorIntegrationService	68
Setting up the Abstract MQTT driver network	70
Checking in a visitor	74
Checking a visitor out	78
Purge Visitors On Checkout enabled	78
Purge Visitors On Checkout disabled	79
VisitorIntegrationService - Configuration Problem Points and Failures	79
Chapter 4. Badge management	83
Creating a single badge (manual entry)	83
Creating multiple badges (batch-create)	83
Manually assigning a new badge	83
Enrolling from a reader to assign a new badge	84

Assigning an existing badge	84
Capturing a photo and associating it with a person	85
Importing a photo	87
Cropping a photo	88
Printing badges	91
Chapter 5. Threat-level management	93
Setting up threat levels	95
Adding (or editing) a threat level group	96
Assigning a remote station to a threat level group	98
Directly assigning a threat level to a person	98
Assigning access rights to threat level groups	99
Threat level response	100
Adding a threat level group to an access right	100
Directly assigning a threat level to an access right	101
Configuring a threat level on a door strike	101
Configuring a threat level for a reader	102
Activation level input	103
Activation level output	103
Activation badge	103
Creating an activation badge	104
Assigning a threat level to an activation badge	104
Chapter 6. Reports	107
Viewing a report	108
Adding a custom report	109
Editing a custom report	110
Deleting a custom report	110
Creating an email schedule for reports	111
Assigning a schedule to a report	111
Printing a report	112
Purging history records from a remote controller	113
Purging history records from a Supervisor station	113
Opening an exported CSV file in Microsoft® Excel®	113
Chapter 7. Station save, backup and restore	115
About station save	115
Saving a station	115
Data backup	117
Backing up a local station	118
Backing up the station using station copier	121
Creating a system backup	123
Creating a backup schedule for a system backup	124
MySQL and MS SQL Database backups	126
Data restore	126
Viewing backup history	127
Restoring station(s) using the Web UI	127

Troubleshooting 128

Badge creation troubleshooting 128

About this guide

This guide is for the facility manager who is responsible for setting up operating procedures, managing tenants, and configuring options.

This document is part of the Niagara Enterprise Security technical documentation library. Released versions of software include a complete collection of technical information that is provided in both online help and PDF formats.

Document change log

The following list describes significant documentation changes.

March 17, 2025

- Updated the "Getting Started" chapter to include the "NAC Controller Setup Menu" and related topics on NAC controllers.
- Removed Assure ID references.

April 11, 2023

Updated "Visitor management with Sine" chapter.

August 4, 2022

Added "Visitor management with sine" section in People Management chapter.

January 24, 2020

Minor changes to topics in the preface.

August 8, 2019

Reorganized document and added updates related to Niagara 4.8 release.

October 9, 2018

Minor editorial updates.

September 17, 2018

Initial release for version 2.4

Related documentation

These documents provide additional system information.

- *Niagara Enterprise Security Installation and Maintenance Guide*
- *Niagara Enterprise Security Reference*
- *Niagara Enterprise Security Operator's Guide*

Chapter 1. Getting Started

This system is a comprehensive building access control solution, built on an open, IP-based platform.

System architecture provides the following:

- LAN or WAN connection using standard TCP/IP communications
- A browser interface with multiple-user access
- Support for a network of controllers whose relationships can be configured, with a single Supervisor, and the possibility for multiple peer and subordinate relationships in a hierarchy
- A network of door control modules and remote input/output modules
- Global access control functions for all devices connected on the local and network controllers
- Intrusion zones and access zones that span multiple controllers
- Global administration of access control and monitoring functions for all devices connected to the controllers
- An embedded database to store credential information, as well as event and alarm transactions

This system runs on a Java virtual machine (JVM) that supports application programs running on any platform without a program having to be rewritten or recompiled for each separate platform.

Logging in to the system

To use this system you need to connect to the station using a browser and log in using valid credentials.

Prerequisites:

Get the network address of the station that you want to log in to from your system administrator. This may be an IP address or a URL depending on how your station is configured and how, or if, it is routed to the Internet.

Step 1. From a computer that is on the system network, open a browser.

Step 2. In the browser address bar, type the IP (Internet Protocol) address of the computer (Supervisor PC) or remote controller, for example, <https://192.168.1.123/login>
The login window opens. If you are logging in to the system for the first time, the default **Username** is "admin" and the **Password** can be left blank. To ensure security, change these settings immediately on initial setup.

Step 3. Enter your **Username** and **Password** and click **Login**.
You are logged in to the system and the interface opens.

Changing passwords

You should change each password, especially the admin password, on a regular basis. The security of your system depends upon your vigilance. This procedure documents a task performed in both the Supervisor PC and remote controller stations using the system's browser interface. The alternative Supervisor station command is in parenthesis.

Prerequisites:

You are logged in to the station with admin privileges.

Step 1. Navigate to **Controller Setup (System Setup) > User Management > Change Password**.
The Users view opens.

Step 2. In the **Current Password** property, type the current password.

Step 3. In the **New Password** property, type a new strong password.

Step 4. To confirm that you typed the name correctly, type the new password again in the **Confirm New**

Password property, and click **Save**.

If the two values match, the system implements the change.

Step 5. To return to the home view, click **Home**.

Logging out of the system

Always log out and close the system interface when you are finished. Failure to log out and close the browser window could result in unauthorized use of your account.

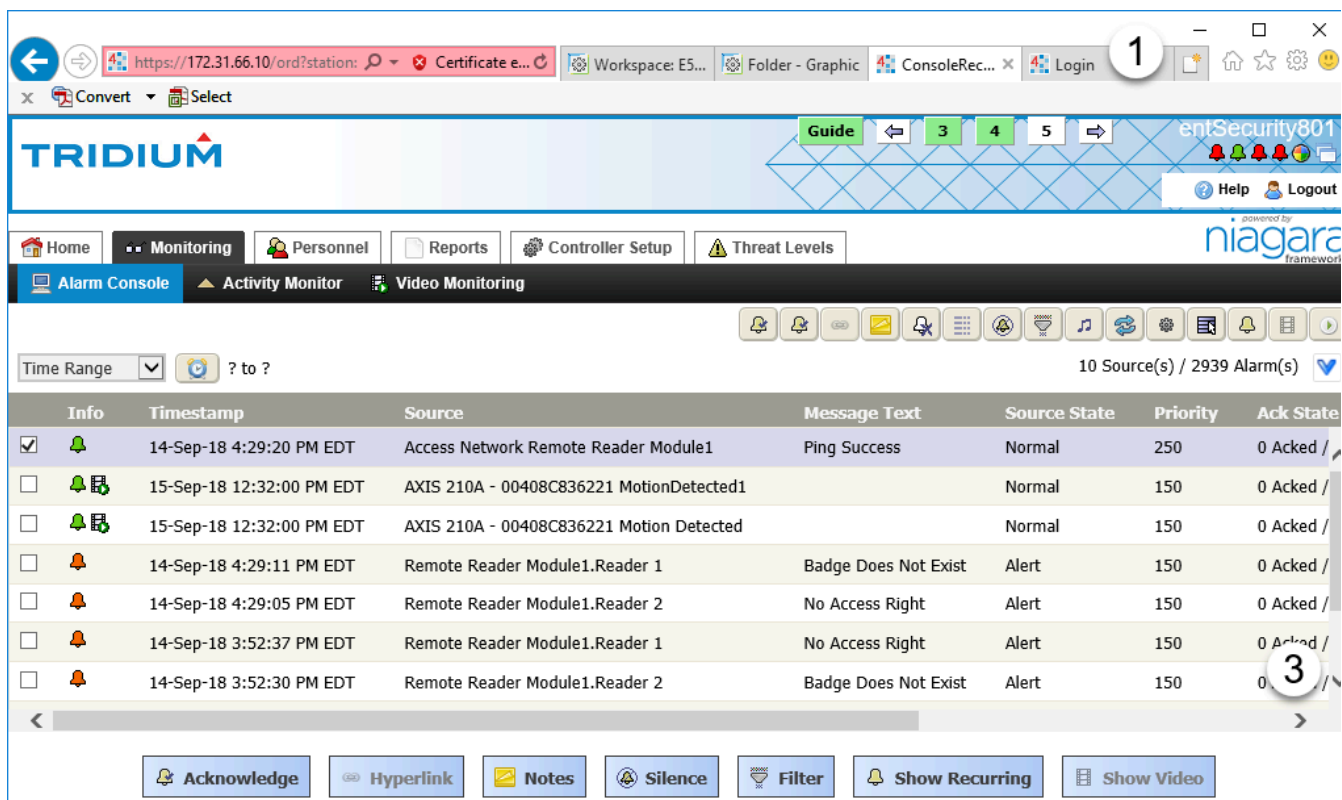
Step 1. In the system title bar, click the **Logout** button.
The system logs you out.

Step 2. To close the browser, click **File > Exit**.
The browser closes.

Browser controls

The user interface runs in a standard browser and has standard browser controls in addition to the custom window controls.

Figure 1. Browser and display controls



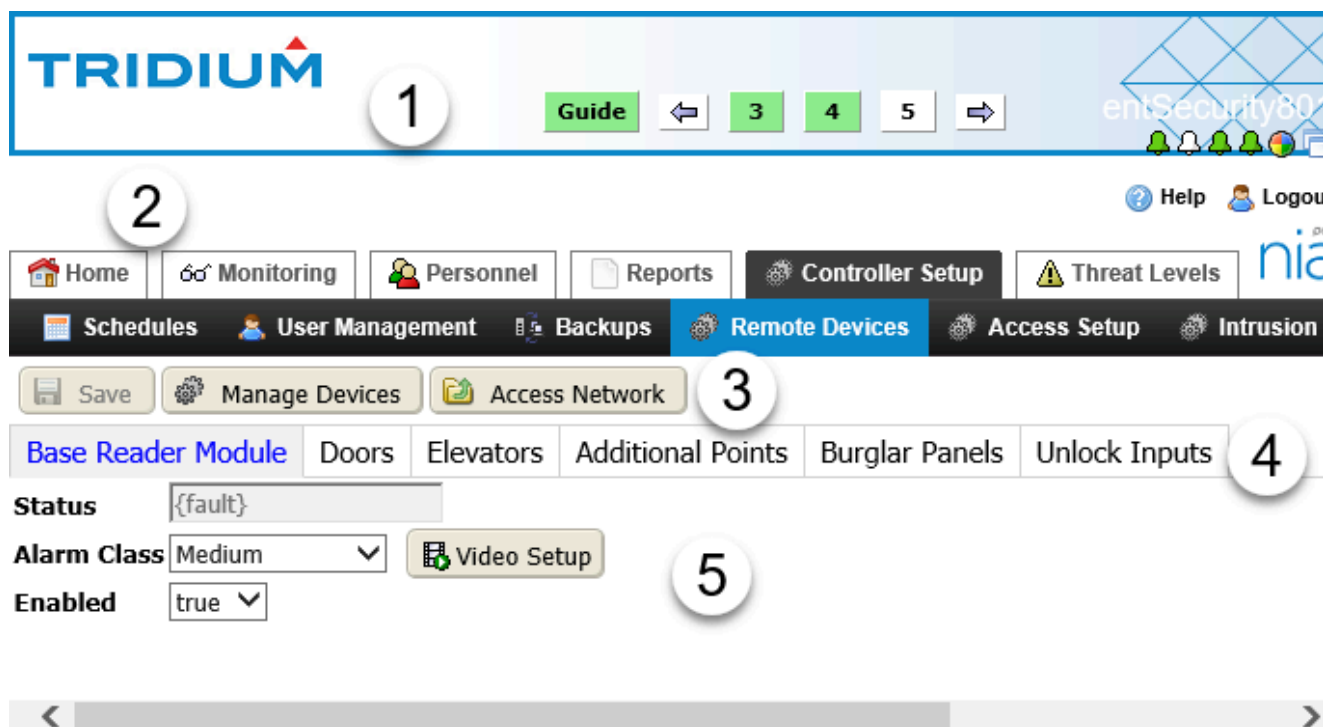
1. The browser window and controls provide standard web browser features, such as the status bar in the lower left corner of the browser.
2. Scroll bars appear in window areas when portions of content are not visible. They may be along the right or bottom portions of a window and browser area.

- Border controls allow you to drag any outside border to adjust the entire window. Drag the border between the separate panes of some view areas to change their relative sizes.

User interface

When you log in, the user interface screen displays with the main menu across the top of the screen.

Figure 2. Example user interface



- Title bar
- Menu bar
- Links
- Tabs
- View area

Title bar

This title bar area along the top part of the interface contains controls and indicators that are visible and available throughout the system:

- The station and system names are in the top right corner.
- Indicators and links are below the names.
- The Help and Logout links are always visible.

Menu bar

This bar is directly below the title bar. It contains two rows of menus that are visible by default. Some menu items, when selected, display another sub-menu view.







Menus may display different selection options depending on the user log-in type and whether or not the menu has been customized. You can customize menus to add links to new graphic views that you create.

View pane

This (largest) area of the interface extends across the lower portion of the system of the screen and displays the currently-selected view. Most views have a view title in the top left corner, control buttons and links below the control buttons. often information is grouped under appropriately-titled tabs.

Title bar controls

The indicators and links available under the station and system names are:

-  The Alarm console link opens the alarm console in the view area. The alarm icon's color reports the current alarm state. The icon flashes red when an alarm indicates a fault or offnormal state.
-  The Job Service link displays when a job has a start time of less than one hour. Clicking this icon opens the Job Service view. To open the Job Service view when no link is available, click **System (Controller) Setup > Miscellaneous > Jobs** from the main menu.
-  The Tenant Filter link opens the **Tenant Filter** window. You use this window to limit the information displayed to only data that belongs to the tenant or tenants assigned to the current user.
-  The Pop Out in New Window opens the current window in a new, full-page window.
-  **Help** The Help button opens a page context-sensitive help related to the current view. If no context-sensitive help is available, the complete Help Table of Contents open.
-  **Logout** The Logout button logs out of the system.

NOTE: Always log out and close the browser when you are finished with a session.

Menu bar

The menu bar is located directly below the title bar and contains two rows of menus that are visible by default.

Figure 3. Menu bar



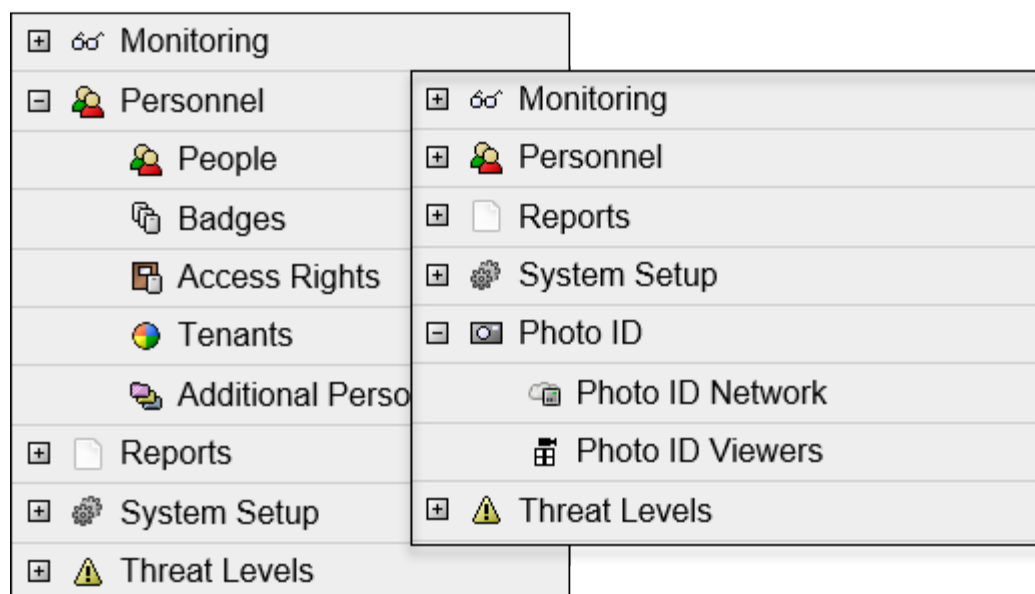
The primary menus provides a common set of tabbed menus with secondary menu tabs beneath the primary row. Additional options display as menu pages. You can customize menus (navigation) to add links to new graphic views that you create.

Secondary menus provide access directly to views or to menu pages that contain additional related links.

Some menus provide tabs. More or fewer tabs may display, depending on user type log-in privileges and navigation customization.

By default, the primary menus include the following titles:

- Home provides access to the other primary menus by displaying a main menu page and an expanding navigation menu.

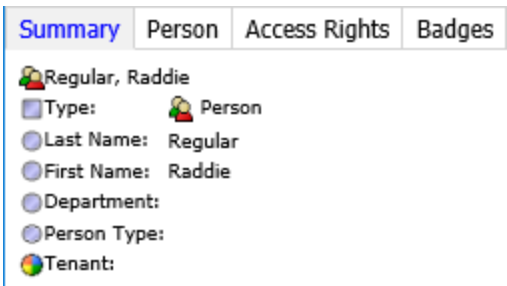
Figure 4. Home view menu with Personnel expanded

- Monitoring provides access to the **Alarm Console**, **Activity Monitor**, and **Video Monitoring** menu items.
- Personnel provides access to people-related views, such as badge, access right, tenant, and personnel views.
- Reports provides access to history reports (such as alarm history and attendance history) as well as hardware reports that list types of equipment included in the system.
- Controller Setup (System Setup in a Supervisor station) provides access to a wide variety of configuration menus that you can use to setup hardware, alarms, access and intrusion zones, and other functions.
- Threat Levels provides access to Threat Level and threat level setup views.

Tabs

The tabs segregate properties and related table views. The view pane may display one of a variety of types of layouts, depending on the function of the view.

Figure 5. People summary showing tabs.

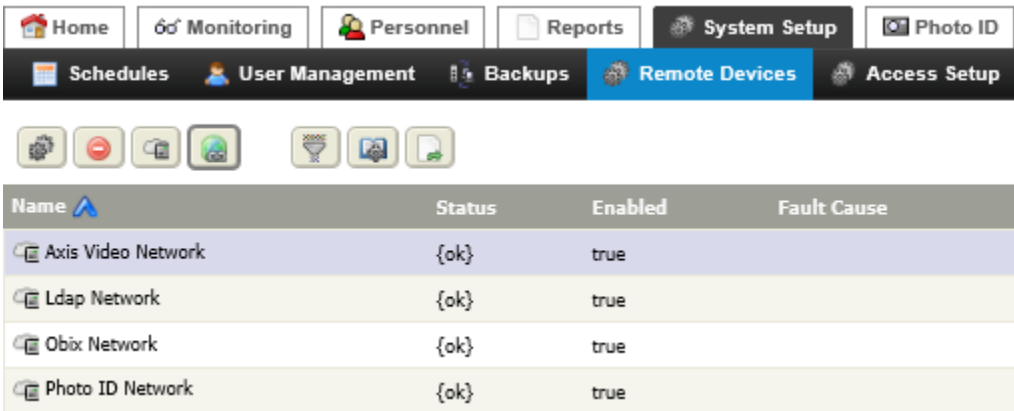


NOTE: You can move among tabs without losing unsaved data, however, you must click the button before leaving the view or data is lost.

About the view pane

The View pane is the largest area of the user interface and is located below the title bar and menu bar.

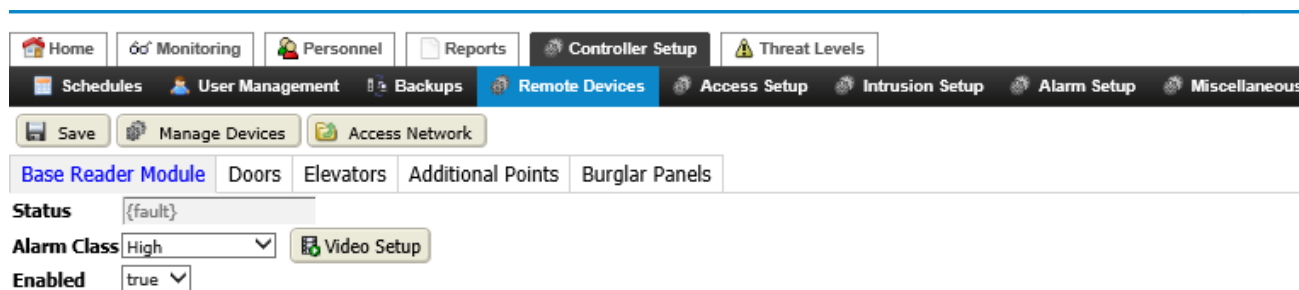
Figure 6. View pane with table view



The view pane may display one of a variety of layouts, depending on the function of the view. The following view layouts are used most often:

- Table views display information in tabular form. You can sort, filter, rename and customize them using a standard set of control buttons. Table views include reports, lists of people, hardware, access zones, access rights, and many other types of information. Several table views use the learn mode to add or assign information to the currently listed table. Many table views also have a *Auto Refresh* option that, when clicked, refreshes the table data.

NOTE: If a table requires more than 5,000 lines, a message alerts you that only the first 5,000 records are available for viewing. To view all relevant data, filter the table so that its maximum display value does not exceed 5,000 lines.
- Edit views display properties and option lists that you use to create and configure selected items.

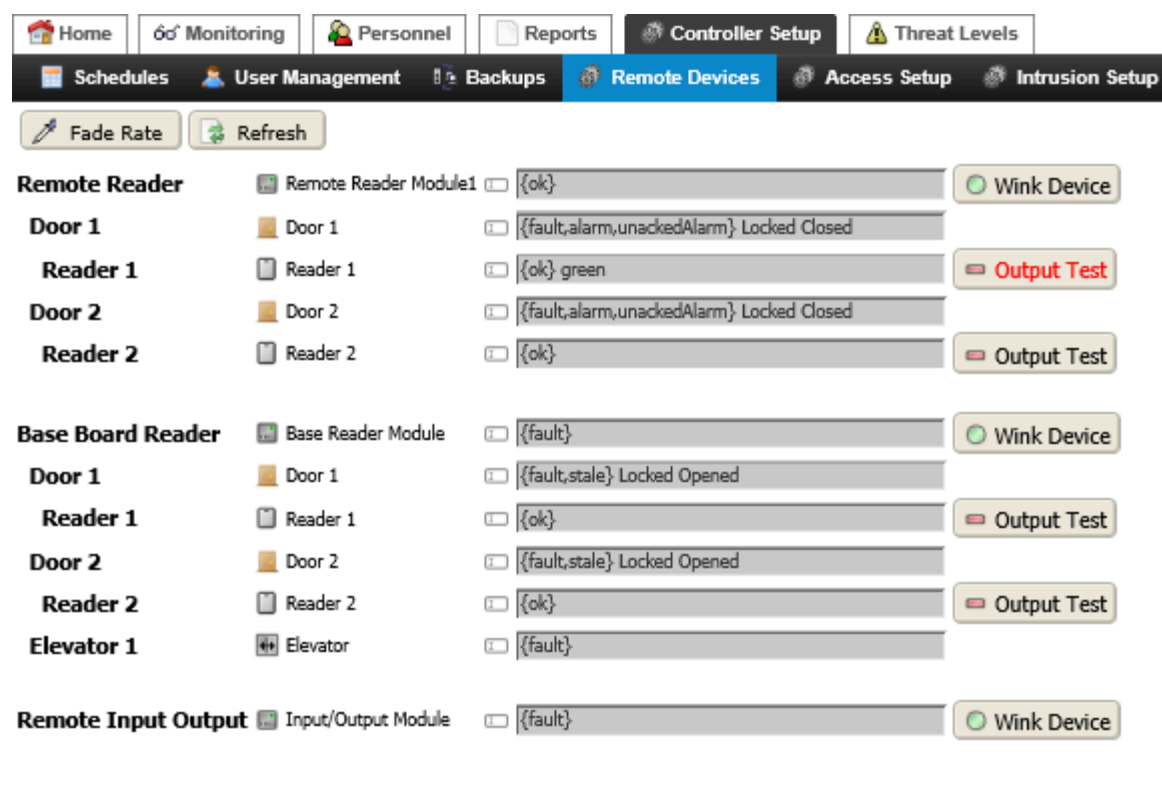
Figure 7. View pane with edit view

These views usually have control buttons located directly below the view title for performing save, refresh, or other context-appropriate actions.

Another characteristic of edit views is the presence of tabs for grouping information. Tabs allow you to conveniently view more information in a small amount of user interface space. Switching among tabs does not typically require a save action because you are not leaving the current page when you change tabs.

- Function views include views that perform a maintenance or communication action, such as a system backup or a network identification action.

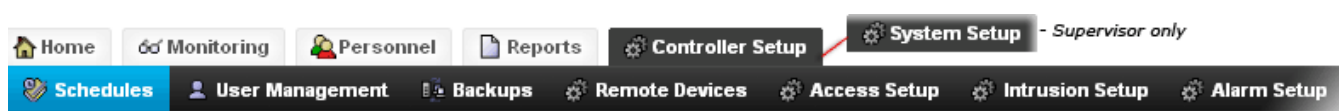
Figure 8. View pane with a typical function view



Controller (System) Setup menu

Setup features configure system components and network properties, as well as user preferences and other variables. Setup views include a variety of interfaces that allow you to perform configuration tasks related to devices, users, as well as the performance and maintenance of the system.

Figure 9. Controller Setup menu

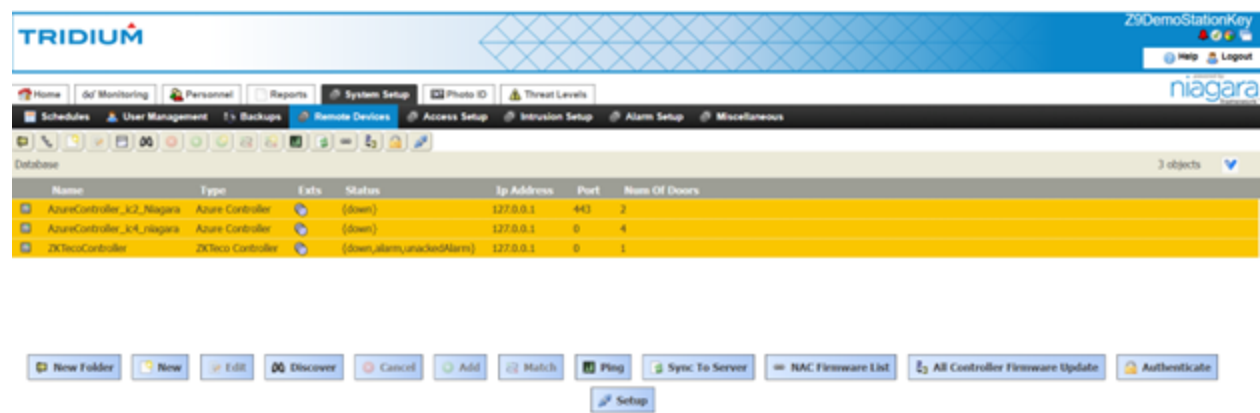


In a Supervisor system, configuration features are accessed using the System Setup menus. In a remote controller, similar features are accessed using the Controller Setup menus. When features are the same for both the Supervisor and controller stations, this documentation refers to them as Controller (System) Setup features.

NAC Network Setup Menu

NAC network Setup features configure system components and network properties, along with user preferences and others. Setup views for the NAC Network under Remote modules include various interfaces that allow you to perform configuration tasks related to the NAC Controller, Doors, and Reader, as well as the NAC Server's network connection property.

Figure 10. NAC Network Device Manager view



In a supervisor system, the NAC network view consists of actions and properties to add, discover, and configure NAC controllers.

Add NAC Controller Manually

The NAC network view consists of an "Add" option that enables the user to configure or add an NAC controller to the system.Click the New button on the Device Manager view.

- Step 1. Click the **New** button on the **Device Manager** view.

☒ Type to add

Azure Controller ▾

☐ Number to add

[1 - 100]

☐ Number of Doors

▾

OK

Cancel

The **New** window opens.

- Step 2. From the drop-down list, select the type and number of controllers you want to configure and the number of doors, and then click **OK**.
- Step 3. Once the controller type is selected, configure the NAC Controller properties, such as **Address** and **Port**, from the **NAC Device Add** window.

Name	Type	Enabled	Ip Address	Port	Num Of Doors
ZKTecoController1	ZKTeco Controller	true	127.0.0.1	0	1

Name

ZKTecoController1

Type

ZKTeco Controller

Enabled

true

Ip Address

127.0.0.1

Port

0

Num Of Doors

1

OK

Cancel

Step 4. After the device configuration update, click **OK** and check if the controller is added to the server.

Add Controller using Discover

To use this option, you must connect the controllers to the same network where the server is running before discovering the controller in the Device Manager view.

Click the Discover button at the bottom of the Device Manager view. Now the Discover job would search for the controller in the local network database and list all the controllers on the network.

The screenshot displays the TRIDIUM Niagara Enterprise Security Facility Manager interface. The top navigation bar includes tabs for Home, Monitoring, Personnel, Reports, System Setup, Photo ID, and Threat Levels. Below this, a sub-navigation bar contains tabs for Schedules, User Management, Backups, Remote Devices, Access Setup, Intrusion Setup, Alarm Setup, and Miscellaneous. The main area is split into two panes. The top pane, labeled 'Discovered', shows a table with columns: Device Name, Address, Type, and Number Of Doors, currently displaying 0 objects. The bottom pane, labeled 'Database', shows a table with columns: Name, Type, Exit, Status, Ip Address, Port, and Num Of Doors, currently displaying 3 objects. A toolbar at the bottom includes buttons for New Folder, New, Edit, Discover, Cancel, Add, Match, Ping, Sync To Server, NAC Firmware List, All Controller Firmware Update, and Authenticate.

This View has two panes :

- The Database pane at the bottom is where you can see all the devices or modules that are currently part of the system database. You can double-click an item in this pane to open its edit view.
- The Discovered pane (top pane) lists the modules or devices that the discovery job found on the network. Click on the discovered controller and then click on the **Add** option. Once the **Add** window opens, check the configuration properties such as the **IP Address** and **Port** of the device. Then, click **OK** to add the controller to the server.

Setup the NAC Network

The setup option lists a view to configure the **NAC Network**. Under the **NAC Device Manager** view, click on the **Setup** option and configure the server properties.

Step 1. Within the Setup menu, navigate to **HTTP Comm Config**.



The screenshot shows the Niagara Enterprise Security Facility Manager web interface. The top navigation bar includes the TRIDIUM logo, a Z9DemoStationKey, and a Logout button. Below the navigation bar, there are several tabs: Home, dd Monitoring, Personnel, Reports, System Setup, Photo ID, Threat Levels, Schedules, User Management, Backups, Remote Devices, Access Setup, Intrusion Setup, Alarm Setup, and Miscellaneous. The 'Remote Devices' tab is selected. Under this tab, there is a sub-menu with 'HTTP Config' and 'NACNetwork'. The 'HTTP Config' sub-menu is selected, and the 'NAC Http Comm Config' page is displayed. This page has a 'Save' button and a 'NACNetwork' button. The 'NAC Http Comm Config' section includes a 'Fault Cause' dropdown menu, a 'Use Tls' dropdown menu (set to 'true'), an 'Address' section with 'Ip Address' (set to 'localhost') and 'Port' (set to '446'), and a 'Connection Timeout' field (set to '0').

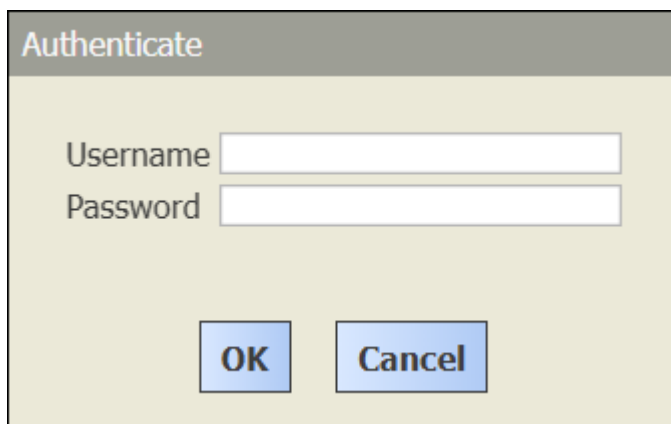
Step 2. Enter the **IP Address** as `localhost`.

Step 3. For the **Port**, enter the port number already set for **Niagara Access** (NAC Server) in the Niagara Access Configuration application and click **SAVE**.

Step 4. Access the **NAC Device Manager** to establish and authenticate the connection to the NAC server.

Step 5. Click on the **Authenticate** command under the Device Manager view to enter the server credentials.

Step 6. Enter the username and password that have already been set for **Niagara Access** (NAC Server), and click **SAVE**.



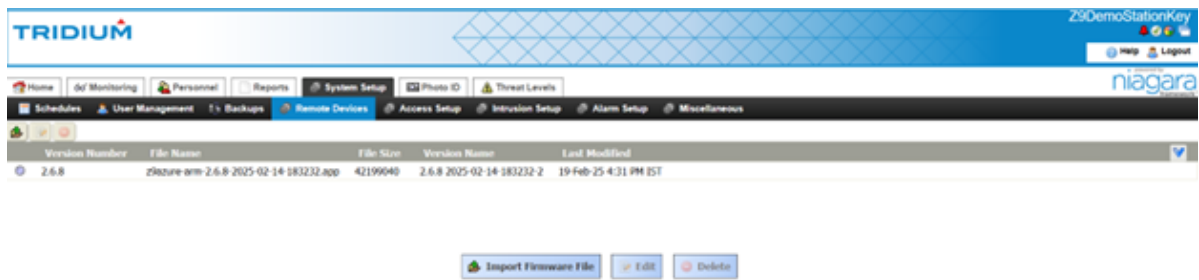
The screenshot shows a dialog box titled 'Authenticate'. It has a 'Username' label and a text input field, and a 'Password' label and a text input field. At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'.

Upload NAC Firmware files

The view provides a list of firmware upgrade files for the controller, including the latest versions that need to be used for uploading the firmware.

Step 1. Click on **NAC Firmware List**, and the **NAC Firmware UX Manager** will open.

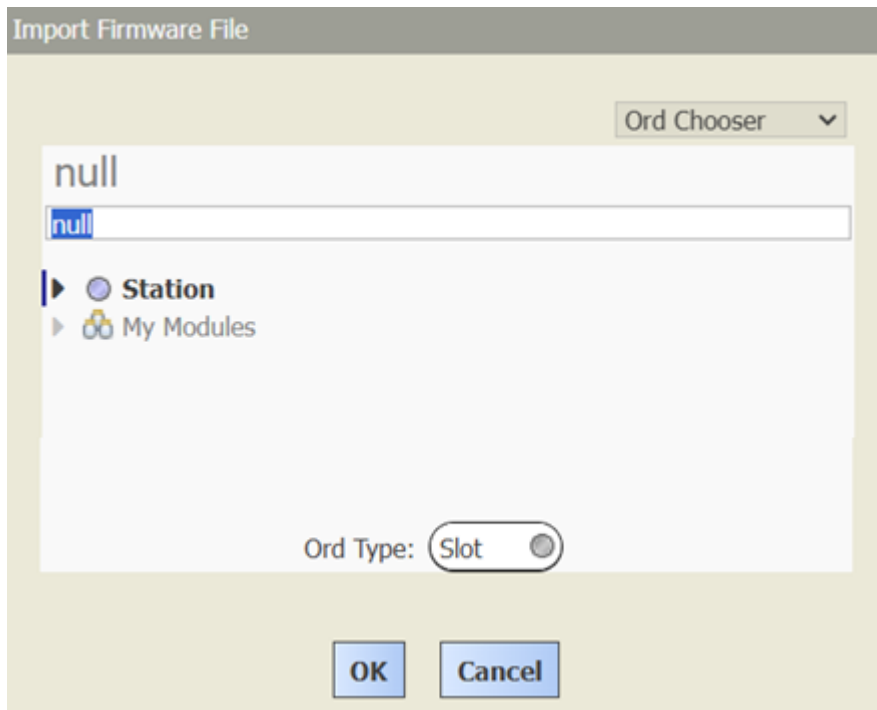
Step 2. Click on the **Import Firmware File** button to store the firmware file on the server.



The Store Firmware File on the Server window opens.

Step 3. Click on the **Import Firmware File** option. The **File Chooser** window opens.

Step 4. Select the appropriate firmware file for the controller and click **Open** **Ok**.



Step 5. Click **OK** to add the Firmware file.

Result

Navigate to the Firmware List in the **UX Manager** view and observe that a new entry is there with updated file details.

Discover, Learn, Add, and Match

The manager views, such as the Station Manager - Database view, provide a way to find network modules and devices, and add them to the system database. The system runs this discovery action as a two-step job.

1. First step: The system discovers (learns) device candidates for inclusion in the system database.
2. Second step: The system presents a list of candidates from which you manually select and add modules and devices to the database. If you already added devices to the database using a New window, the discover process lets you match found candidates to existing device records.

NOTE: You do not need to use discovery if you already added a device. If the device shows a valid status, {ok}, in the Database pane, it is already on line and discovery is not necessary.

The result of the discovery job is a table view, where each row represents a unique module or device.

Figure 11. Network Discovery view after discover job

Station Name	Host Name	Scheme	Fox Port	Status	Actual Role	Role Status
Station1	localhost	foxs	4911	{down}	Peer	{ok}
entSecurity801	localhost	foxs	4911	{disabled,fault}	Peer	{ok}

Discovered

Page 2 of 8 Page Size 20

Station Name	Host Name	Scheme	Fox Port	Already Exists
J17_1927	HTSWin2012R2.tridium2012.net	fox	1927	false
J18_1928	HTSWin2012R2.tridium2012.net	fox	1928	false
J18_1928	HTSWin2012R2.tridium2012.net	fox	1928	false

This view has two areas or panes:

- The Database pane (top pane) lists the devices or modules that are currently part of the system database. You can double-click an item in this pane to open to its edit view.
- The Discovered pane (bottom pane) lists the modules or devices that the discovery job found on the network.

Discovery control buttons

In addition to the standard control buttons (Hyperlink, Delete, Rename, Filter, Refresh, and Export, the Database and Discovery panes contain control buttons specifically related to discovery.

Database pane control buttons

The Database pane lists the devices that are currently in the system database. You double-click an item to edit available device properties.



These control buttons perform unique functions related to discovery:

- Discover opens the Discover window, which defines the database search. Based on this information, the discovery job interrogates the target location for data, such as historical and current values.
- Learn Mode buttons open and close the Discovered pane in a manager view to show or hide the control buttons and any discovered items (devices, points, database properties, etc.).

Discovered pane control buttons

This pane displays the results of the discovery job and lists the modules and devices found on the network. Devices that already exist in the system database appear in the database pane and appear dimmed in the Discovered pane.

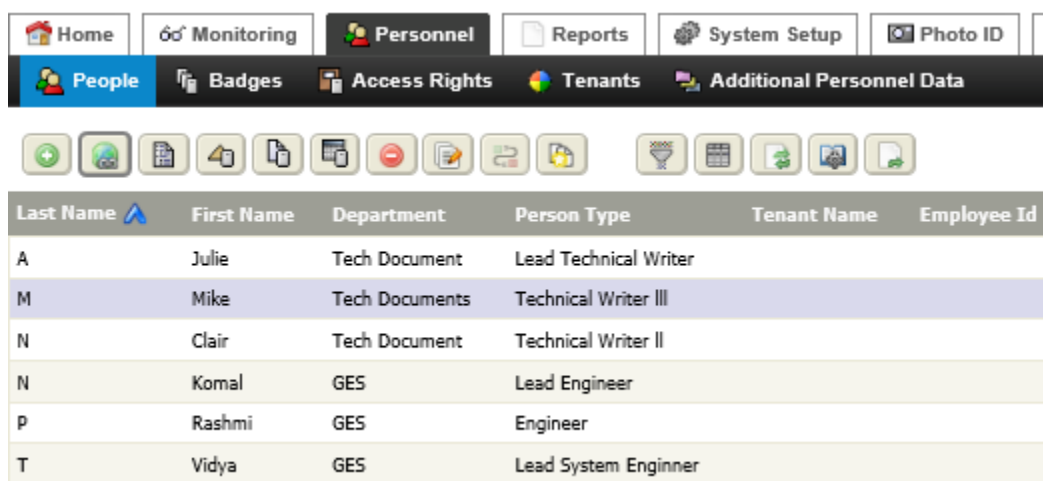
The control buttons in this pane specifically relate to the discovery process.

-  Add discovered item(s) moves one or more discovered items from the Discovered pane to the Database pane. It is available when items are selected (highlighted) in the Discovered pane. Before the item(s) are added, a window opens with properties to configure them.
-  Match initiates an action to add a single item to the system database. It is available only when you select an item in both the Database pane and the Discovered pane of a manager view. This action associates the discovered item with the selected item that is already in the database—usually an item previously added off line. The added item assumes the properties defined for it in the database. You can edit properties after adding the item. (This button also synchronizes similar schedules (subordinate to supervisor) under a single name.)

About table views

The Alarm Console and other views present information in tables. You can customize this information by sorting, filtering, editing column order, and by removing and adding columns. In addition, you can export tables for processing in a spreadsheet or other application. This topic introduces table controls and options.

Figure 12. Table controls and options (People view table)



Last Name	First Name	Department	Person Type	Tenant Name	Employee Id
A	Julie	Tech Document	Lead Technical Writer		
M	Mike	Tech Documents	Technical Writer III		
N	Clair	Tech Document	Technical Writer II		
N	Komal	GES	Lead Engineer		
P	Rashmi	GES	Engineer		
T	Vidya	GES	Lead System Enginner		


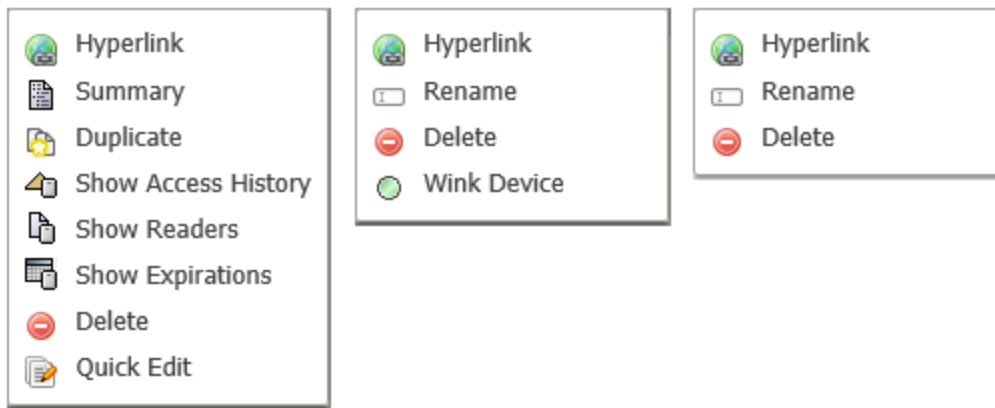
- The View Title displays the name of the view.
- Control buttons add, link, delete, filter and work with the displayed data in a variety of ways that are context sensitive. Tool tips describe the function of each control button. Buttons remain dim until one or more table rows are selected.
- Column headings indicate the type of data. To sort a table with reference to a column, click once on the column heading. The up (ascending) or down (descending) arrow on the column heading indicates the sort order.
- Page display controls indicate the number of pages of data.
 -  Previous and next arrows provide incremental control over displaying multiple pages of data.
 - Page boxes select the page to view (type the page number in the box and press Enter).
 - Scroll bars and mouse wheel provide scrolling options.

Table right-click menus

In table views, controls are located both across the top of the view and in context-sensitive right-click menus provide options for working with the database records in table views.

Figure 13. An example three right-click menus

Each menu includes optional actions that are appropriate for the type of table view. The first menu is from right-clicking a person record on the People view. The second menu is from right-clicking a remote reader module record in the Remote Module Setup view. The third menu is from right-clicking a role in the Roles view. The following describes the options in these menus:

- **Hyperlink** links to the edit view or window for the selected item. It is the same as double-clicking the table row.

Summary opens the **Summary** window for the selected item, which shows how item properties are currently configured. Double-clicking on any row in a table opens the Summary tab, which contains the same information as the **Summary** window.

Duplicate opens a **New** window and populates each property with properties from the selected item. Using this button speeds the item creation.

Show Access History opens the Access History view for the selected record.

- **Show Readers** displays an appropriate readers report for the selected records.

Show Expirations opens the Person Access Right Report view.

Delete removes the selected item (row) from the table. This button is available when you select an item.

Quick Edit opens the **Quick Edit** window for the selected item(s). This feature allows you to edit one or more records without having to leave the current view.

Rename opens the **Rename** window with which to change the name of the selected item.

- **Wink Device** access sends a message to a device expecting to receive a response.

Sorting table data by column

By default, the system displays the records in a table descending order based on the first column in the table. You can change both the sort order and the column used to sort.

Prerequisites:

The current view contains a table.

The Alarm Console is a good example of how to sort a table.

Time Range ? to ?

6 Source(s) / 6 Alarm(s)

Info	Timestamp	Source	Message Text	Source Sta
<input type="checkbox"/>	01-Jun-18 9:45:31 AM EDT	NiagaraNetwork Station1	Ping Failed	Offnormal
<input type="checkbox"/>	29-May-18 5:13:28 PM EDT	NiagaraNetwork entSecurity802	Ping Failed	Offnormal
<input type="checkbox"/>	28-May-18 9:31:30 AM EDT	NiagaraNetwork MyStation10	Ping Failed	Offnormal
<input type="checkbox"/>	23-May-18 1:29:05 PM EDT	Remote Reader Module.Door 2.Exit Request	Supervised Fault Detected	Fault
<input type="checkbox"/>	23-May-18 1:29:04 PM EDT	Remote Reader Module.Door 1.Exit Request	Supervised Fault Detected	Fault
<input type="checkbox"/>	23-May-18 1:14:31 PM EDT	Nrio Network remoteReader_1	Ping Failed	Offnormal

The default view of this table displays alarm records in descending order () by Timestamp. This displays the most recent alarms at the top of the table.

- Step 1. To use a column other than the first column to sort the table, click the column title.
The system displays table records in ascending order () based on the column you clicked.
- Step 2. To change the sort order to descending, click the column title again.
The arrow changes to descending order () based on the column you clicked.
- Step 3. To again display information in an ascending order, click a column title.

Adding columns to a table

Each table view opens to a set of default columns. You can add and remove columns as needed.

Prerequisites:

A table view is open.

- Step 1. Click the Column Chooser button ().

The Column Chooser view opens.


Columns for People

Icons: Save, Edit, Delete, Up, Down, Add, Remove

Name	Display Name	From Type
lastName	Last Name	entsec:Person
firstName	First Name	entsec:Person
department	Department	entsec:Person
personType	Person Type	entsec:Person
tenantName	Tenant Name	entsec:Tenant

Row Type
Report Type
Pre-Filtering

From	Property	Linked Property
entsec:Person	Last Modified	
entsec:PersonZoneJoin (person)	Person Id	
entsec:PersonLdapServerJoin (person)	Last Name	
entsec:SupervisorZoneJoin (person)	First Name	
entsec:Badge (owner)	Middle Initial	
entsec:PersonInfo (person)	Employee Id	
entsec:PersonAccJoin (person)	Department	
	Person Type	

- Step 2. In the lower table, select a node under the **From** column that contains the properties from which to choose.
The Property and Linked Property drop-down lists populate with available properties.
- Step 3. Select the Property or Linked Property to include and click **Add Column**.
The system adds the property to the columns table at the top of the view.
NOTE: The addition is not final until you click the Save button ().
- Step 4. After adding any additional columns, click the Save button at the top of the view.
The **Save** window prompts you to confirm.




- Step 5. To confirm the configuration, click **Yes**.
The system adds the column(s) to the right end of the table.

Deleting table columns

This procedure documents how to delete table columns.

Prerequisites:

The table exists.





- Step 1. Click the Column Chooser button ().
The Column Chooser view opens.
- Step 2. In the upper half of the view, select the row that represents the column you want to delete and click the Delete button ().
The system removes the row from the table.
- NOTE:** The deletion is not final until you click the Save button ().
- Step 3. After deleting any additional columns, click **Save** at the top of the view.
The system opens a @Save confirmation window.
- Step 4. To confirm the deletion, click **Yes**.

Editing table column order


This procedure explains how to change the order of the columns in a table.

Prerequisites:

The table exists.

- Step 1. Click the Column Chooser button ().
The Column Chooser view opens. The top-to-bottom order of the table rows at the top of the view relates to the left-to-right column order in the target table.
- Step 2. In the upper half of the view, select the row that represents the column to move and click the Up and Down buttons ( ) repeatedly until you position the property in the desired order.
- NOTE:** The new order is not final until you click the Save button ().
- Step 3. To save, click Save button at the top of the view.
The system opens a @Save confirmation window.
- Step 4. To confirm the column order change, click **Yes**.

About filtering tables

The system displays data in table views. Clicking the Filter button () opens a **Filter** window with which to set up search criteria (the columns to filter on). By defining exact, include, and match case properties, you can select precisely the records you are interested in viewing. The system uses these criteria to query the database.

You can define a single filter property or combine properties. Be as precise as you can when filtering records stored in a large database. Alarm and other data grow quickly. If a query generates a table larger than 5,000 records, a message alerts you that only the first 5,000 will be available for viewing.

NOTE: Filter windows are context sensitive so that the available properties reflect only the data in the currently active table view. For example, the **Filter** window contains **Timestamp** only for tables that have a Timestamp column.

Wild cards and filter properties

The percent (%) character (wild card) may precede, trail, or surround a filter string. The filter properties: **include**, **exact**, and **match case** further limit search results.

Figure 14. Example search with leading wild card

access Access History Alarm History Intrusion History Attendance History Audit History Log History						
Page 2 of 11 Page Size 20						
Timestamp	Operation	Target	Slot Name	Old Value	Value	User Name
18-Jul-18 6:56 PM IST	Added	Orion Person, N, Komal				admin
18-Jul-18 6:56 PM IST	Added	Orion Person, P, Rashmi				
18-Jul-18 6:55 PM IST	Login	/Services/WebService				
18-Jul-18 6:34 PM IST	Logout (Timeout)	/Services/WebService				
18-Jul-18 6:12 PM IST	Login	/Services/WebService				
18-Jul-18 5:42 PM IST	Logout (Timeout)	/Services/WebService				
18-Jul-18 5:27 PM IST	Login	/Services/WebService				

Filter

Timestamp

Today

>>

☒ Operation

%

Must Include

☒ Case Sensitive

☒ Target

%

Must Include

☒ Case Sensitive

☐ Slot Name

%

Must Include

☒ Case Sensitive

☐ Old Value

%

Must Include

☒ Case Sensitive

☐ Value

%

Must Include

☒ Case Sensitive

☐ User Name

%

Must Include

☒ Case Sensitive

Ok

Cancel

The example above filters on **Station Name** using the **include** and **match case** properties. A string, such as %8000 with the include box selected, returns records with the following possible values in the Station Name column: HQ-8000, myStation-8000, but not myStation-HQ.

In another example, the string myStation , with the **exact** check box selected, returns only results that have myStation as the complete Station Name. More or fewer characters in the name exclude the record from the filtered results.

You may add other criteria to further refine this search.

Table 1. Filter properties

Property	Description
include	Includes results that match the pattern defined by the wild card expression.
exact	Looks for the specific string text. If you use the percent character, the system looks for the actual percent symbol and does not use it as a wild card.
match case	Configures the search to be are case-sensitive.

String filter functions

These functions are available for use to provide advanced filtering options.

Table 2. String functions

Characters	Description
	Two pipes (vertical bars) define the OR function.
&&	Two ampersands define the AND function.
!	A pipe followed by an exclamation point define the OR NOT function.
&!	The ampersand followed by an exclamation point define AND NOT function.

The following examples illustrate how the functions filter this list of data characters: A, AB, AC, ABC, B, BC, C. Note the different results.

Figure 15. String filter examples


Filter	Result
%A% && %C%	ABC, AC
%A% && %C% &! %B%	AC

Filtering data in a table

Filtering tables, such as lists of personnel or the data in the report views, removes records from the view that you do not need.


Prerequisites:

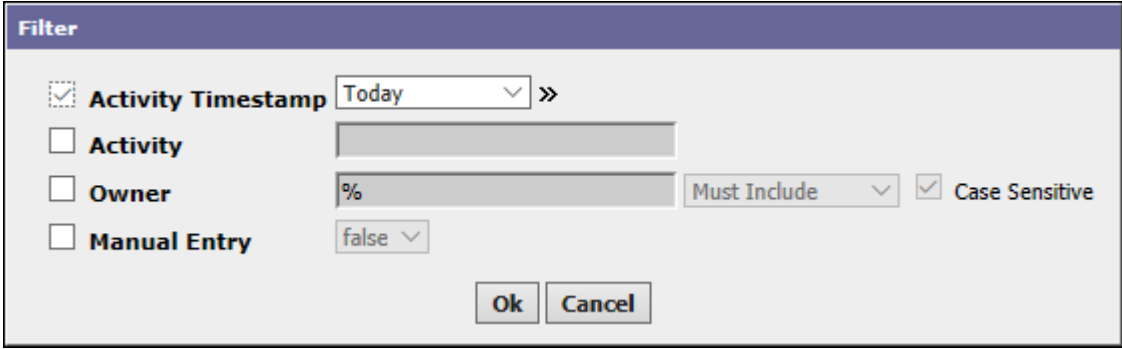
A table view is open.

- Step 1. Click the Filter button ().
The appropriate Filter window opens. The filter criteria reflect the table column (property) titles.
- Step 2. To designate the properties to filter on, enable one or more check boxes.
The selected properties names change from read-only to active.
- Step 3. Fill in a value for each property and select or clear the **include**, **exact**, and **match case** check boxes as needed.
The system constructs a database query.
- Step 4. To apply the filter, click **Ok**.
The system recreates the table and displays the query results based on the filter criteria.


Filtering using time

Timestamp properties are available in many filter windows.

- Step 1. Click the Filter button () in any table view, such as the Alarm Console view.
A **Filter** window opens.



The example shows the attendance history **Filter** window.

- Step 2. Click the selection box next to a general period of time for a Time drop-down list (**Normal Time**, **Ack Time**, etc.)
This activates the property. The time options list offers preset periods (Today, Yesterday, Month-to-Date, and others). When you choose the **Time Range**, the system displays a clock button ().
- Step 3. Choose a time option from the drop-down list.
- Step 4. If you chose **Time Range**, click the clock icon.

The system opens the **Time Picker** window on which to specify a range of time values.

The **Time Picker** window has a title bar with the same name. It contains two rows of time selection controls. The first row is for the minimum time, with a checked checkbox, a 'min' label, and dropdowns for 20, Apr, 2017, 12, 00, PM, and EDT. The second row is for the maximum time, with a checked checkbox, a 'max' label, and dropdowns for 20, Apr, 2017, 05, 00, PM, and EDT. At the bottom are 'Ok' and 'Cancel' buttons.

Notice that the **Time Picker** window has **min** and **max** properties for specifying a fixed filtering time range or for choosing an open-ended start and end time.

- Step 5. To select a more specific range than the time options offered in the Time list, click the browser icon (>>) to open the **Advanced Time Range Options** window. The system opens the **Advanced Time Range Options** window and changes the browser icon to red.

The **Advanced Time Range Options** window has a title bar with the same name. It contains fields for 'Start Time' (12:00 AM) and 'End Time' (12:00 AM). Below these are checkboxes for 'Days Of Week' (Sun, Mon, Tue, Wed, Thu, Fri, Sat), all of which are checked. At the bottom is a 'Schedule' dropdown menu with a red browser icon and the text 'None', followed by a red '>>' button. At the very bottom are 'Ok' and 'Cancel' buttons.

NOTE: Make sure that the inquiry you configure using the filter window and these advanced time range options makes sense. For example, if you select a specific date using the filter window, and then exclude that specific day by de-selecting it using the **Days of Week** properties in this window, the system responds with a message, *Advanced Filtering too Strict*.

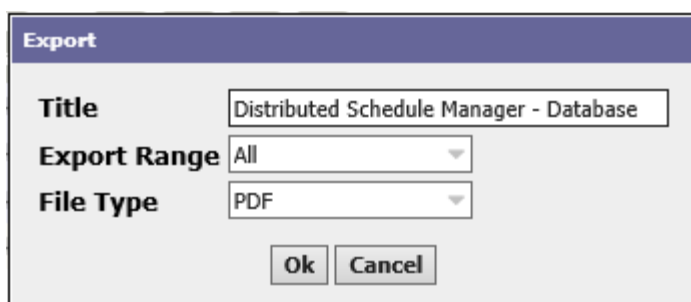
- Step 6. Configure the properties in this window to set specific time ranges and days of week for filtering tables and reports.
- Step 7. Configure the **Schedule** property to assign specific times to individual days and click **Ok**. **Schedule** works together to further restrict which records display.

Exporting data to PDF or CSV

All views that display the Export button () allow you to export the table of data to either a PDF or CSV (Comma Separated Values) file, which you can import to a third-party program, such as Excel. You may export all data in the table (includes all pages) or just the page that is currently displayed in the view.

- Step 1. Navigate to the view that contains the data to export.
- Step 2. To export only selected records, do one of the following:
- To select non-contiguous rows, hold the **Ctrl** key and click each row.
 - To select contiguous rows, hold the **Shift** key, and click the first and last row.
- Step 3. Click the Export button ().

The **Export** window opens.



Step 4. Give the file at least a **Title**, select the file type, and click **Ok**.

- PDF (Portable Document Format) is for ultimately printing the exported data.
- CSV (Comma-Separated Values) is for processing the exported data in a spreadsheet or other application.

Depending on your browser, a window opens with options for saving or viewing the exported file.


Quick editing common properties

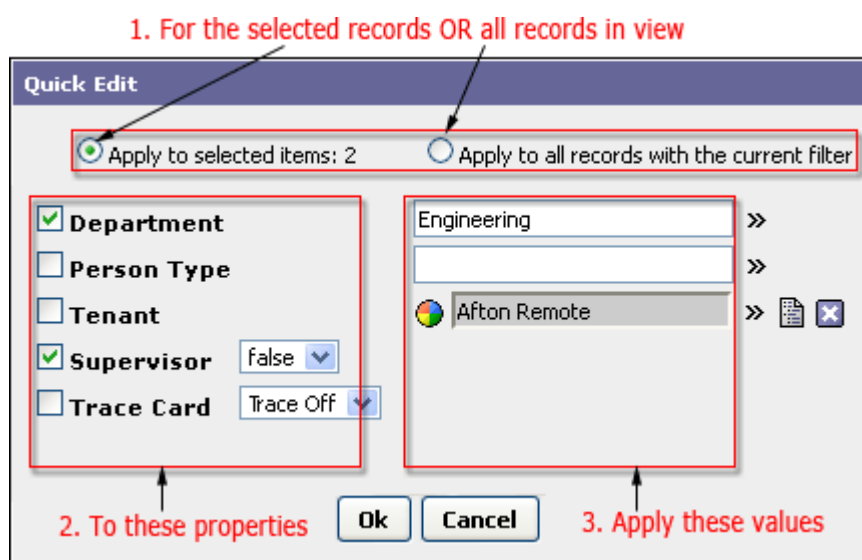
The **Quick Edit** window provides a way to edit the most common configured properties for each record in the database. The properties available to edit depend on the type of record. Many other properties may define each record. To edit the not-so-commonly-configured properties, access the property sheet for the record type.

Prerequisites:

The current view shows a table of database records.

Step 1. Select the record to edit.

Step 2. Click the Quick edit button () at the top of a view.
The **Quick Edit** window opens.



Step 3. Choose to which records to apply your changes:

- **Apply to selected items:** n applies the change(s) to the currently-selected records.
- **Apply to all records with the current filter** applies the change(s) to all records based on the current table filter.

Step 4. Fill in the values to change and click **Ok**.
The system updates the record(s) in the database.

Adding, discovering (learning), and matching

Modules and devices, to be connected, or that are already connected to the network need to be identified, named and added to the system database. To assist with this process, the system runs a discovery job. Using the results of this job you add the newly-found object or match it to its record that is already in the database. Once added, you can enable or disable a driver directly from this view by right-clicking on the driver in the table and selecting **Enable /Disable Networks** from the popup menu.

NOTE: This section refers to connecting the JACE controllers. To connect other Entsec controllers, refer to the NAC Network Setup Menu.


Adding remote modules and devices off-line


An off-line device is a module or device for which information about the unit has been added to the system database before the actual unit is physically installed on the network. The ability to add device records to the database before the device is physically on the network can speed the implementation of a new system. This procedure describes how to add remote modules and devices to the system database before they are physically connected to the network.

Prerequisites:


NOTE: If the remote module or device is already connected to the network (on line), skip this procedure and add the device using the discovery process.

Step 1. Under the **Controller Setup** menu, click **Remote Devices > Remote Modules > Remote Module Setup**.
The Access Device Manager-Database view opens.

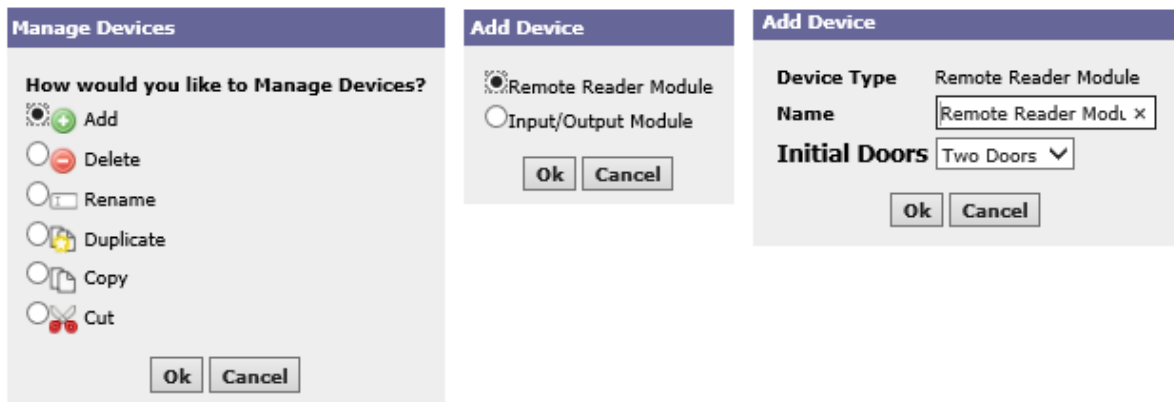


Display Name 	Enabled	Status	Device Type	Uid	Installed Version	Available Version
Base Reader Module	true	{fault}	Base Board Reader	000000000000		1.34
Input/Output Module	true	{fault}	Remote Input Output	000000000000		1.34

The Database pane lists the devices that are currently in the system database. You double-click an item to edit available device properties.

Step 2. Click the Manage Devices button ().


The **Manage Devices** window opens.




- Step 3. Select the **Add** option and click **Ok**.
The **Add Device** window opens.
- Step 4. Select the option that matches the type of module you are adding, and click **Ok**.
Another **Add Device** window opens.
- Step 5. Enter a descriptive name for the module and click **Ok**.
A new device is added to the Database pane at the top of the view.
- Step 6. Repeat these steps for all modules, up to a maximum of 15 modules.
- Step 7. Physically install each module.
- Step 8. Discover the module(s) and match each with its record in the database.


Discovering modules and devices

Discovery finds network modules and devices and presents them in a list so you can add them to the system database or match them with records already in the database. Adding a discovered device is similar to adding an off-line device with the added bonus that values for some properties are pre-populated because the device is on line. Matching a discovered device to its record in the database completes a configuration that you started off-line. Whether you add or match, you can edit the configuration of each device later.


- Step 1. Under the **Controller Setup** menu, select **Remote Devices > Remote Modules > Remote Module Setup**.
The Access Device Manager - Database view opens. The Database pane lists the objects (if any) that are already added to the database. On initial setup, there may be no objects in the Database pane.
NOTE: If a device appears in the Database pane, and its status shows {ok}, it is already on line and information about it is in the system database. Discovery is not necessary.
- Step 2. At the top of the view, initiate the discovery job by clicking the Discover button ().


The system runs a device discovery job to learn (find) and display the devices that are available on the local area network. A progress bar appears over the view. When the discovery job finishes all discovered objects appear in the Discovered pane below the Database pane. The result of the discovery job is a table-based view with two panes, where each row represents a unique device.

						
Display Name	Enabled	Status	Device Type	Uid	Installed Version	Available Version
Base Reader Module	true	{fault}	Base Board Reader	000000000000		1.34
Remote Reader Module	true	{fault}	Remote Reader	000000000000		1.34
Remote Reader Module1	true	{ok}	Remote Reader	00001065ec78	1.34	1.34

Discovered 				
Address	Device Type	Uid	Version	Used By
1	Remote Reader	00001065ec78	1.34	Remote Reader Module1

- The Database pane (top pane) lists the modules and devices that are currently in the system database.
- The Discovered pane (bottom pane) lists the modules and devices found on the network by the discovery job. Devices that already exist in the system database appear in the database pane and appear dimmed in the Discovered pane.

Step 3. To close the Discovered pane, click the Learn Mode button ().
The Discovered pane closes.

Step 4. To open the Discovered pane again, click the Learn Mode button again ().
The Discovered pane opens.


Adding discovered objects

After a discovery job runs, devices that are connected to the network, but are not in the database need to be identified, named and added to the database.

Prerequisites:

The discovery job found devices that need to be added (they appear in the Discovered pane, but not in the Database pane).

Step 1. Select one or more discovered device(s) and in the Discovered pane.

Step 2. To add the device(s) to the database, click the Add button () or right-click the selected row and click **Add**.
The **Add** button is available when you select (highlight) a device in the Discovered (bottom) pane. The **Add** window opens. The properties in this window already contain acceptable values, otherwise communication to the device would not have occurred. Usually, only the name needs to be changed. You can always edit these properties later.

Step 3. Change the name and click **Ok**.
The system adds the device(s) to the database and the device(s) appear in the Database pane.

Step 4. Double-click the module row in the Database pane.

An **edit** window opens.


- Step 5. For each added module, edit the available properties, including defining the **Alarm Class** and click **Save**.

Matching discovered objects

After a discovery job runs, devices or modules that were added to the database while off-line need to be matched to the installed devices.

Prerequisites:

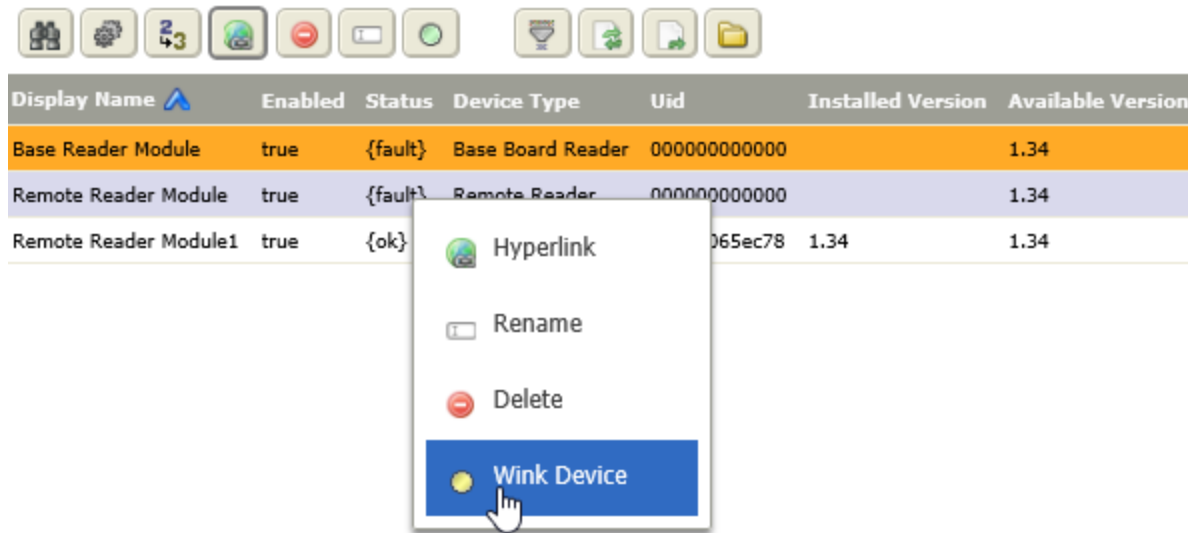
The discovery job found devices that need to be matched.

- Step 1. Select a device row in the Database pane and the same device row in the Discovered pane.
- NOTE:** Match is strictly a one-to-one function for discovered-to-database objects. Match is unavailable any time you select multiple items in either the top or bottom pane.
- Step 2. To match the device with its record in the database, click the Match button () or right-click the row in the Discovered pane and click **Match**.
- Step 3. To edit the database record for the matched module, double-click the module row in the Database pane.
- An edit page opens. Matching populates the discovered device's address values. These properties are valid, otherwise communication to the discovered device would not have occurred.
- Step 4. For each matched object, edit the available properties, including defining the **Alarm Class**, and click **OK**.
- The system adds the device or module to your station database. You can always edit the device component properties after you click **OK**.


Finding a device to match

The wink action makes it easy to match the entry in the Discovered pane with the actual hardware device that the entry represents. This can be especially helpful when you have a lot of devices on your network and are naming and adding them to your database.

Right-click the device in the Database pane and click **Wink Device**.




The device comes on line and cycles the first relay output on and off for 10 seconds.

NOTE: The Wink button changes from green to yellow while the wink action is active. Another way to wink a device in the Database pane is to select it and use the Wink control button () at the top of the view.

Configuring inputs and outputs

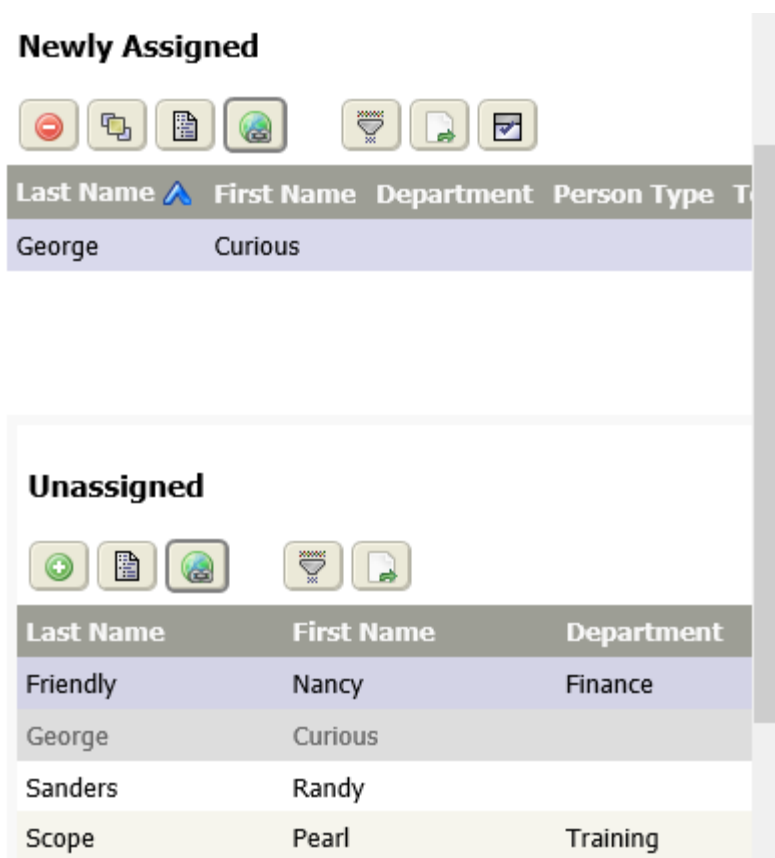
This procedure documents how to configure inputs and outputs. Configuration properties are similar for inputs and supervised inputs. This procedure describes how to configure existing inputs and outputs. Input and output configuration is similar, with differences noted in the procedure. These inputs are described in more detail in the mounting and wiring documents listed in the [Setup prerequisites](#) topic.




- Step 1. From the main menu, click **Controller Setup > Remote Devices > Remote Modules > Remote Module Setup**.
The Access Device Manager- Database view opens.
- Step 2. Double-click the module that contains the point(s) to edit.
The Edit Module view opens.
- Step 3. Select the Additional Points tab.
- Step 4. To rename an individual point, click the Manage Devices button ().
- Step 5. Click the point link to configure.
The Edit Point view opens. The point name appears in the view title and the configuration tab displays by default.
- Step 6. Configure the properties on each tab and click the **Save** button.

Assigning and unassigning items

In many views, you can use the learn mode with the **AssignUnassign** and buttons to add or remove items from the Database view.

- Step 1. Open a table view with a Newly Assigned pane;



- Step 2. Click the Assign Mode button ().
The Unassigned pane opens with a list of possible items for adding to the Newly Assigned pane at the top of the view.
- Step 3. To assign an item, select one or more items in the Unassigned pane and click on the Add (Assign) button ().
Newly assigned items are dimmed in the Unassigned pane and no longer available after you save the assignment.
- Step 4. To remove an assigned item, select one or more items in the Assigned or Newly Assigned pane and click the Unassign button ().


Mapping cameras connected to a Supervisor PC


To associate alarms in a host controller with one or more video cameras installed on the Supervisor PC, you map the camera(s) in the host controller.

Prerequisites:

You are connected to the host controller's station.

NOTE: Not all video drivers support remote video streaming and mapping. Refer to your camera documentation.

- Step 1. Open the Station Manager by clicking **Controller Setup > Remote Devices > Station Manager**.
The Station Manager-Database view opens.
- Step 2. Select the station name and click the Summary button ().
The station's summary page opens.

- Step 3. Click the Device Exts tab.
A summary list of the device extensions associated with the station opens.
- Step 4. Click the Cameras [hyperlink](#).
- Step 5. The Camera Manager view opens.
- Step 6. To discover cameras, click the Discover button ().
The system displays the found cameras in the Discovered pane.
- Step 7. Select and add the cameras connected to the Supervisor station.



Mapping cameras connected to a remote controller

To view in a Supervisor station the video streams coming from one or more video cameras installed on a remote controller, you map the camera(s) to the Supervisor station.

Prerequisites:

You are working in a Supervisor station.

NOTE: Not all video drivers support remote video streaming and mapping. Refer to your camera documentation.

- Step 1. To open the Station Manager, click **System Setup > Remote Devices > Station Manager**.
The Station Manager view opens.
- Step 2. Select the station row and click the Summary button ().
The Summary tab opens.
- Step 3. Click the Device Exts tab.
A summary list of the device extensions associated with the station opens.
- Step 4. Click the cameras [hyperlink](#).
- Step 5. The Camera Manager view opens.
- Step 6. To discover cameras, click the Discover button ().
The system displays the found cameras in the Discovered pane.
- Step 7. Select and add the cameras connected to the remote host.

Chapter 2. Special event scheduling

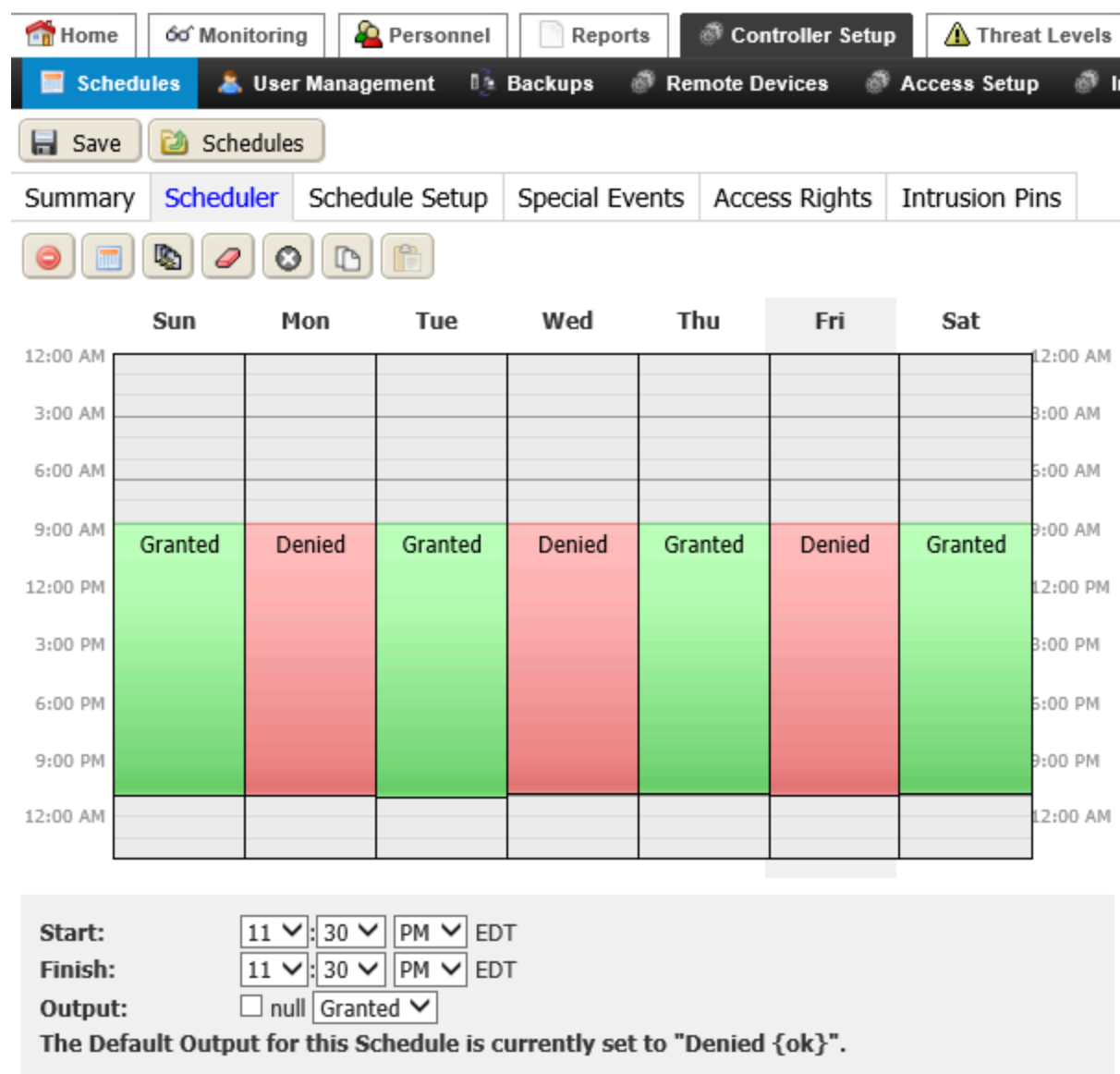
The system supports two types of schedules: weekly schedules, which define normal weekly hours of operation and one-off special events, and calendar schedules, which define recurring special events. The *Installation and Maintenance Guide* provides a procedure for creating weekly schedules. This chapter covers the scheduling of special events.

Weekly schedules

A weekly schedule defines normal working days. Two types of special events configure exceptions to the normal weekly schedule:

- One-time only events, such as three hours off to view a solar eclipse, apply to individual weekly schedules only.
- Recurring special events, such as Christmas Day or Martin Luther King Day, reside on a calendar schedule. Weekly schedules reference calendar schedules. Since special events on a calendar schedule apply to any weekly schedule that references the calendar schedule, you can globally change the days of recurring special events in all weekly schedules by editing the calendar schedule.

Figure 16. Weekly scheduler view



The scheduling interface uses a simple calendar view. The screen capture is an example of a schedule used to configure access rights for a daily shift.

All special events on a weekly schedule take priority over regular weekly events. Among special events, you define relative priorities by the order of listing in the Special Events table, as follows:

- Highest priority is at top of list. These special events, when active, always occur.
- Lowest priority is at bottom of list. These special events occur only if not overlapped by other special events that are active during the same period.

Special events

The system provides multiple ways to define a special event:

- By specific date (**Date** option)
- Based on when the special event begins and ends (**Date Range** option)
- By defining a movable date based on the day of the week, the week within any month, and the month in the year (**Week and Day** option)
- By a combination of day within the month, month within the year, day of the week, week of the month and year (**Custom** option)
- By referencing a Calendar Schedule, which defines a recurring event.

NOTE: Special event are currently not supported for NAC Controllers.

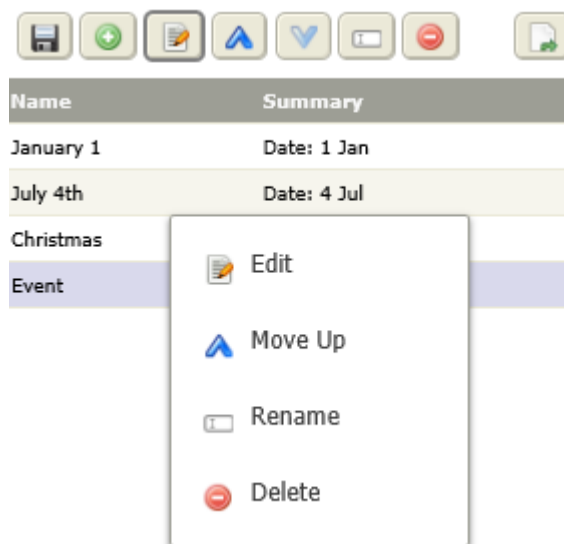
Adding a special one-time event

This procedure adds a one-time event to a weekly schedule.

Prerequisites:

The weekly schedule exists.

- Step 1. Open the schedule.
- Step 2. To add the special event, click the **Add** button.
The **Add** window opens.
- Step 3. Enter at least a descriptive name (**Display Name**) for the special event.
The name defaults to **Event**. You can change it later to something else.
- Step 4. To change a special event's priority, select it and use the priority arrow buttons.




Adding a special event by referencing a calendar schedule

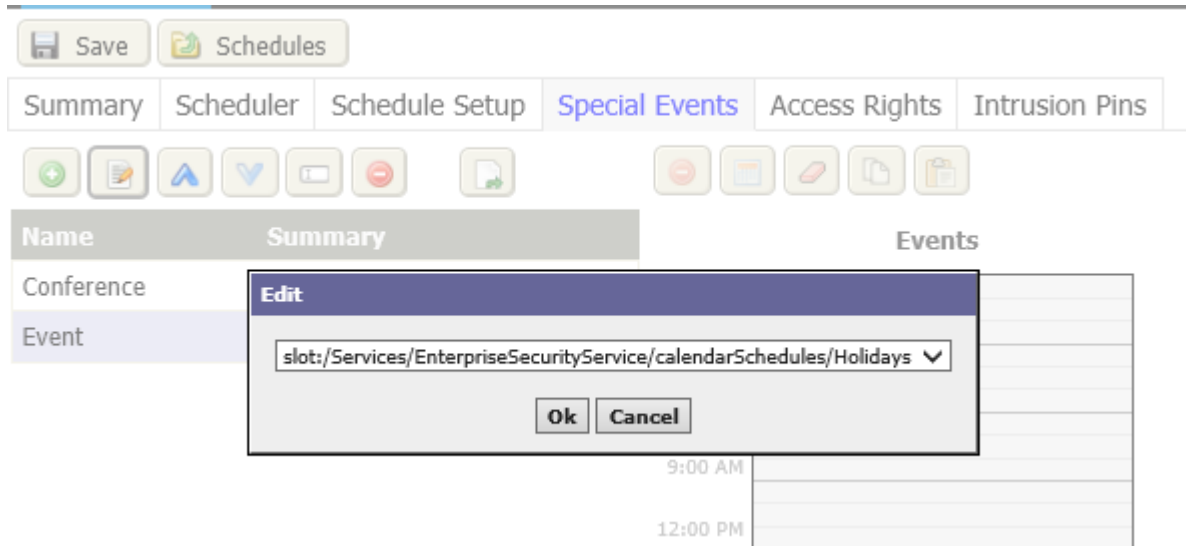
Special events defines exceptions to the weekly schedule as special events. A special event may be a one-time occurrence, such as three hours off to view a solar eclipse, or it may be a recurring special event, such as Christmas Day or Martin Luther King Day.

Prerequisites:

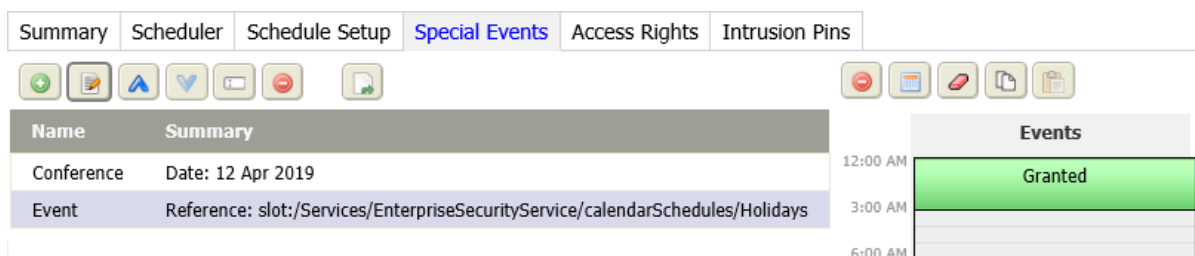
The schedule exists.

- Step 1. Click **Controller Setup > Schedules**, double-click a schedule, and click the **Special Events** tab.

- Step 2. To add a new special event, click the Add button ().
The **Add** window opens.
- Step 3. To add the special event by referencing a calendar schedule, enter a **Display Name** for the event, select **Reference** for **Type**, and click **Ok**.
The **Edit** window opens with a drop-down list of the ORDs for all the calendar schedules in the system.





- Step 4. Select a calendar schedule from the drop-down list and click **Ok**.
The newly-created special event exists in the Special Events table, but still needs to be added to the **Events** calendar. The table row remains selected for further editing, except for **Type**.
- Step 5. With the special event selected, click in the right-side **Events** column and drag to define the event start and end times.
The system blocks out the time by highlighting it..



The **Start**, **Finish**, and **Output** properties work the same as on the Scheduler tab of the Add New Schedule view. You can also right-click in the column for an event menu. This is useful to add an all-day event or set the entire day to the schedule's default value.

NOTE: You must drag to add the event to the Events column of the calendar for it to occur. If the Events column is empty, the special event relinquishes control back to any lower-priority scheduled events, and finally intermingles with the weekly schedule. To completely override the weekly schedule, configure a special event for the entire day.

- Step 6. Once you have several events on the schedule, use the Move Up and Move Down priority control buttons ( ) or right-click actions to prioritize the events.

All special events take priority over regular weekly events. Among special events, the order of listing in the **Special Events** table defines the relative priority of the events, as follows:



- The highest priority special event is at top of list. High-priority events, when active, always occur.
- The lowest priority event is at bottom of list. Low-priority events do not occur if other special events, which are active during the same period, overlap them.

Setting up holidays and other special events on a calendar schedule

You configure holidays and other special events on a global calendar schedule. Other weekly schedules include holidays and special events by referencing the calendar schedule that defines them. This way, if you use multiple schedules, you have to set up holidays only once.

Prerequisites:

This procedure explains how to set up a calendar schedule with holidays and other special events.


- Step 1. To access the Calendar Schedules view, click **Schedules > Calendar Schedules**.
The Calendar Schedules view opens.
- Step 2. To add a calendar schedule, click the **Add** button ().
The Add New Calendar Schedule view opens.
- Step 3. Enter a name for the calendar schedule in the **Display Name** property.
- Step 4. To add an event, click the Add button () on the Events tab.
- Step 5. Enter a name for the holiday or event in the **Display Name** property.
- Step 6. Do one of the following:
 - If the special event occurs on a single, specific day, select **Date** for **Type**. The four options work together to identify the single date. For example, if you select a weekday of **Tuesday**, month of **5**, and set the remaining properties to **Any Day** and **Any Year**, the special event occurs only on a Tuesday that falls on the fifth day of any month in any year. If a month does not have a Tuesday the fifth, no event is scheduled to occur that month.
 - If the special event takes place over two or more days, select **Date Range** for **Type**. The three options work together to identify the beginning and ending dates. While the start day can be after the end date, this only makes sense if year property is set to **Any Year**. For example, the start day can be in December and the end date in March indicating that the event occurs during December, January and February.
 - If the date of the special event differs each year, but you can define it based on the day of the week, the week in the month, and the month in the year, select **Week and Day** for **Type**. The three options work together to identify the date. For example, if weekday is set to **Monday**, week to **3**, and month to **February**, the event occurs only on the third Monday in February.
 - The **Custom** option is the most flexible, allowing you to configure any conceivable date. An example of where you might use this option is for the Thanksgiving holiday in the U.S., which is always the fourth Thursday in November.
- Step 7. Define the date, day or range and click **Ok**.
You can make only one selection for each property. This includes an **Any...** option, in addition to the specific options.
The system creates the special event.
- Step 8. Configure the schedule properties on the **Schedule Setup** tab and save the schedule by clicking **Save**.
NOTE: You can move between tabs without losing unsaved data, however, you must click the **Save** button before leaving the view or data are lost and no new schedule is added.

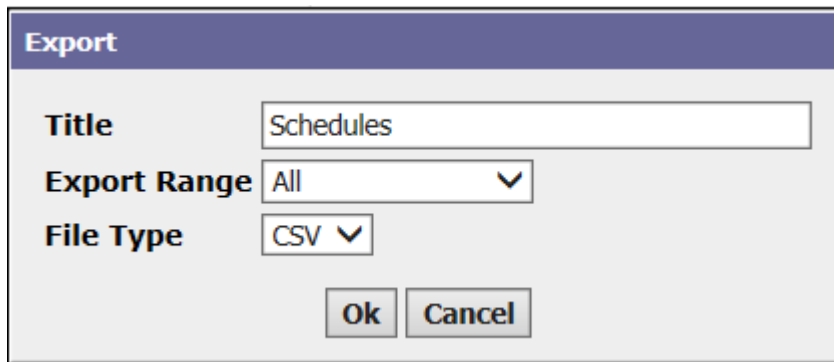
Exporting a schedule to a CSV file

This procedure documents how to export a schedule as a CSV file.

Prerequisites:

You start out working on a Supervisor station.

- Step 1. From the main menu, click **System Setup > Schedules**.
The Schedules view opens.
- Step 2. Select the schedule to export and click the Export button ().
- Step 3. Select **CSV** for **File Type**.
The window changes size.




- Step 4. To continue, click **Ok**.
The system prompts to confirm the download and downloads the CSV file.
- Step 5. Save the file to a location where you can be sure to find it.

One way to discover and export schedules

You may use the Join (Add) Station view to discover and export schedules.



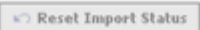
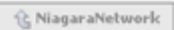
Prerequisites:

You are working in either the Supervisor or a controller station using the web UI.

- Step 1. If needed, return to the main menu.
- Step 2. Click **Controller (System) Setup > Remote Devices > Station Manager**.
The Station Manager - Database view opens.
- Step 3. Select a station in the database and click the Join button ().


The Add Station view opens.

Add entSecurity601

Step 1: Make sure the System Date Times are synchronized within 1min of each other.

Supervisor Time 16-Sep-09 8:44 AM EDT
Subordinate Time 16-Sep-09 8:44 AM EDT
Time Difference < 1min



Step 2: Use the Distributed Schedule Manager to import schedules.

[Distributed Schedule Manager](#)

Step 3: Make sure the database will be imported properly.

Record Type	Import Status
Tenants	Not Configured
Keypad Formats	Not Configured
Wiegand Formats	Not Configured
Personnel	Not Configured
Badges	Not Configured
Niagara Integration IDs	Not Configured
Access Rights	Not Configured
Intrusion Pins	Not Configured

Above is a view of the link that takes you to the Distributed Schedule Manager view.

- Step 4.** Click the **Distributed Schedule Manager** link.
The **Distributed Schedule Manager - Database** view opens.

Home

Monitoring

Personnel

Reports

System Setup

Threat Levels

Schedules

User Management

Backups

Remote Devices


Access Setup


Intrusion Setup

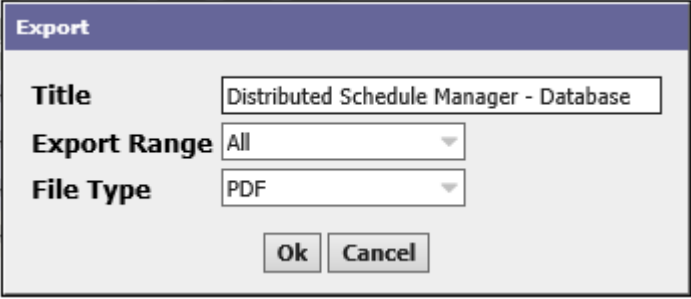
Display Name	Usage	Status	Out Source	Out	Next Time	Next Value	Supervisor Id
After Hours	Access Right	{ok}	Default Output	false {ok}	09-Jan-19 6:00 PM EST	true {ok}	/Services/EnterpriseSecurityService
Always	Access Right	{ok}	Week: wednesday	true {ok}	10-Apr-19 12:00 AM EDT	true {ok}	/Services/EnterpriseSecurityService
Weekend	Access Right	{ok}	Default Output	false {ok}	12-Jan-19 12:00 AM EST	true {ok}	/Services/EnterpriseSecurityService
Working Hours	Door Unlock	{ok}	Week: wednesday	true {ok}	09-Jan-19 6:00 PM EST	false {ok}	/Services/EnterpriseSecurityService

Discovered

Display Name	Path	Supervisor Id	Type Str
6-to-6 Schedule	slot:/Services/EnterpriseSecurityService/schedules/\$36\$2dto\$2d6\$20Schedule	NULL	schedule:BooleanSchedule

- Step 5. To discover additional schedules, click the Discover button (). The Discovered pane opens with the additional schedule(s).
- Step 6. Select the schedule records to export in either pane.

- Step 7. Click the Export button () for the pane.
The **Export** window opens.


The image shows a dialog box titled "Export". It has three fields: "Title" with the text "Distributed Schedule Manager - Database", "Export Range" with a dropdown menu set to "All", and "File Type" with a dropdown menu set to "PDF". At the bottom are "Ok" and "Cancel" buttons.

Export	
Title	Distributed Schedule Manager - Database
Export Range	All
File Type	PDF
<div>Ok Cancel</div>	

- Step 8. Fill in the properties and click **Ok**.

Another way to discover and export schedules

This method uses the Station Device Properties view to discover and export schedules.


- Step 1. If needed, return to the main menu.
- Step 2. Click **System/Controller Setup > Remote Devices > Station Manager**.
The Station Manager - Database view opens.
- Step 3. Select a station and click the **Summary** button in the toolbar.
The Station Device Properties view opens.
- Step 4. Choose the Device Exts tab and click on the [Schedules](#) link.
The Distributed Schedule Manager - Database view opens.
- Step 5. Click the Export button ().
The **Export** window opens.
- Step 6. Fill in the properties and click **Ok**.

Chapter 3. People management

For the purposes of this chapter, people include tenants, employees (personnel), and visitors. Managing the information the system maintains for these people includes creating and editing tenant records, individual personnel (employee) records, monitoring access, and viewing reports. This work must be done in the Supervisor station.

Creating a new tenant

Tenants separate personnel based on the company they work for. This is important when managing a multi-company building.

- Step 1. Click **Personnel > Tenants**
The Tenants view opens.
- Step 2. Click the **Add ()** button.
The **Add New Tenant** view opens.

Save

Tenants

Summary

Tenant

Niagara Integration IDs



Intrusion Pins

People

Badges

Threat Level Groups

Access Rights



Tenant Name

Description

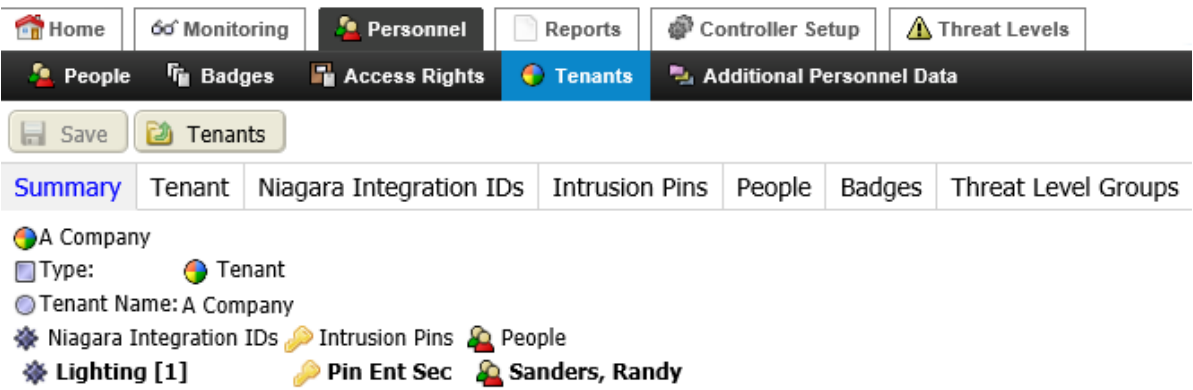
- Step 3. Provide the **Tenant Name** and an optional **Description** for the tenant.
- Step 4. Configure the individual tabs for each tenant and click **Save**.
Each tab provides a set of standard control buttons and two tables. The tables include assigned and unassigned assets (people, integration IDs, access rights, and badges) to associate with the specific tenant.
The new tenant is created and the edit tenant view opens with the newly created tenant properties.

Editing an existing tenant

Once created, you may edit tenant information as required.

- Step 1. Click **Personnel > Tenants**.
The Summary tab of the Tenants view opens.
- Step 2. To edit a tenant, double-click the tenant row in the table.

The view associated with that particular tenant opens.



This view displays no updated information until you enter data using the remaining tabs and save the updated information. The Summary tab may also include context-appropriate lists of the integration ID, people, badges, and access rights associated with the tenant.

- Step 3. Edit the information on each tab for the selected tenant and click **Save**.
The Summary tab of the Tenants view updates.

Creating a person record

This procedure documents how to add person records in the station database.

Prerequisites:

Access rights and person types have been created.

- Step 1. From the **Home** menu, click **Personnel** or expand **Personnel** and click **People**.
- Step 2. click Add New Person ().

The Add New Person view opens.

The screenshot displays the 'Add New Person' form. At the top, there are 'Save' and 'People' buttons. Below them are tabs for 'Summary', 'Person' (selected), 'Access Rights', and 'Badges'. To the right of the tabs is a toolbar with icons for saving, adding, deleting, and other actions. The form fields are as follows:

- Last Name:** Cruise
- First Name:** Tgm
- Middle Initial:** (empty)
- Employee Id:** (empty)
- Department:** (empty)
- Person Type:** (empty)
- Tenant:** None
- Supervisor:** false
- Trace Card:** Trace Off
- PIN:** PIN (number only): (empty), Confirm PIN: (empty)
- Portrait:** (camera icon)

Step 3. Fill in at least **Last Name**, **First Name**, **Department** and **Person Type**.

Step 4. To assign one or more access rights to the person, click the **Access Rights** tab. You must assign at least one access right.

Step 5. When you are finished, click **Save**.

Editing an existing person record

This topic documents how to edit existing person records

Prerequisites:

One or more records for the person exist in the station database.

Step 1. From the **Home** menu, click **Personnel** or expand **Personnel** and click **People**.

Step 2. Do one of the following:

- To make available all data for editing, double-click the person row in the table and click the **Person** tab.
- To edit only essential information (**Department**, **Person Type**, **Tenant**, **Supervisor**, **Trace Card**, **Add Access Rights**, and **Remove Access Rights**), select the person row in the table and click **Quick Edit** (📄).

The Quick Edit window includes the most frequently-changed properties.

If you opened the Person tab, in addition to the same properties as those available on the Quick Edit view, you can change the person's PIN and badge.

Step 3. Do one of the following:

- If you selected a quick edit, choose to which records you want your change to apply, make your change and click **OK**. You are done.
- On the Person, Access Rights, and Badges tabs, make your changes and click **Save**.

Step 4. To return to the People view at any time, click **People**.


Combining person records

On occasion you may find two person records in the station database for the same individual. Both may contain needed information. This procedure uses the match feature to combine the records so that you do not have to delete and re-enter information.

Prerequisites:

Two records for the same person exist.

Step 1. From the **Home** menu, click **Personnel** or expand **Personnel** and click **People**.

Step 2. Ctrl + click to select the two records and click the Match button ().
A window opens with the properties as configured.

Step 3. Select the properties to keep from each record and click **OK**.
The system combines properties and saves one record, deleting the other.

Creating a PIN for a person

A PIN may be required along with a badge (card) to gain access to a building.

Prerequisites:


You are working in the web UI, usually on a Supervisor PC.

Step 1. To open the personnel record for the individual that needs the PIN, click **Personnel**.

If the person is not already in the database, click the Add button (



) and create a person record.

Step 2. Filter the table to locate the person, double-click the person row in the table or select the person role and click the Hyperlink button ().


Step 3. Click the Person tab.

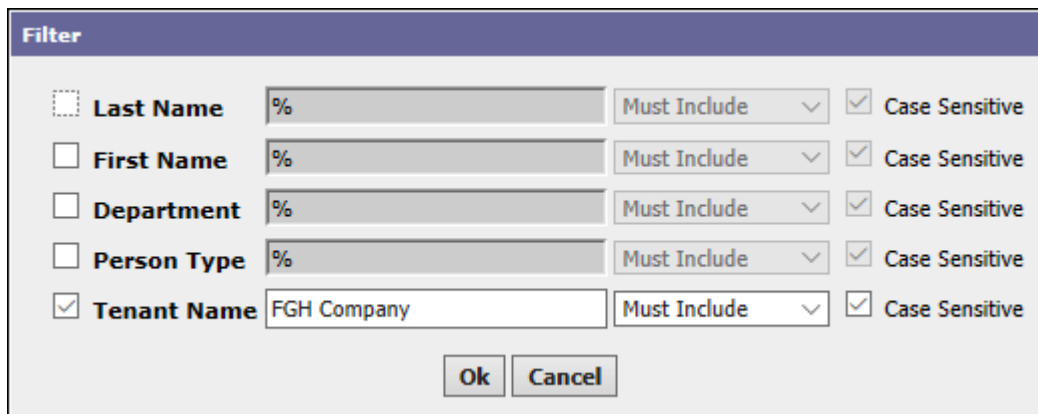
Step 4. Enter and confirm the PIN and click **Save**.

Filtering personnel records by tenant

If each person in the database has the **Tenant** property defined on their personnel record, you can sort the table in the People view to display only personnel assigned to a specific tenant or tenants.

Step 1. Click **Personnel**.
The People view opens.

Step 2. Click the Filter button ()
The Filter window opens.



Field	Value	Operator	Case Sensitive
<input type="checkbox"/> Last Name	%	Must Include	<input checked="" type="checkbox"/>
<input type="checkbox"/> First Name	%	Must Include	<input checked="" type="checkbox"/>
<input type="checkbox"/> Department	%	Must Include	<input checked="" type="checkbox"/>
<input type="checkbox"/> Person Type	%	Must Include	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Tenant Name	FGH Company	Must Include	<input checked="" type="checkbox"/>

Ok Cancel

Step 3. Click the check box next to **Tenant Name**, replace the percent symbol (%) with the tenant name, and click the **Ok** button.
The system displays only personnel for the tenant.


Assigning an access right to a person

The system grants access to a person by matching the access right on the person's personnel record with the access right that is associated with a door's reader. This procedure documents how to assign or change an access right on a personnel record. an individual person may have multiple access rights.



Prerequisites:

The personnel record for the person exists in the Supervisor station database. You are working at the Supervisor PC using the web UI.

Step 1. On the home page, click **Personnel**.

Step 2. Locate the person (you may need to filter the personnel records), and double-click the record or select it and click the Hyperlink button ().
The personnel record opens to the Summary tab.

Step 3. Click the Access Rights tab.

- Step 4. To display the available access rights, click the Assign Mode button ().
The system retrieves the available access rights and displays them in the Unassigned pane.
- Step 5. Select the right to assign, click the Assign button (), and click **Save**.

Access rights limited by time range


You assign specific rights to personnel. At the time you make this assignment, you can limit the person's use of the right based on a time range.

This time range is not the same as using a schedule to specify when the access right itself is effective. This only relates to a an individual person's ability to use the access right and not the access right's validity or availability for other personnel. For example, one person may have an access right assignment with an effective time range of 1 day while another person may have the exact same access right assignment with an effective time range of 2.5 years.

When access rights are assigned to a person the default time range (**Start Date** and **End Date**) of that assignment are always in effect. This means that, unless the time range of this person's access right assignment is changed (using the **Change Assignment Properties** window) the access right is immediately effective and never ends.

Editing access right effective date and assigned threat level

Access right **Effective Date** and **Assigned Threat Level** apply only to a single access right assignment. To change these properties, you navigate to a view that includes both the person and the assigned access right. The following steps describe how to change these properties starting from the Access Right view. Similar steps may be used to change these properties starting from the Add New Person and edit person views.



- Step 1. From the main menu, select **Personnel > Access Rights**.
The Access Rights view opens.
- Step 2. To edit the access right, double-click its row in the table.
The edit view opens.
- Step 3. Click the People tab and highlight the person whose access right effective date you want to change.
- Step 4. In the toolbar menu, click the **Change Assignment Properties** button ().
The **Change Assignment Properties** window opens.
- Step 5. Configure the properties: **Start Date** and **End Date** and **Assigned Threat Level**, and click the **Ok** button.
The access right properties are changed.
- NOTE:** Changing the **Assigned Threat Level** in an access right breaks the connection between the access right and the threat level defined by the access right's associated threat level group. Future changes to the threat level as defined in the threat level group will not affect the threat level that has been configured directly on an access right.
- Step 6. To update the database, click the **Save** button at the top of the view.

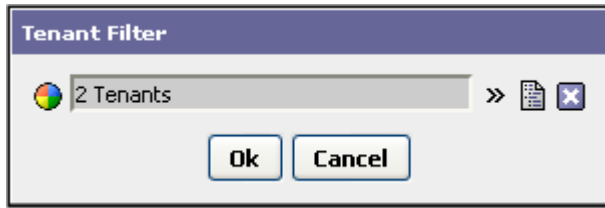
Restricting available information by tenant



In a system that supports multiple tenants, data must be restricted so that only authorized system users may gain access to the information that applies to a specific tenant. The information that can be controlled by tenant includes: personnel, badge, access right, intrusion PIN, Niagara Integration ID, user, and tenant records. If the **Tenants** property on a user record identifies a specific tenant value, that user can view only personnel, badge, access right, etc. information, which contains the same **Tenants** property values.

Prerequisites:

You are working in a Supervisor station. You have created tenant records for all tenants in the building

- Step 1. Create or edit a system user, access right, intrusion PIN or Niagara Integration ID.
- Step 2. For each record, click the chevron (>>) to the right of the Tenants property, select the tenant from the Ref Chooser window and either click the Assign button () and click **Ok**.
This associates the record with the specific tenant.
- Step 3. To limit the records that are available based on the current tenant, click the Tenant Filter icon () in the top right corner of the view.
The **Tenant Filter** window opens.



- Step 4. Click the chevrons to the right side, select the tenant from the Ref Chooser list, click the Assign button (), and click **Ok**.
The system hides restricted information (data assigned to a tenant other than the current tenant) and the Tenant Filter icon changes to a lock icon (). More than one tenant may be added the viewing restriction by using the Tenant Filter window. You add or remove tenant filters to show or hide information.
- Step 5. To remove the restriction, click the lock icon, and click the X icon to the right in the **Tenant Filter** window.
All data are available for viewing.

Result

The **Tenant Filter** window can restrict information that the current user sees in several specific views. When using this feature, be aware that:


- The system filters information a user can view based on the **Tenants** property values that are associated with the user. For example, "Tenant A" and "Tenant B" cannot view "Tenant C" information because it is not available to them.
- If a tenant is assigned a single **Tenants** property value, the **Tenant Filter** window opens as read-only, since no additional filtering is available.



Managing occupants in an access zone

Normally, occupants enter and exit an access zone by scanning their badge at a card reader. This procedure allows you to manually update who is currently in the zone and to remove occupants from the zone.

Prerequisites:

The access zone exists in the local station. Your role allows you to change access zone properties (write enabled).

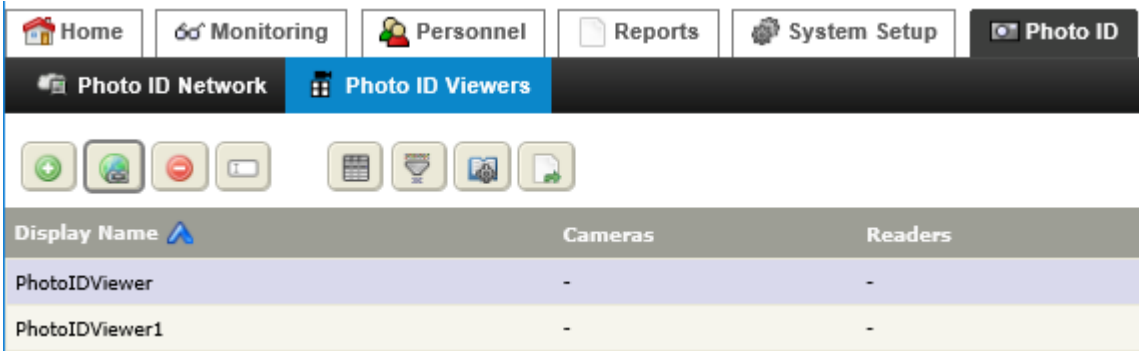
- Step 1. From the main menu, select **Controller Setup > Access Setup > Access Zones**.
The Access Zones view opens
- Step 2. Double-click an access zone row in the table.
The edit view for the access zone opens.
- Step 3. Click the Occupants tab, and click the Assign Mode button ()
A list of the personnel currently in the zone opens in the Assigned pane, and a list of personnel who are authorized to enter and exit the zone opens in the Unassigned pane.

- Step 4. To manually add personnel to the zone, select one or more persons in the Unassigned pane and click the Assign button ().
- The system adds the person to the list of Assigned occupants in the zone. To manually remove an occupant from the station’s access zone, select the person row in the Assigned pane and click the Unassign button (). The system removes the person from the zone.
- Step 5. If a number of people have left the zone without using the card reader, click the Access Zone tab and configure the **Passback Timeout** and **Reset Occupancy Enabled** properties.
- Establishing a **Passback Timeout** allows people to re-enter a space after the time-out expires without triggering a passback violation.
 - Configuring a **Reset Occupancy Time** removes all occupants from a zone at a defined time. After the set time passes, occupants may re-enter.
- Only system users whose role is configured with access zone write enabled may change these properties.

Monitoring door entries

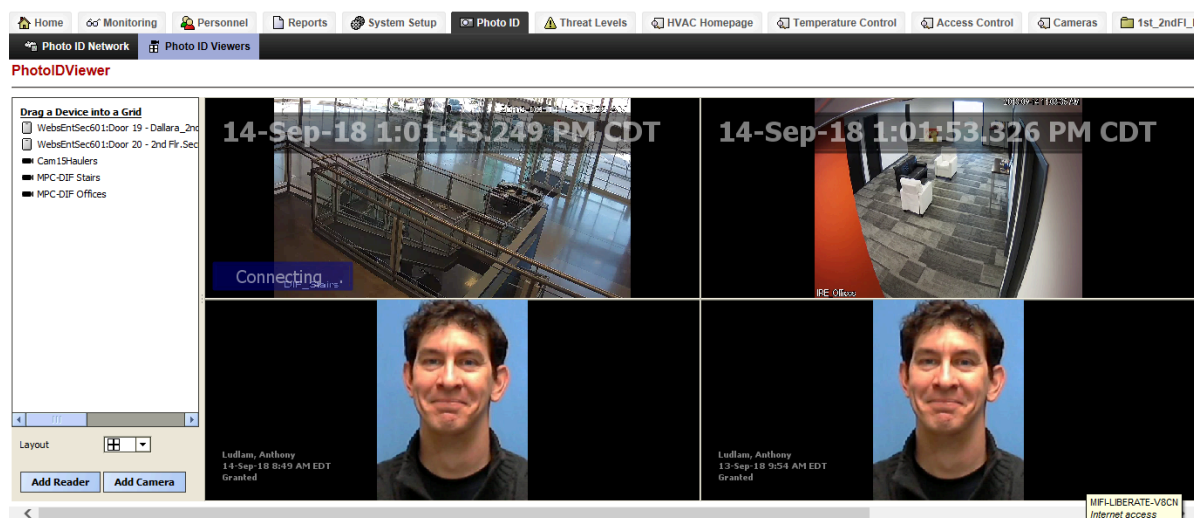
This feature selects a door (card reader), and displays the photo and the name of the person associated with a badge swipe.

- Step 1. Starting from the home (main menu view, click **Photo ID > Photo ID Viewers**. The Photo ID Viewers view opens.

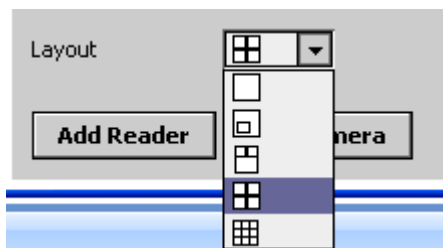


- Step 2. Double-click the **PhotoIDViewer** row.


The viewer window opens.



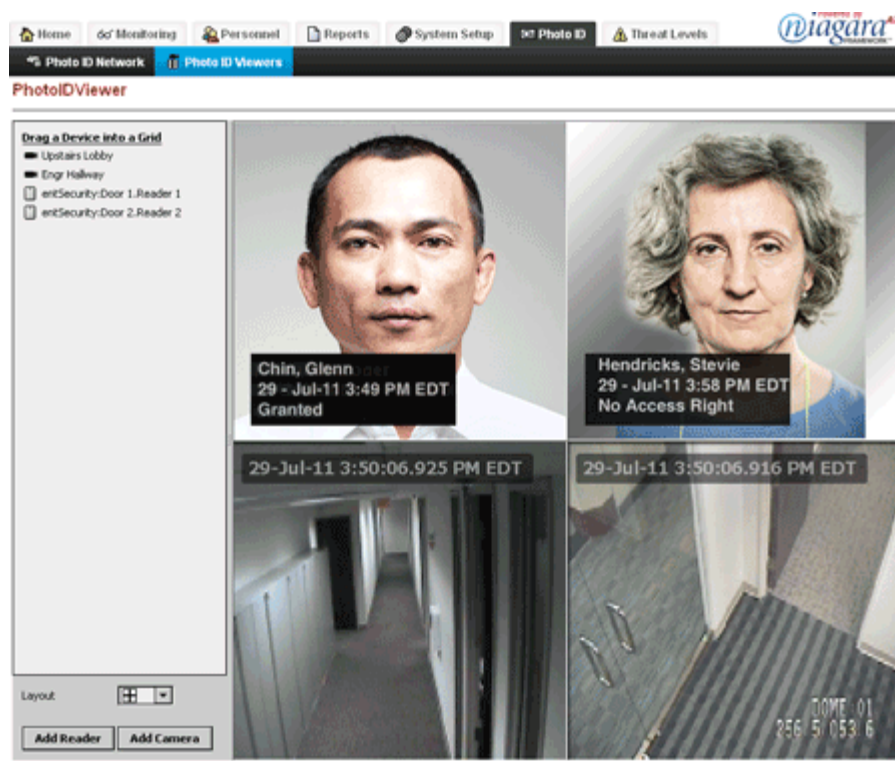
The layout above provides a grid for input from two card readers and two cameras. To change this layout, click the **Layout** drop-down menu.



Setting up the grid involves populating the device list on the left followed by dragging and dropping the readers and cameras from the list to the surveillance grid.

- Step 3. To populate the list, in the lower left corner, click the **Add Reader** or **Add Camera** buttons. The **Add Reader** or **Add Camera** window opens.
- Step 4. Select the device(s) and click the Add button (). The card readers and cameras populate the left pane of the view.
- Step 5. Drag each device name from the left pane to one of the quadrants.


As soon as someone swipes their badge, the photo associated with the person displays in the grid along with the feed from the surveillance camera.



You do not see a photo and personnel data along with the photo until someone swipes a badge. Unlike the example above, you would expect to see the same person in the video feed.

Manually inserting an attendance record

The system's time and attendance function marks badge transactions with a date and time that a badge holder arrives and departs work. These arrival and departure times are used by an external reporting system to calculate and report time worked. This attendance record keeping is handled automatically based on when the person swiped their badge. On occasion, you may need to make changes to the attendance records.

- Step 1. From the main menu, select **Reports > Attendance History**.
The Attendance History view opens.
- Step 2. Click the Add button ().
The manual **Add** window opens.
- Step 3. Fill in the timestamp, activity and owner (person for whom you are entering the attendance record) and click the **Ok** button.
The new record appears in the Attendance History view.

Tracing a person's entry and exit activity

The system monitors a specific person's entry and exit when you enable the **Trace Card** property for the person and for the reader. You can configure this feature when you initially create the person's personnel record. This procedure explains how to add it to an already-existing personnel record.

Prerequisites:

You are working in the controller station using the web UI.

- Step 1. From the main menu, click **Personnel**, locate the person, and double-click their row in the table.

The edit view for the person opens.

The screenshot shows the 'Personnel' tab in the Niagara Enterprise Security Facility Manager. The 'Person' edit form is open, displaying fields for Last Name (Smith), First Name (Curious), Middle Initial, Employee Id (1234), Department (Accounting), Person Type (Management), Tenant (TenantA), Supervisor (false), and Trace Card (Trace On). The 'Trace Card' dropdown is highlighted with a red box. Below the form, the 'Access Rights' tab is visible, showing a list of access rights with 'Trace Card Alert' highlighted.

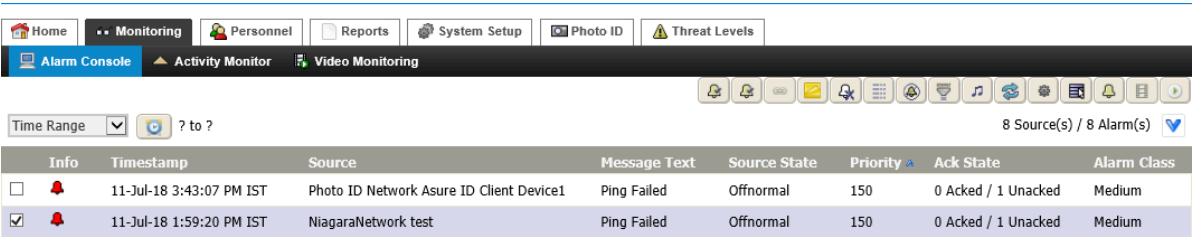
- Step 2. Click the **Person** tab, and change **Trace Card** from **Trace Off** to **Trace On**.
- Step 3. Click the **Access Rights** tab, double-click the access right assigned to this person, and click the **Readers** tab.
The edit view for the access right opens.
- Step 4. Double-click the reader assigned to the access right and click the **Activity Alert Exts** tab.
- Step 5. Assign an alarm class to the **Trace Card Alert** property and click the **Save** button at the top of the view.
When the system grants this person access at the designated door, the system also generates a trace card alarm.
NOTE: If the system denies access for any reason, it generates no alarm.


Displaying the person's photo on a history report

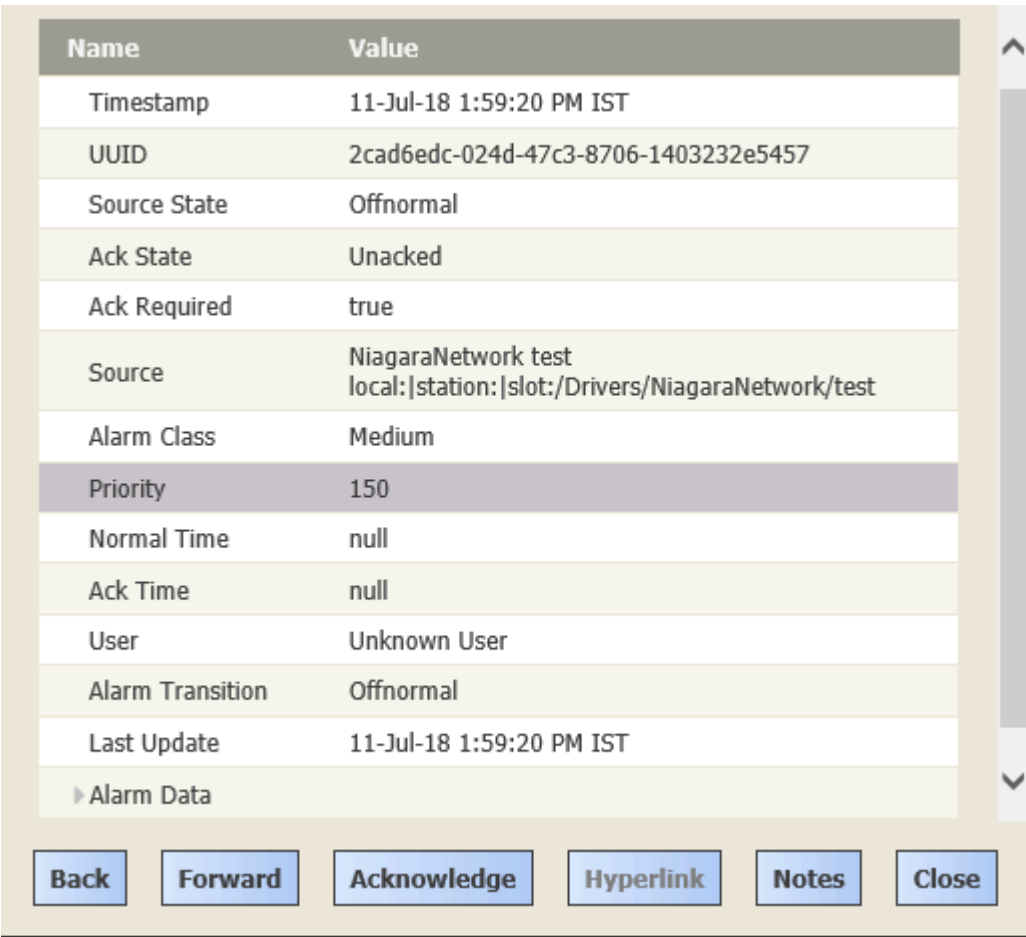
This feature displays the current photo associated with a history record. You may view the photo associated with a history record on the following reports: Alarm console, Activity monitor, Access history, and Attendance history. For example, the report can show the photo associated with the badge used to arm an intrusion zone. This photo is the one that is on file at the time of viewing the history.

- Step 1. From the home view click **Monitoring**.

The Alarm Console opens.



- Step 2. Select an alarm and click the Alarm Details button ().
The Alarm Details report opens.



- Step 3. Click the person's name next to **person** in the **Alarm Data** section of the properties list.

The person Summary opens.



The screenshot shows a 'Summary' window for a person. On the left, there is a list of properties: Type (Person), Last Name (Prospect), First Name (Wendy), Department, Person Type, and Tenant. To the right of this list is a portrait photo of a woman with brown hair, smiling. Below the photo, there is a 'Badges' section showing a badge icon and the text '00000 [0]'. At the bottom right of the window is a 'Done' button.

NOTE: Many data properties on the Alarm Details and person Summary windows are hyper links that, when clicked, provide additional information.

Easy Lobby visitor management

For systems with integrated visitor management, such as that provided by Easy Lobby, the visitor management system manages visitor entry and exit. The system automatically adds people when the visitor management system checks them in, and automatically deletes or disables them when they visitor management system checks them out or when their authorized visit expires.

A delay between the time the visitor management system checks visitors in or out, and when the information is available to the system is to be expected. This delay is usually about 30 seconds. Some configuration options, such as how long it takes to communicate the information from Easy Lobby to the system, require admin access to Workbench to configure.

For specific procedures that document how to check in a single visitor, multiple visitors, and repeat visitors refer to the visitor management system documentation. For Easy Lobby, this would be the [Easy Lobby SVM Installation, Administration, and User Guide](#).

Visitor management with Sine

Sine is a cloud-based visitor management application used by site administrators to manage visitor check-in and check-out requests.

This application provides these functions:

- Device configuration using the SinePro application
- User hierarchy creation for collaborators and delegators
- Site creation
- Pass configuration
- Check-in and check-out form creation and editing

- Notification management
- Badge printing
- Integration with third-party applications
- Report generation
- Delivery of invitations to hosts

Sine integrates with Microsoft Teams, Slack and WebHook. Sine-Pro can initiate visitor check-in and check-out requests in Enterprise Security.

Before beginning the configuration, the user must complete the following prerequisites for Sine and Niagara Station.

Prerequisites

You should provide Sine and station prerequisites before beginning the configuration.

Sine prerequisites


- **Creating a Sine Pro Account**

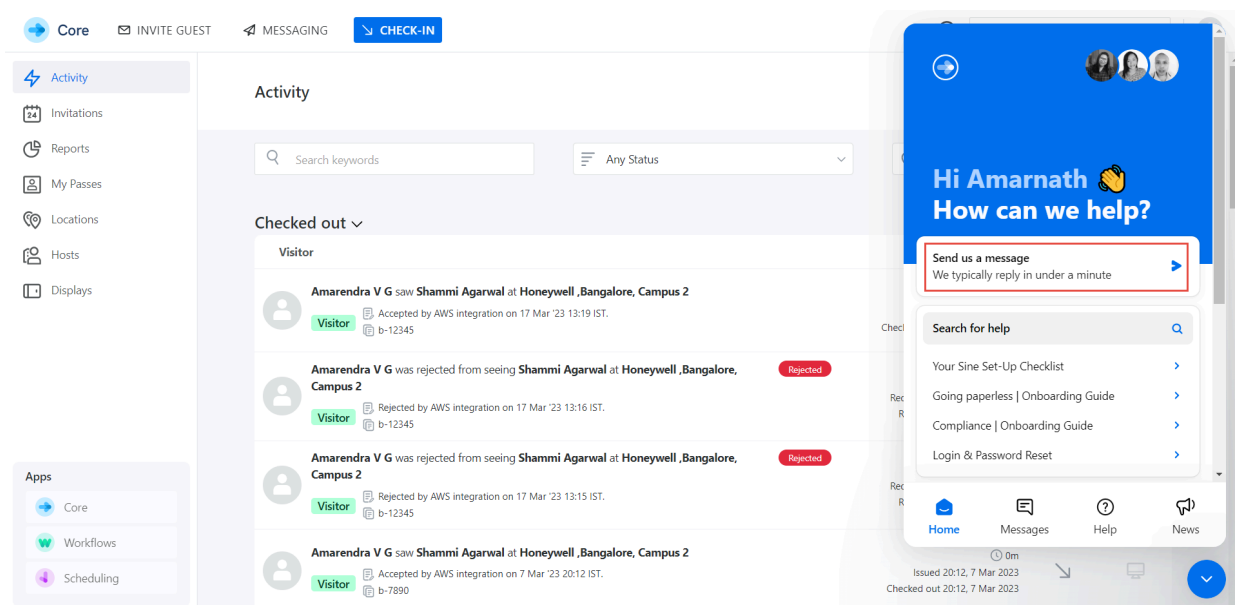
You should create a Sine Pro account as the first step. Refer to the link for creating a Sine Pro Account [Creating Sine Pro account](#)

- **Creating a site in Sine Pro Dashboard**

After logging into the Sine Pro account, you must create a site for the physical location where you intend to use Sine visitor management Refer to [Creating a site \(Creating a Site\)](#).

- **Enabling the CalbackService for WebHook** The callback Service needs to be enabled so the Niagara station can send a response to Sine when the check-in requests are approved or rejected. To enable the callback service for WebHook, the user must send a request to Sine Team. Follow the below steps to enable the Callback Service:

1. Log in to Sine Pro account.
2. In the Sine Pro dashboard, click on the Chat icon in the bottom right corner of the screen  and go to Messages.
3. Click on **Send us a message** and request the sine team to enable the callbacks and sign in pending for WebHook.



4. Once it's done and confirmed by the Sine Team, you can proceed with the configuration steps.

Niagara Station prerequisites

- **Adding necessary features and drivers to Niagara Station**

The Niagara station has the license for sineVisitorManagement and the MQTT driver. Contact the Tridium team to add these features to your license.

- **Providing AWS Certificate**

The device certificate (AWSCert.crt) must be imported into Niagara station. The device certificate is provided by the system integrator. For the demo purposes, contact the Tridium team.

Sine configuration

Some procedures occur on the cloud side. Others in the station. This topic summarizes the cloud-side configuration steps.

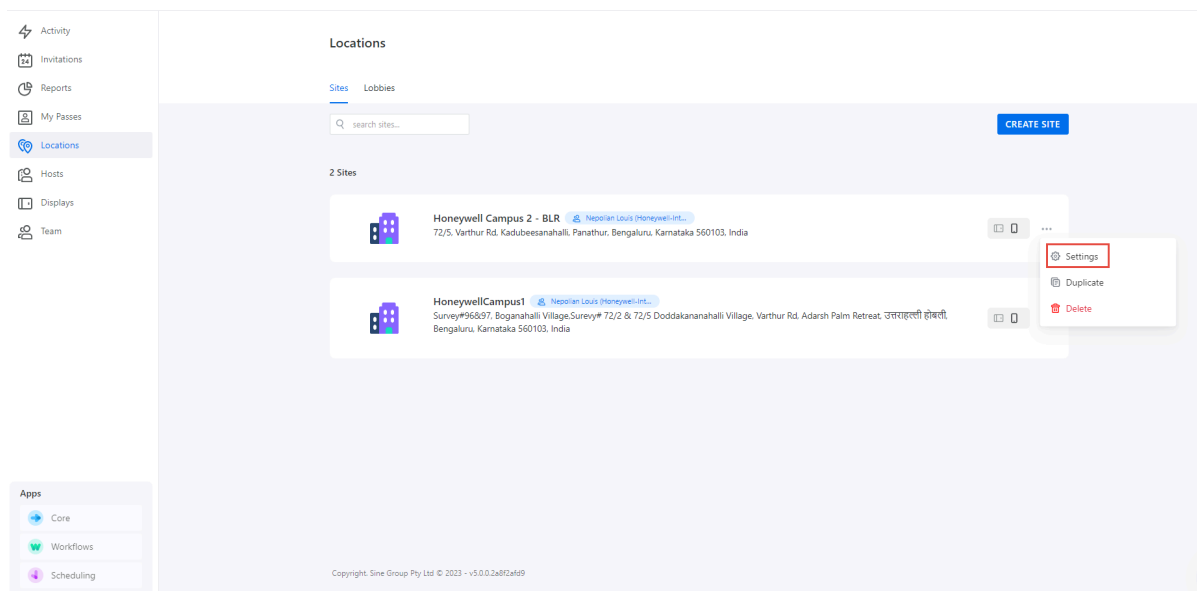
- Configure the site's webhook which includes setting up URLs, keys, visitor types and hosts.
- Set up check-in forms.

Configuring Sine and WebHook

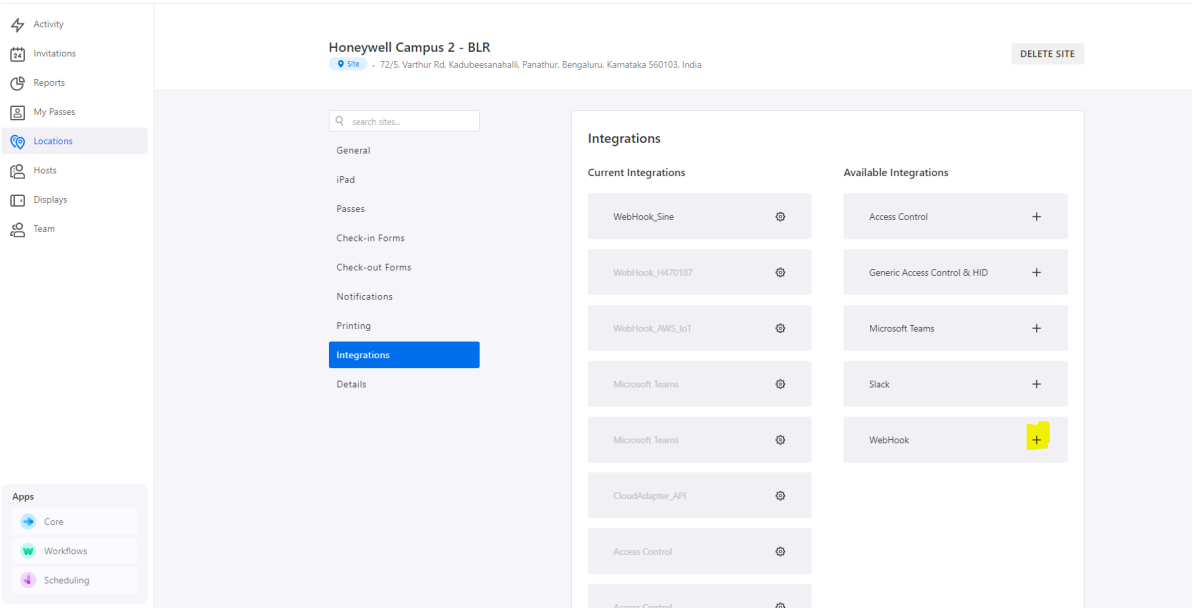
A WebHook is an HTTP-based callback function that allows lightweight, event-driven communication between two APIs (Application Programming Interfaces). Web applications use webhooks to receive small amounts of data from other applications. The Sine WebHook notifies visitor actions to the **UserService**. Contact the Sine System team to enable callbacks. This may take some time.

To configure WebHook:

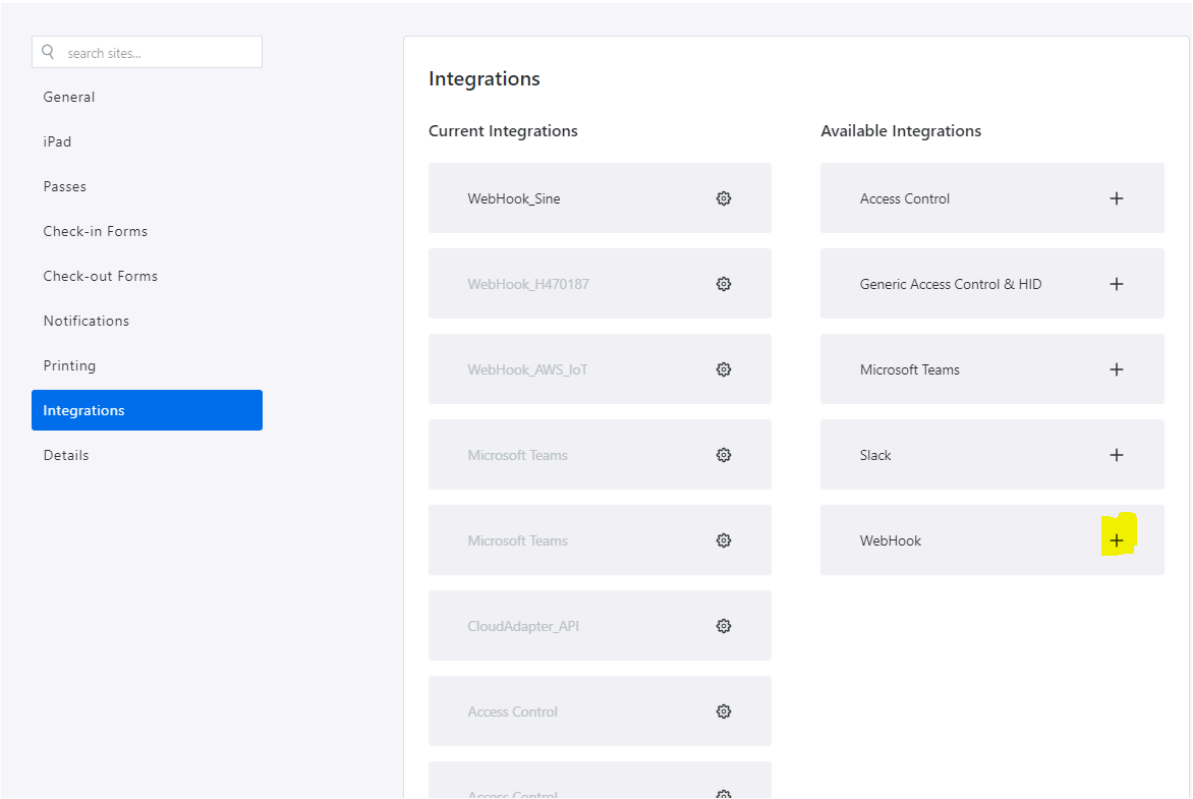
- Step 1. Log in to Sine Pro account (<https://dashboard.sine.co/#/login>).
- Step 2. From the **Sine Pro** dashboard and under the primary menu sidebar on the left-hand side, click on **Locations**.
- Step 3. If multiple sites are listed, hover over the specific site you need to perform the integration and click on **...**. Select **Settings** to open the site dashboard.



- Step 4. From the site dashboard and under the menu sidebar, click on **Integrations**.



Step 5. Under Available Integrations, click + next to WebHook to add a new WebHook.



Step 6. Configure the WebHook as follows:

Integrations

Edit your WebHook ?

Configure


Name	External ID
<input type="text" value="AWS"/>	<input type="text" value="ElgRhcptN4qhsobd"/>
URL	API Key
<input type="text" value="https://0bnxb5thbe.execute-api.us-east-1.amazc"/>	<input type="text" value="304e27f3-6e46-4b49-9032-d9b3f8892d21"/>
Rejection Message	
<input type="text" value="%EXTERNAL_REJECTION_MESSAGE%"/>	

Displayed if a Check-in Request is rejected without a rejection message

Visitor Types	Events
<input checked="" type="checkbox"/> Visitor <input checked="" type="checkbox"/> Contractor <input checked="" type="checkbox"/> Staff	<input checked="" type="checkbox"/> Check-in Request
<input checked="" type="checkbox"/> Courier <input type="checkbox"/> Student <input checked="" type="checkbox"/> Delivery	<input type="checkbox"/> Check-in Reject
<input checked="" type="checkbox"/> Admin	<input checked="" type="checkbox"/> Check-in Success
	<input checked="" type="checkbox"/> Check-out Success
	<input checked="" type="checkbox"/> Invitation Create
	<input checked="" type="checkbox"/> Invitation Update
	<input checked="" type="checkbox"/> Invitation Delete

Status ☒

Enable/Disable your integration

- **Name:** Enter a name for the WebHook.
- **External ID:** Use the Host Sync API Key. From the Sine Pro dashboard and under the primary menu sidebar on the left-hand side, click on **TEAM**  **Team**, and then navigate to the **API** tab to access the **Host Sync API Key**. If this is the first time you are using this API Key, then Generate the API key before using it.
- **URL:** **Webhook** connection URL needs to be requested from Sine Team or Tridium Team by sharing your Account details like Company and Account Id.
- **API Key:** Fill with some placeholder for now. This will be configured after the Enterprise Security is set up with the Visitor Integration Service.
- Under **Visitor Types**, select different types of visitors as needed.
- Under **Events**, select all check-in events needed to notify Enterprise Security about Sine actions. Select other Events as required.

Team

About Collaborators **API** Billing

Host Sync API Key

Your host sync API key can be used to allow the automation of Host directories in Sine.

Host sync API key ⓘ

hvj2qrcuAMFrzYk REGENERATE REVOKE

API Key for Host upload

curl -F "file=@HostsFile.csv" "https://api.sine.co/v1/host/csv-upload/api-key?remove-hosts=true&send-emails=false" -H "X-Sine-API-Key: hvj2qrcuAMFrzYk" COPY

☒ Replace all hosts with CSV (hosts not in data will be deleted)

☐ Send welcome emails to new hosts

Running host upload through your employee directory will override all hosts custom changes and will delete all hosts that have no records in your employee directory.

Step 7. To save the WebHook configuration click **SAVE**

Visitor integration in the Niagara station

These procedures configure the **VisitorIntegrationService** in the station.

- Refresh the API key.
- Establish the MQTT connection.
- Set up visitor types and access right mapping.
- Add points to the **VisitorIntegrationService**.
- Discover and subscribe points.

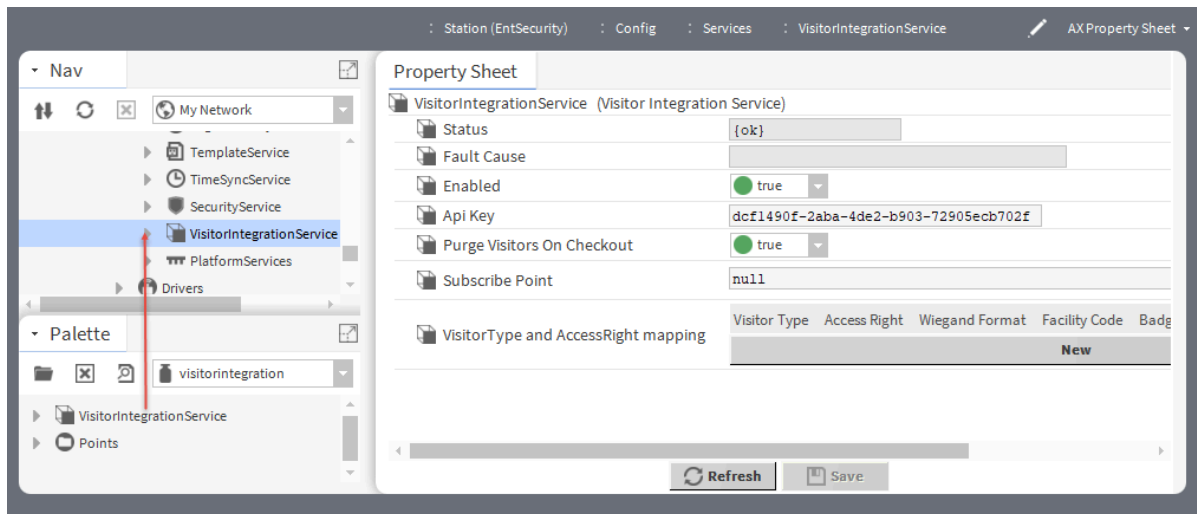
Adding the VisitorIntegrationService


This procedure adds the **VisitorIntegrationService** to the station's **Services** folder.

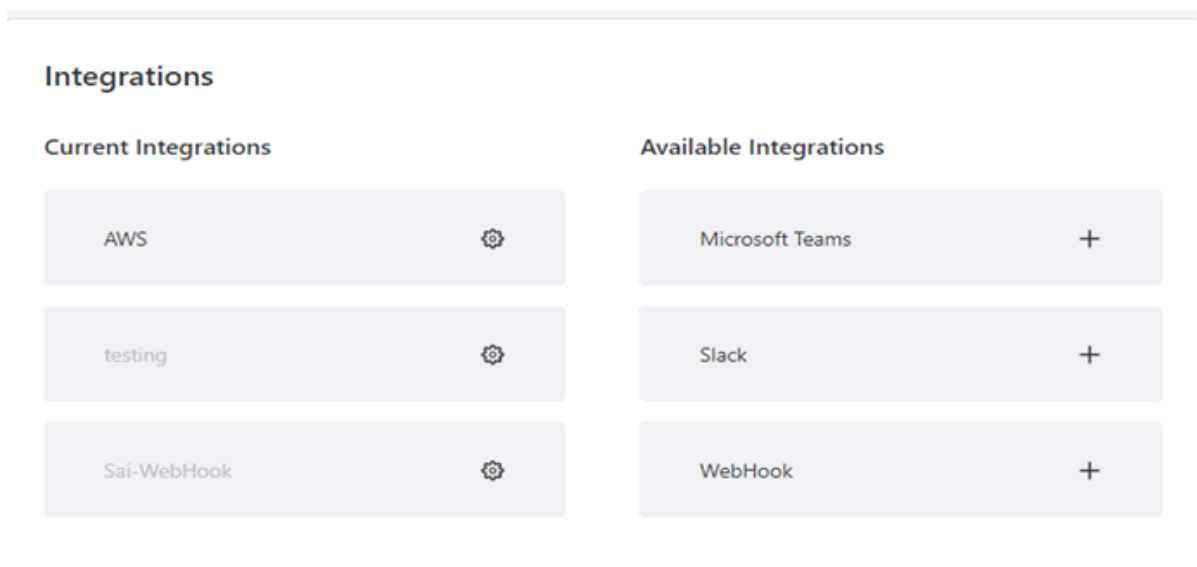
Prerequisites:

Sine Visitor Management is licensed.

- Step 1. In Niagara Workbench, open the **VisitorIntegration** palette and drag **VisitorIntegrationService** component to the **Services** folder (under **Config**) in Nav tree.



- Step 2. Right-click **VisitorIntegrationService** and click **Actions > Refresh Api Key**.
- NOTE:** Once the setup is complete, refrain from changing the API key unless required. If you change the API key, you need to do the entire setup from here on again to ensure completeness. This action provides an API key to connect to the Sine environment.
- Step 3. Double-click the added **VisitorIntegrationService** in the Nav tree to open the AX property sheet. Copy the **API Key** from the AX property sheet and return to the Sine Pro dashboard.
- Step 4. In the Sine Pro dashboard and under the primary menu sidebar on the left-hand side, click on **Locations**. Hover over the site you need to integrate, click on **...**, and select **Settings** to open the dashboard.
- Step 5. Under the site dashboard's menu sidebar, click **Integrations**. Under **Current Integrations**, click on the **WebHook** setting .



- Step 6. Under **Edit your WebHook**, enter the **API key** copied previously from the **AX Property Sheet** of the **VisitorIntegrationService** into the **API Key** field.

The screenshot shows the 'Integrations' section of the Niagara Enterprise Security web application. On the left is a sidebar with a search bar and a list of menu items: General, iPad, Passes, Check-in Forms, Check-out Forms, Notifications, Printing, and Integrations (which is highlighted in blue). The main content area is titled 'Integrations' and contains a sub-section 'Edit your WebHook' with a 'Configure' button and a help icon. The form has the following fields:

- Name:** AWS
- External ID:** ElgRhcptN4qhsobd
- URL:** https://Obnxb5thbe.execute-api.us-east-1.amazc
- API Key:** 304e27f3-6e46-4b49-9032-d9b3f8892d21
- Rejection Message:** %EXTERNAL_REJECTION_MESSAGE%

Below the Rejection Message field, there is a note: 'Displayed if a Check-in Request is rejected without a rejection message'.

Result

The **VisitorIntegrationService** is set up in Niagara station.


Setting up the Visitor Type and Access Right mapping

The **Visitor Type** and **AccessRight** mapping table determine the appropriate access rights and badge details for specified visitor types.

Prerequisites:

The Access Rights with proper Schedules that can be assigned to visitors and readers are already defined and set up in the Niagara Enterprise Security system. Please refer to Niagara Enterprise Security Guide or follow the below steps to set up Access Rights and Schedules.

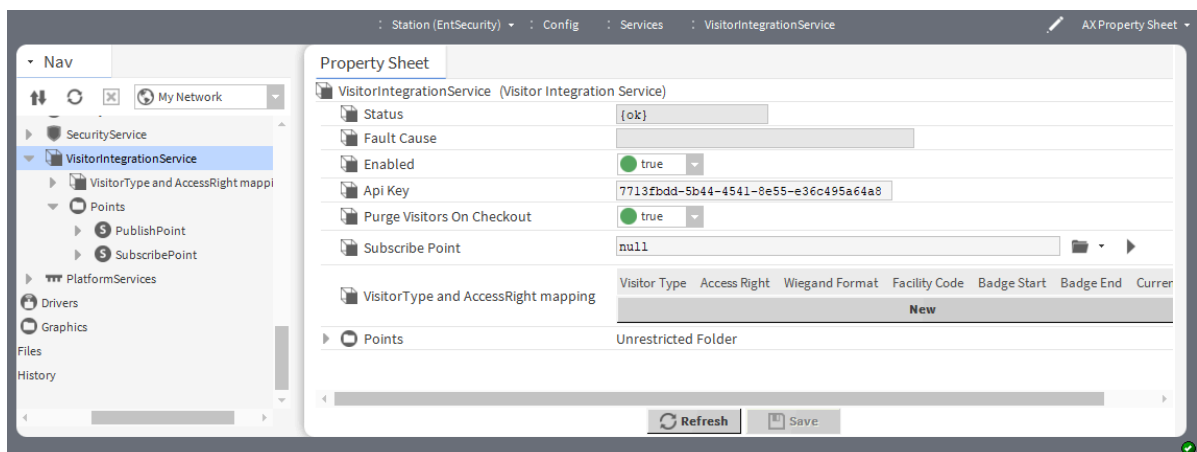
Adding Access Rights and configuring schedules

- Step 1. Navigate to Niagara Enterprise Security web application and log in with your user name and password.
- Step 2. Navigate to **Personnel > Access Rights**. Click on the  icon to add a new access right. Give any name to the access right. Add a schedule to the access right. Click on **Save**.

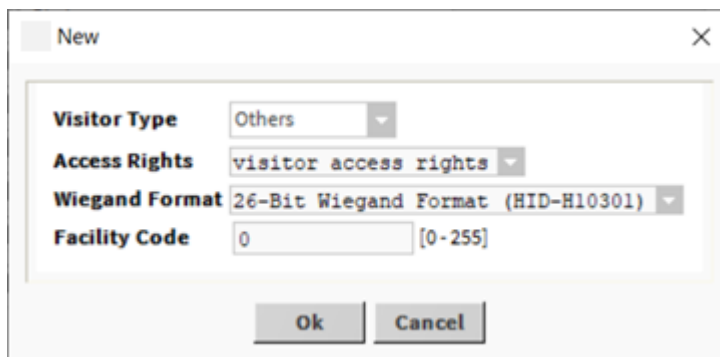


- Step 3. Go back to the Niagara Workbench and navigate to **Config > Services > VisitorIntegrationService** in Nav tree menu bar.

Step 4. Double-click on **VisitorIntegrationService** to open the **AX Property Sheet** and click **Refresh**.



Step 5. To add a new visitor, click **New** on the **Visitor Type and AccessRight** mapping property.

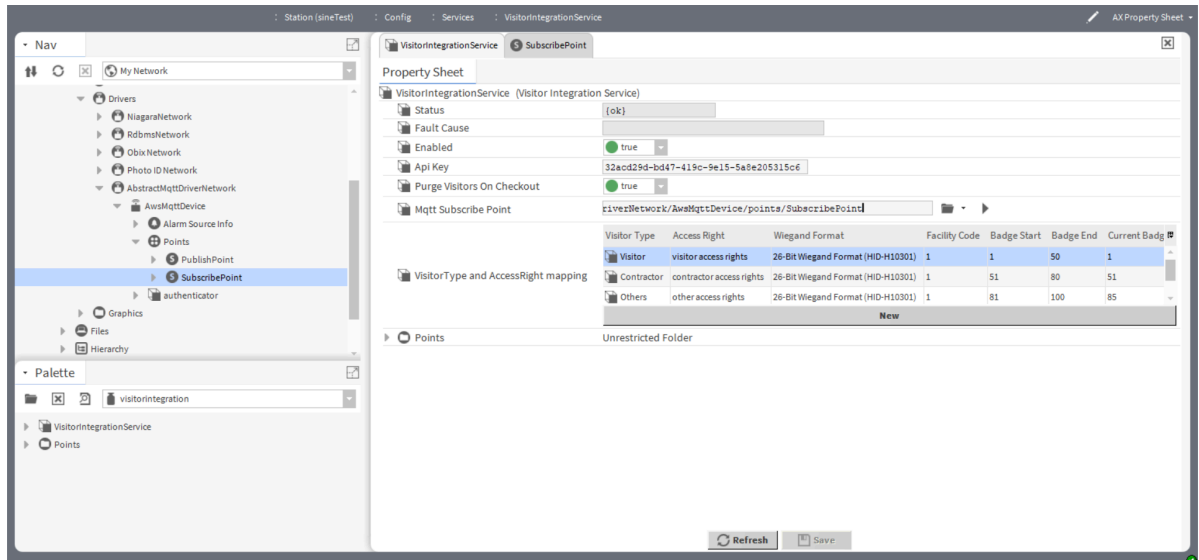


Step 6. Configure all the properties and Click **OK**.

- **Visitor Type** selects among these types: Visitor, Contractor, Staff, Courier, Others.
- **Access Rights** selects from a list of rights previously set up in the system.
- **Wiegand Format** configures the badge layout from the list of previously set up formats.
- **Facility Code** is based on Wiegand Format.

NOTE: For some common configuration issues and their solutions, refer to [VisitorIntegrationService - Configuration Problem Points and Failures](#).

NOTE: If any mapping row has access rights or Wiegand formats that no longer exist in the system or are renamed, that mapping row does not exist.



Step 7. To edit the properties, double-click the added mapping row.

Adding Points to the VisitorIntegrationService

Publish and Subscribe points configure the station to connect to the Sine application.

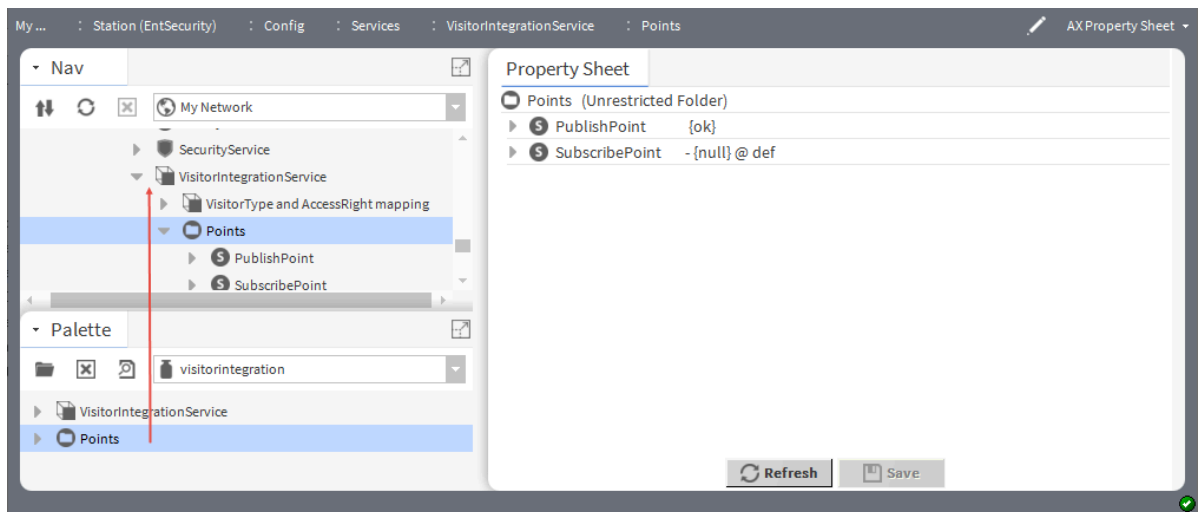
Prerequisites:

VisitorIntegrationService should be added to the Services and the visitorintegration palette is open.

Step 1. Navigate to **Config > Services** in Nav tree menu sidebar and expand the **VisitorIntegrationService**.

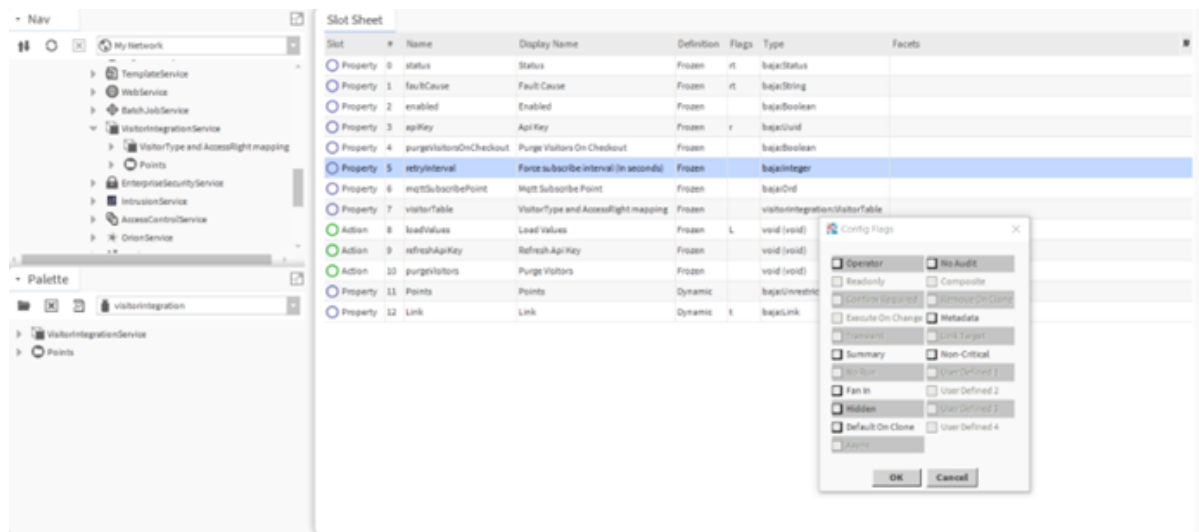
Step 2. Drag the **Points** folder from the visitorintegration palette to the **VisitorIntegrationService** container.

The points folder is added to the **VisitorIntegrationService**.



Step 3. Navigate to **Config > Services > VisitorIntegrationService**.

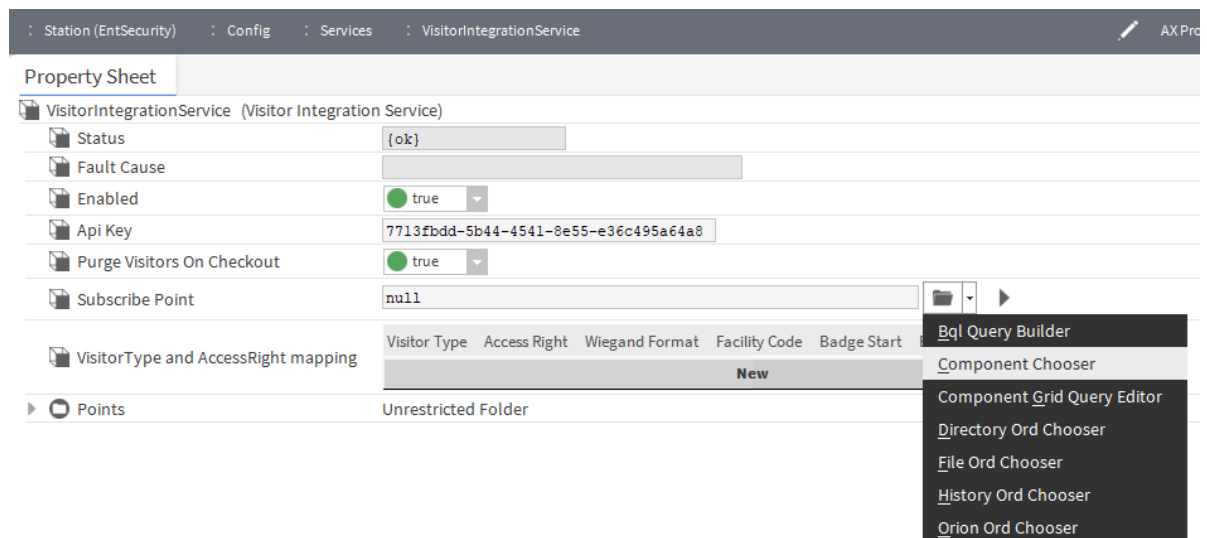
Right-click on **VisitorIntegrationService** > **Views** > **AX Slot Sheet**. Right-click on **retryInterval** > **ConfigFlags**. The **Config Flags** window opens. Remove the check mark for **Hidden**.



Step 4. Double-click on **VisitorIntegrationService** in Nav tree to open AX Property Sheet.

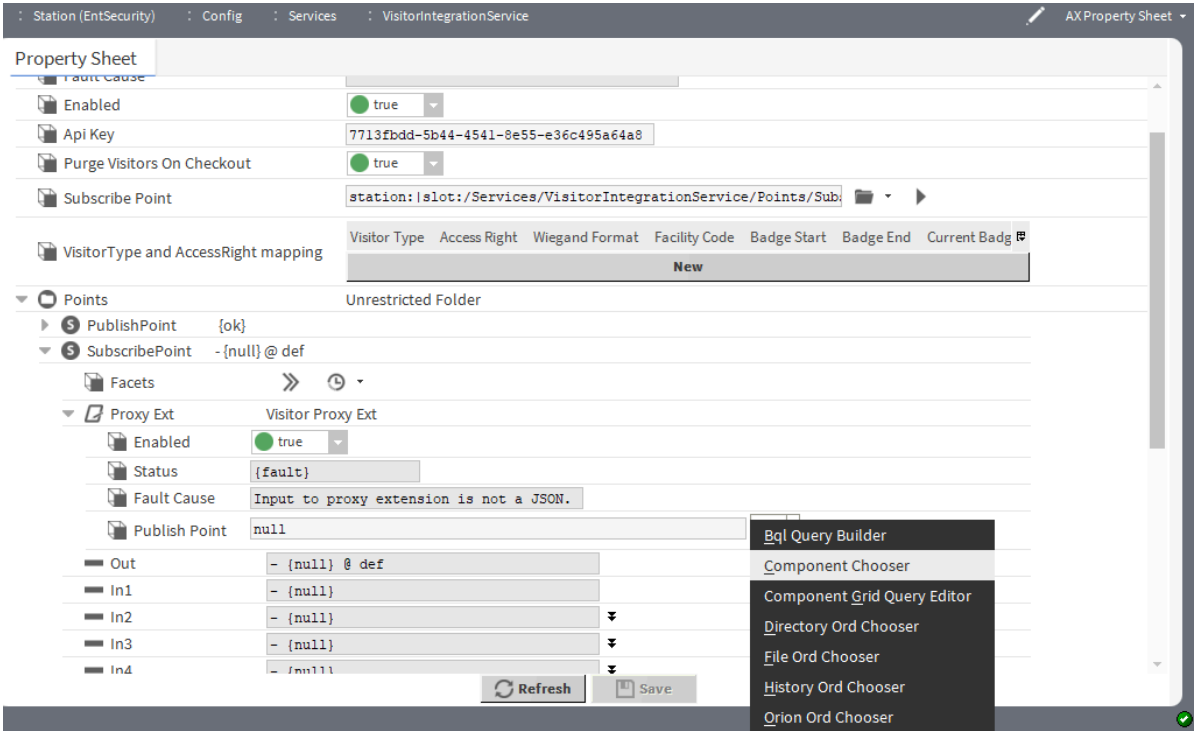
Step 5. Set **Force subscribe interval** (in seconds) to 60.

Step 6. Navigate to **Mqtt Subscribe Point** and click on the downward arrow next to the folder icon. Select the component chooser and select the ord path for subscribe point
 station:|slot:/Drivers/AbstractMqttDriverNetwork/AwsMqttDevice/points/SubscribePoint and click **Save**.



The value of ord for subscribe point is added.

Step 7. Navigate to **PublishPoint** under **Points** > **Subscribe Points** > **ProxyExt**, and then click on the downward arrow next to the folder icon. Select the component chooser and select the ord path for **PublishPoint** as station:|slot:/Services/VisitorIntegrationService/Points/PublishPoint and click **Save**.



Result

The Points are configured in the **VisitorIntegrationService** and ready for connection.

Setting up the Abstract MQTT driver network

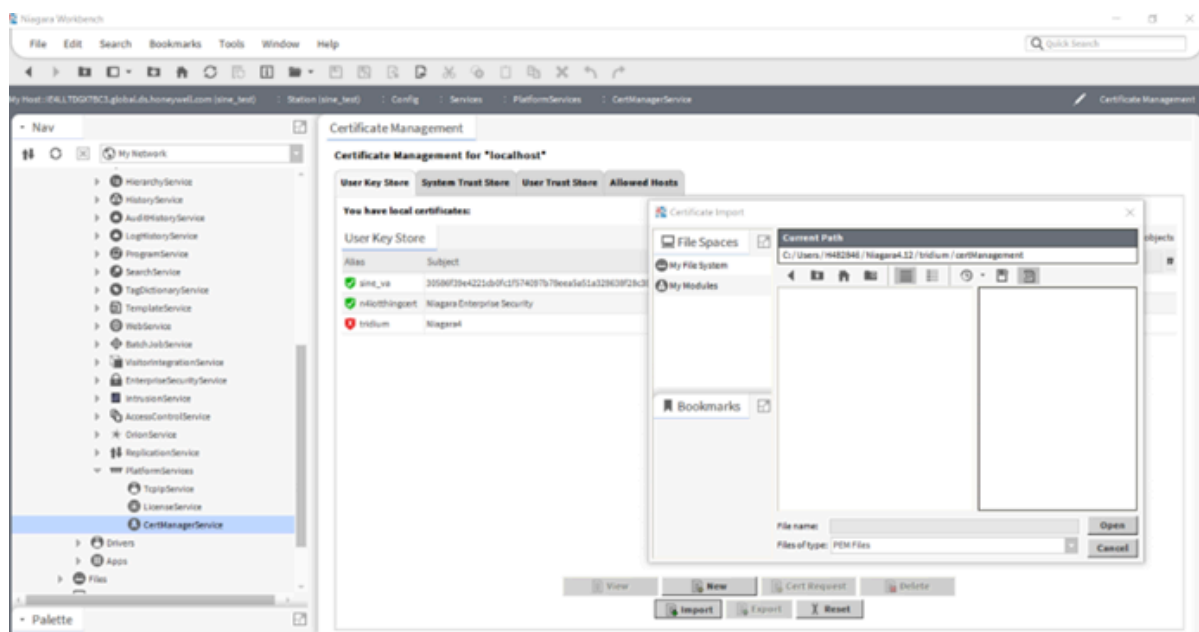
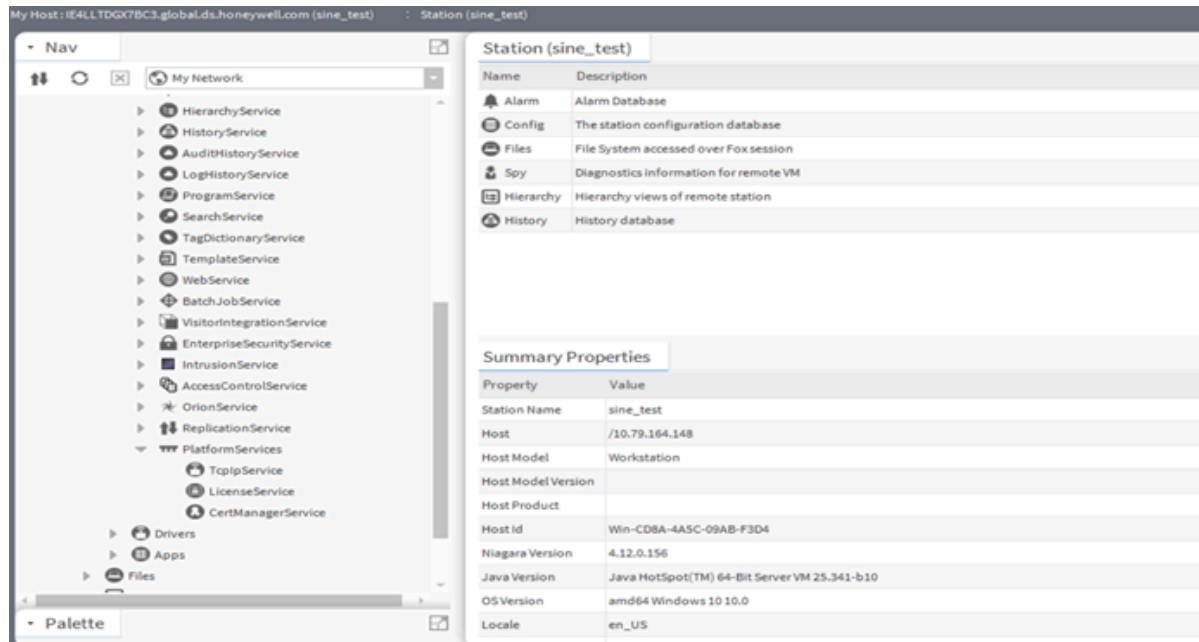
This procedure explains how to establish the connection between Niagara and Sine application.

Prerequisites:

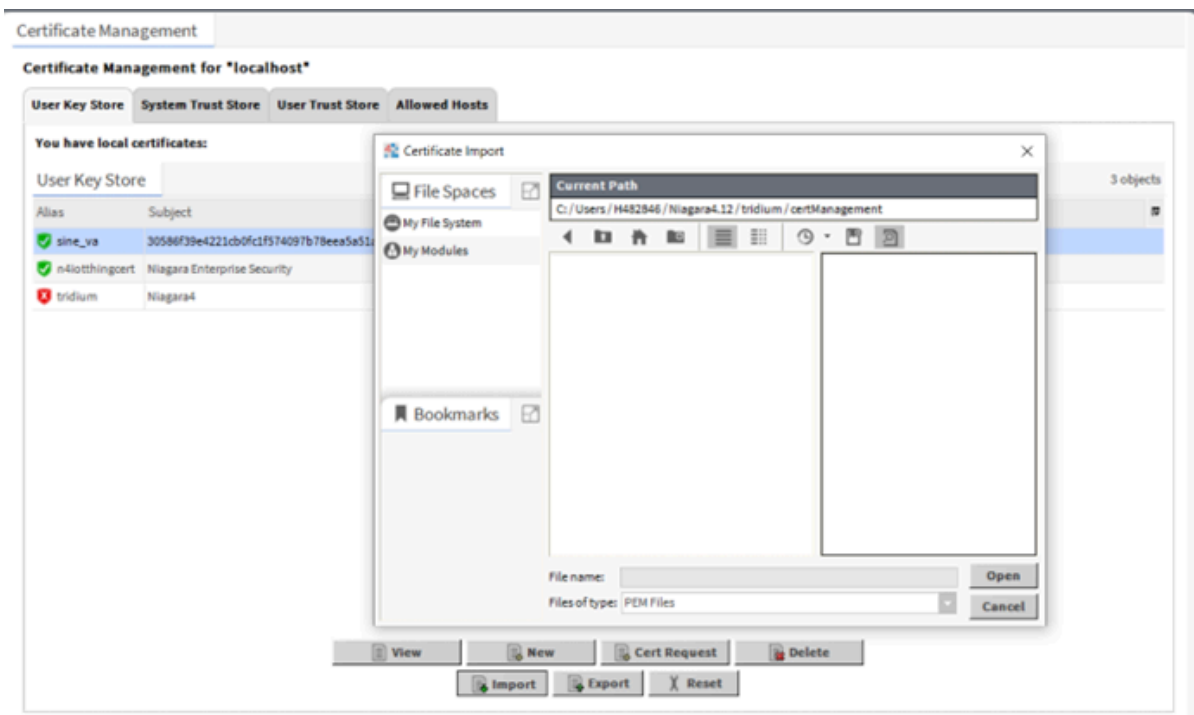
The Niagara station is licensed for **AbstractMQTT** driver, and the device certificate (AWSCert.crt) is imported into Niagara station.

Importing device certificate (AWSCert.crt)

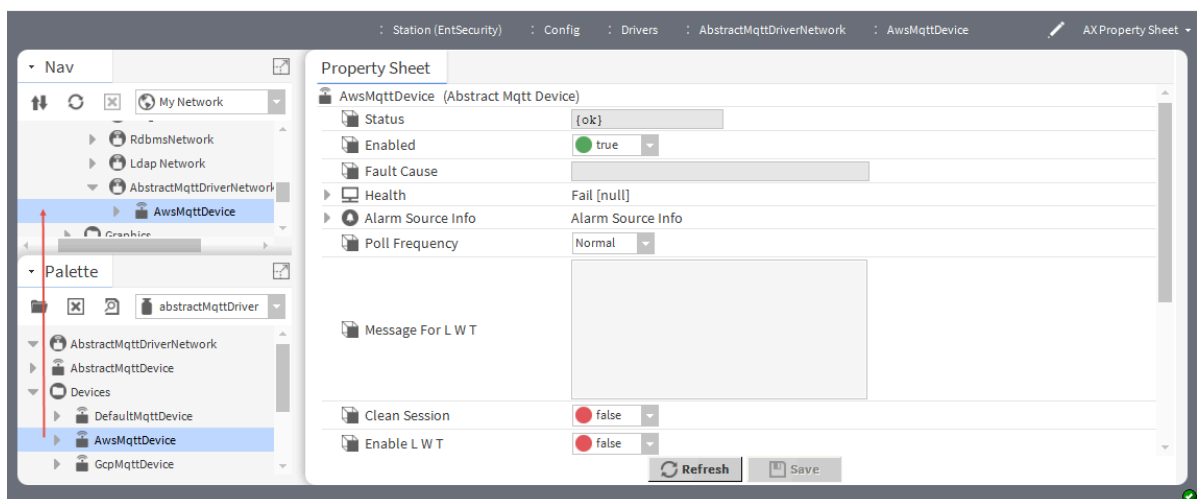
- Step 1. Expand the station property in Workbench and under the Nav tree menu sidebar and navigate to **Config > Services > Platform Services > CertManagerService**.



Step 2. Click on **User key Store** tab and select **Import** button and import the device certificate (AWSCert.crt) shared by Tridium team.

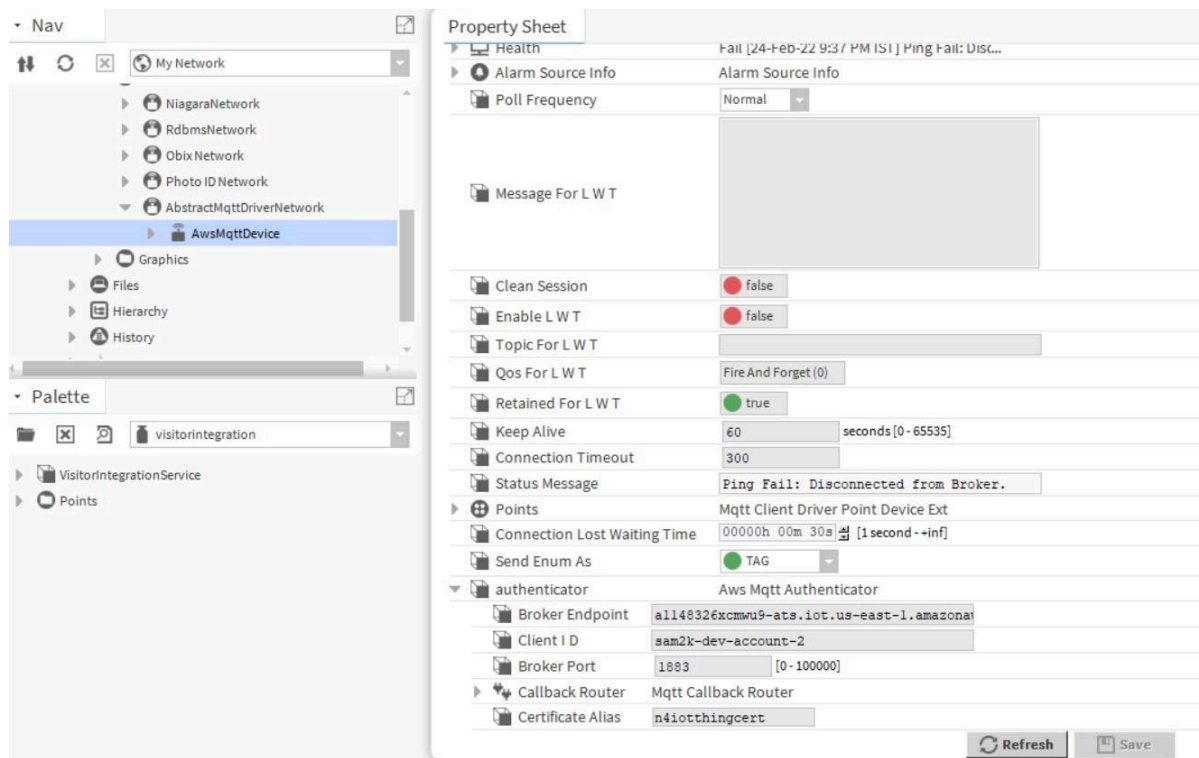


- Step 3. Click on the open palette from the **Palette** menu sidebar and search for **AbstractMqttDriver**. Drag the **AbstractMqttDriverNetwork** component from the **AbstractMqttDriver** palette to the **Drivers** folder (under **Config**) in the Nav tree.
- Step 4. Under the **AbstractMqttDriver** palette, expand the **Devices** folder and drag the **AwsMqttDevice** component from the palette to the added **AbstractMqttDriverNetwork** in the Nav tree.

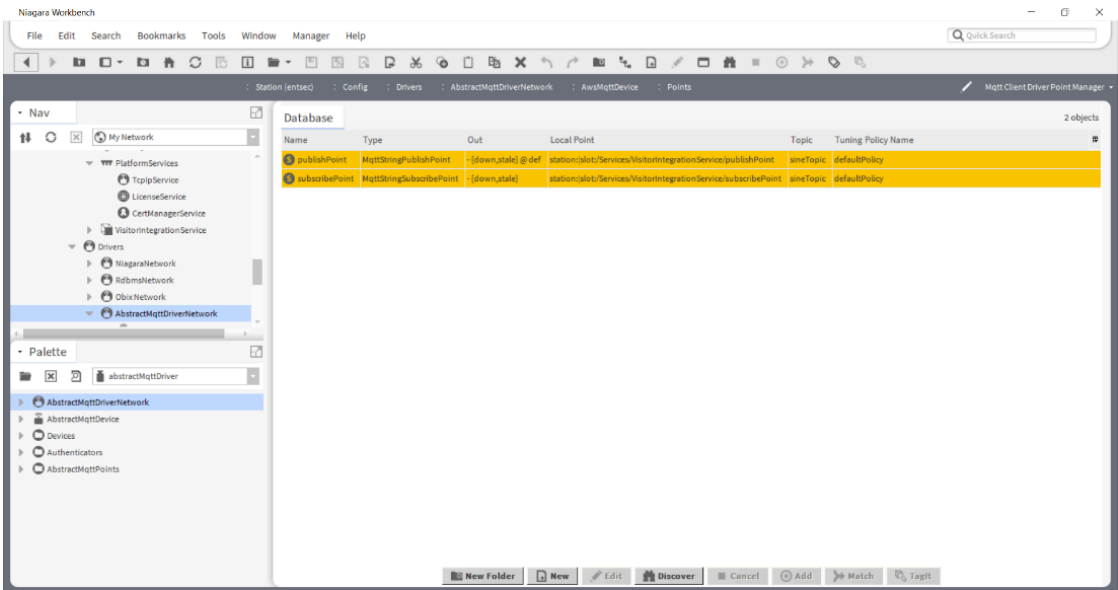


- Step 5. Double-click on the added **AwsMqttDevice** in the Nav tree to open the **AX** property Sheet. Configure the **AwsMqttDevice** as follows;
- Change **Keep Alive** to 65535
 - Expand the authenticator in the property sheet and add **Broker Endpoint** (This needs to be provided by the Tridium or Sine Team).

- c. Add a unique **Client ID** in the authenticator. Add the API Key from **VisitorIntegrationService** here due to its uniqueness.
- d. In **Certificate Alias** and from the drop-down list, select the device certificate (AWSCert.crt) previously provided and added to the **User Key Store** in the **PlatformServices**



- Step 6. Click **Save**. Right click on **AwsMqttDevice**, click **Actions** and then **Connect**.
If the connection is successful, the **Status Message** property value shows **Connected**.
- Step 7. Expand **AwsMqttDevice > Points** and click on **Discover**.
- Step 8. From the discovered points, pull the subscribe point and publisher point to database and edit the parameters as follows:
 - a. For publish point, set **Type** to **MqttStringPublishPoint**. Add topic as **APIKEY/sine topic-ack**. Here **APIKEY** is the api key stored in the **VisitorIntegrationService**.
 - b. For subscribe Point, **Type** will be **MqttStringSubscribePoint**. Add topic as **APIKEY/sine topic**. Here **APIKEY** is the api key in the **VisitorIntegrationService**. Please note that the topic is case sensitive



Step 9. Right click the **Proxy Ext** of subscribe point and click **Actions > Subscribe**.

Checking in a visitor

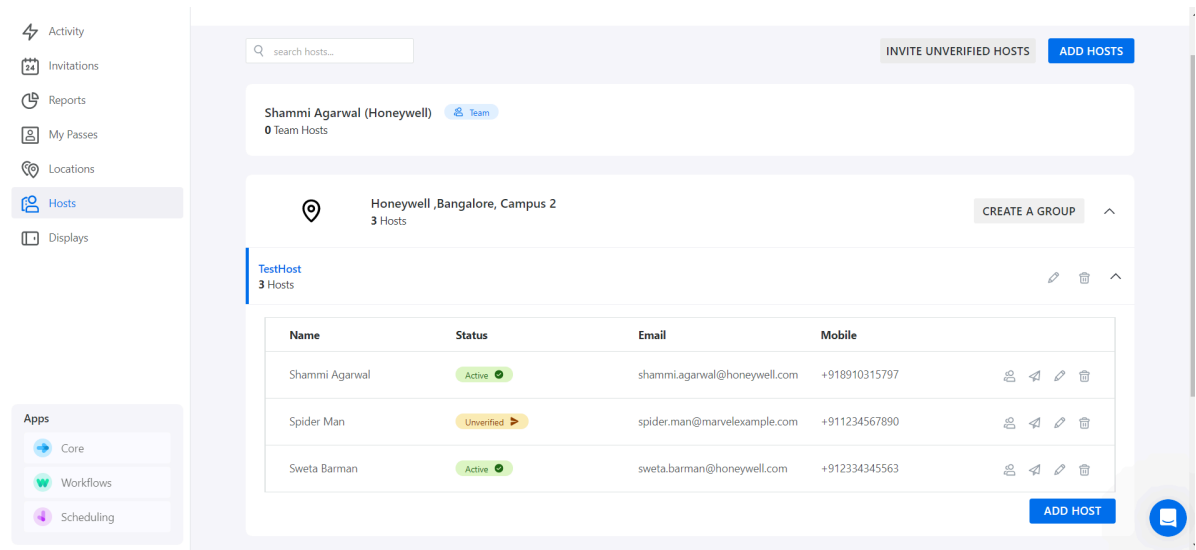
This procedure describes how to check in a visitor.

Prerequisites:

Login to the Sine dashboard, open the Sine pro-Homepage and create the required Host for Check-In Successful.

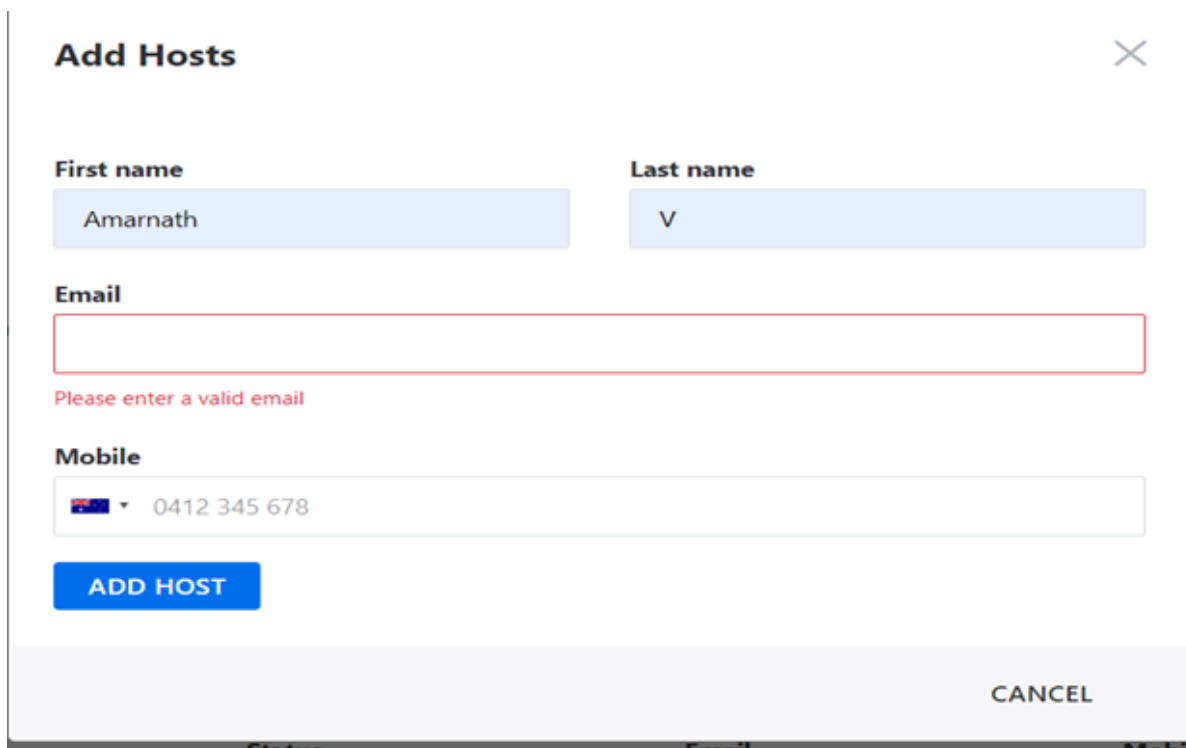
Create Host for Check-In

Step 1. Navigate to the Sine Pro dashboard. Under the primary menu sidebar on the left-hand side, click on Hosts to open the Host dashboard.



Step 2. Click on **Add Hosts**, enter the Host details as required, and then click on **ADD HOST** to save the

new entries.



The image shows a modal dialog box titled "Add Hosts" with a close button (X) in the top right corner. The dialog contains four input fields: "First name" with the value "Amarnath", "Last name" with the value "V", "Email" which is empty and has a red border and a red error message "Please enter a valid email" below it, and "Mobile" with a dropdown menu showing a flag and the number "0412 345 678". Below the input fields is a blue button labeled "ADD HOST". At the bottom right of the dialog is a "CANCEL" button.

First name	Last name	Email	Mobile
Amarnath	V		0412 345 678

Step 3. Go to the Sine ProDashboard and click [CHECK-IN](#) .

The **Visitor Check-in** window opens.

Visitor Check-in

First Name

Last Name

Please enter your first name

Company (optional)

Email (optional)

Mobile (optional)

081234 56789

Site

Honeywell ,Bangalore, Campus 2

Visitor Type

Visitor

Host

(TestHost)

☐ Check-in another guest

CANCEL

NEXT

- Step 4. Complete the form and enter the Visitor's **First Name** and **Last Name** as mandatory properties. Select the visitor type from **Visitor Type** drop-down list and choose the appropriate Site. Then click **Next**.
- Step 5. Enter the badge number preceded by b- in **Badge Number** property (example: b-12345). The badge number can be an existing number already enrolled in the Enterprise Security application and available to assign or it can be any arbitrary number between 1 to 5 digits and less than 65535.

Please read carefully and complete the following questions

Badge (Add "b-" before the badge number) *

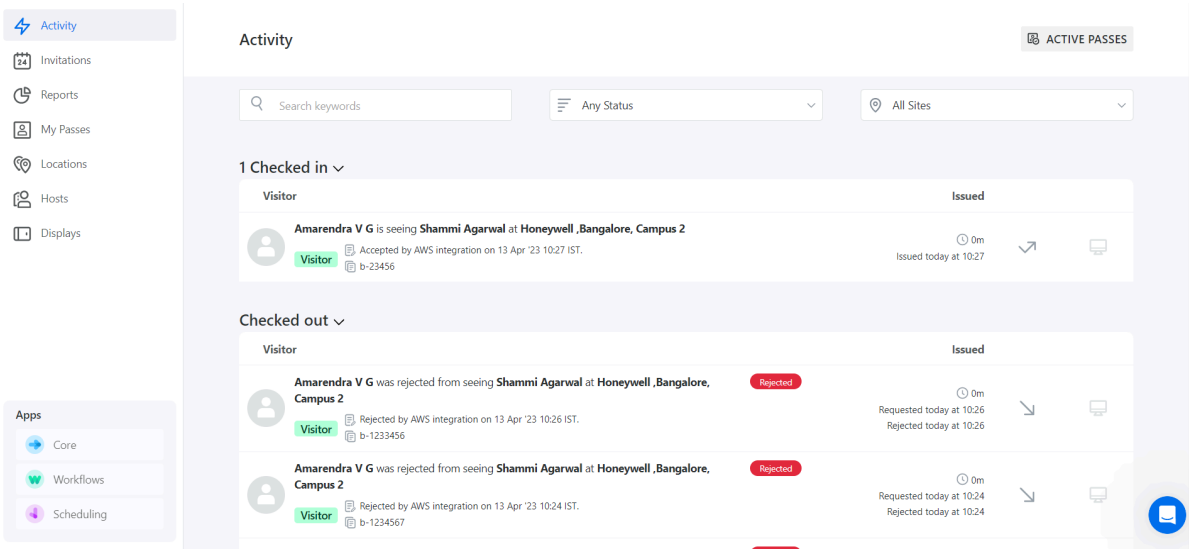
b-12345

☐ Check-in another guest

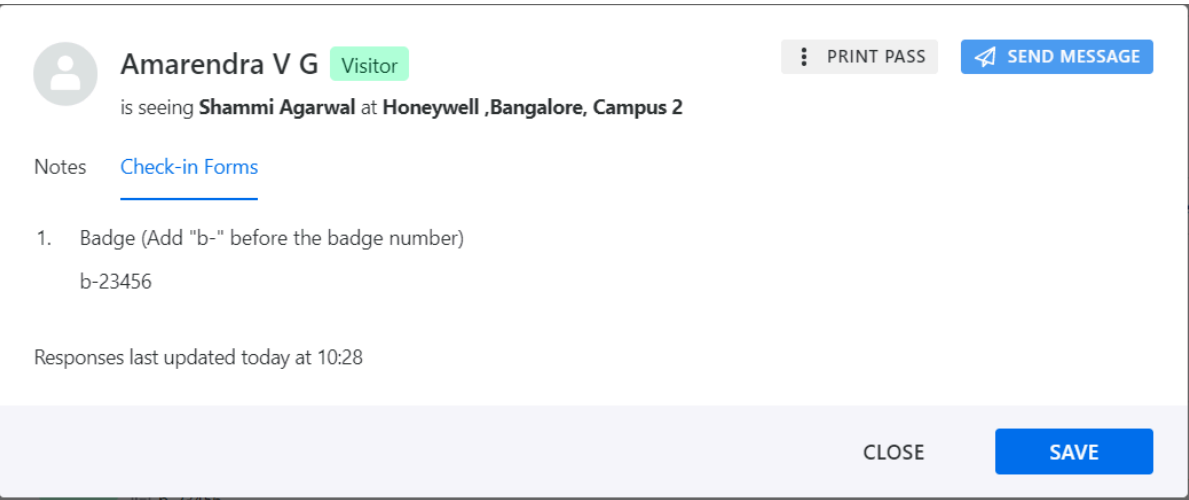
BACK

CHECK-IN

Step 6. Click on **CHECK-IN**. A checked-in message will appear under Activity in the Sine Pro dashboard if the visitor check-in is successful.



Step 7. After check-in, double-click on the checked-in visitor's name in the Activity dashboard to view notes, badge details, and print passes.



Step 8. Log in to the NiagaraEnterprise Security web application to verify the visitor is successfully checked in. Navigate to **Personnel** and click on **People**. The checked-in visitor is listed under **People**.



The visitor is successfully checked in Enterprise Security.


Checking a visitor out

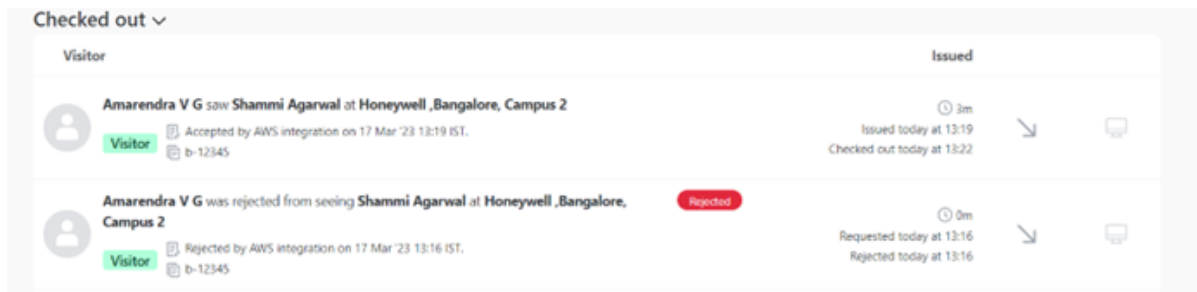
Once the visitor checks out they no longer available on the checked-in list. Checking a visitor out may or may not purge the visitor from the Sine system depending on how you set up the **VisitorIntegrationService**.

Prerequisites:

Login to Sinepro dashboard.

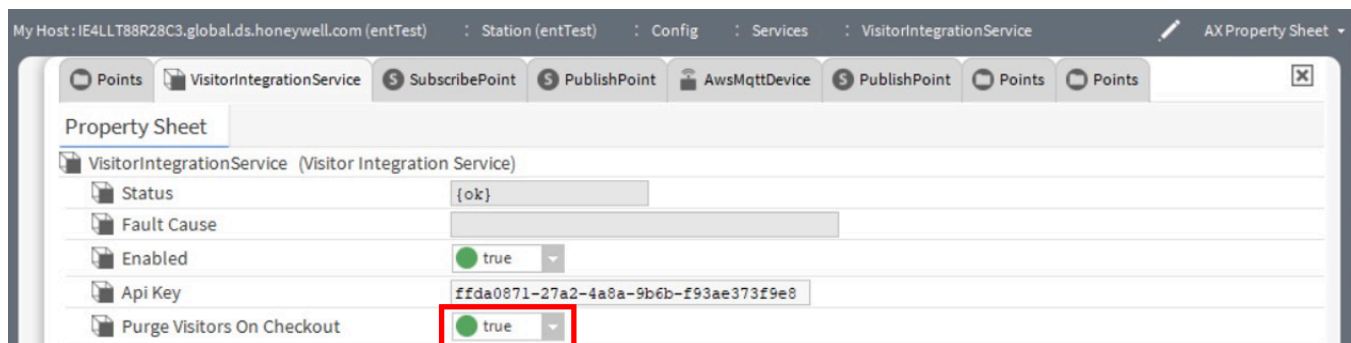
On the Enterprise Security side, configure the **Purge Visitors On Checkout** property in the **VisitorIntegrationService** for checkout.

- Step 1. Navigate to **Activity**, list of checked in user is displayed.
- Step 2. To check out the required user select  .
The user details are listed under checked out group.




Purge Visitors On Checkout enabled

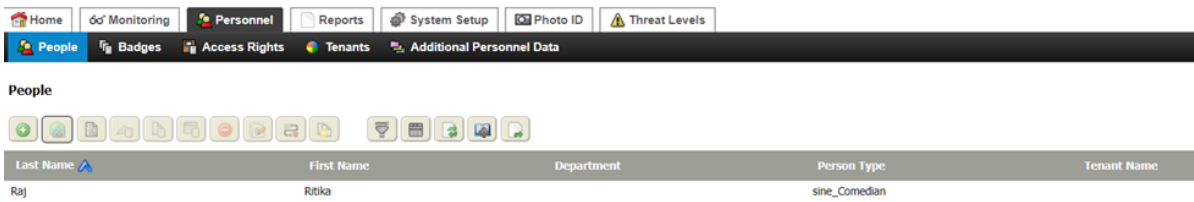
When this property is enabled (set to True) in Workbench, the visitor will be purged from the NiagaraEnterprise Security system upon being checked out in the Sine dashboard. The system will free up the associated badges and make them available for reuse.



Prerequisites:

The Badge is free from Entsec.

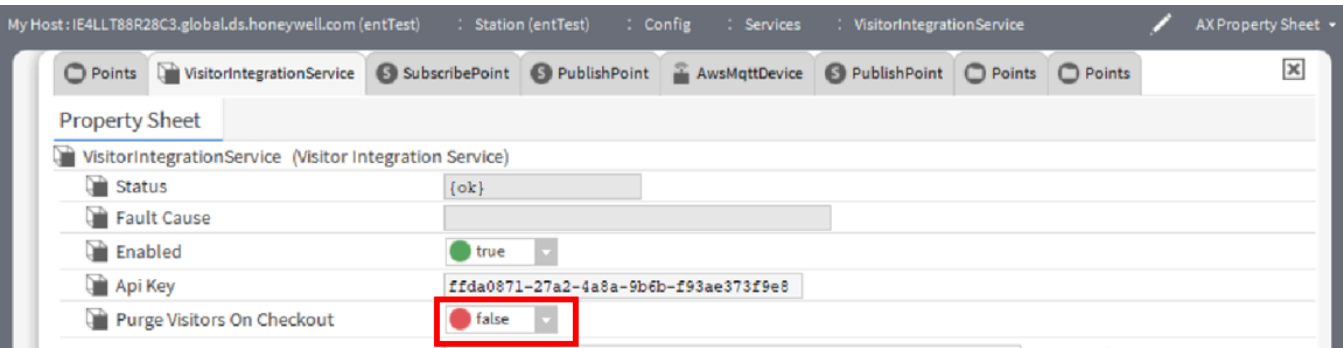
- Step 1. Click on  in Sine dashboard to check out the visitor.
- Step 2. Go to the NiagaraEnterprise Security web application and navigate **Personnel > People**. The visitor is removed from the people list, and their associated badges are free and can be re-assigned to another visitor/user.




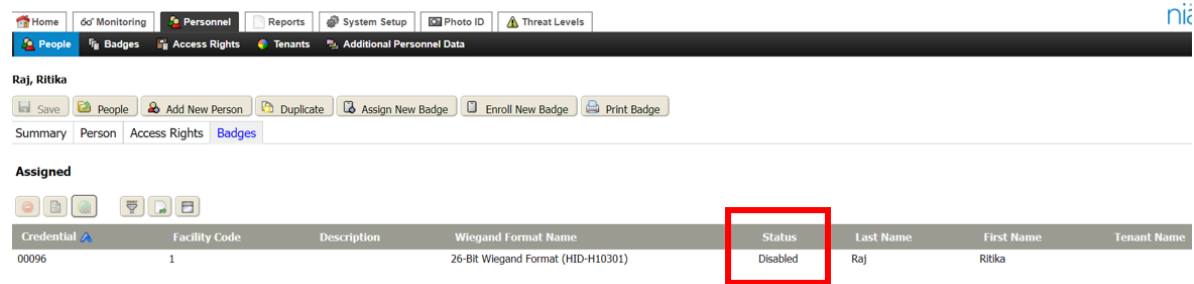
After a check out is complete, audit logs are displayed.

Purge Visitors On Checkout disabled

When this property is(set to False) in Workbench, the visitor will NOT be purged from the NiagaraEnterprise Security system upon being checked out in the Sine dashboard. Still, their associated badges will be disabled and cannot be reused.



- Step 1. Click on  in Sine dashboard to check out the visitor.
- Step 2. Go to the NiagaraEnterprise Security web application and navigate to **Personnel > People**. The visitor still exists under the people list, but their associated badges are disabled and cannot be re-assigned to another visitor/user.

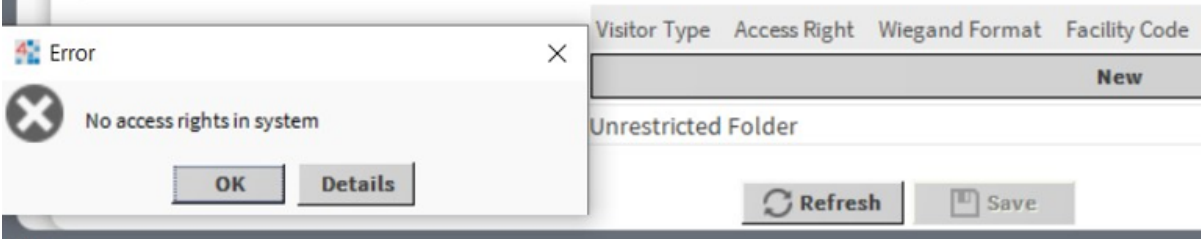


After a check out is complete, audit logs are displayed.

VisitorIntegrationService - Configuration Problem Points and Failures

Topics covered in this section are some common configuration problems and their solutions.

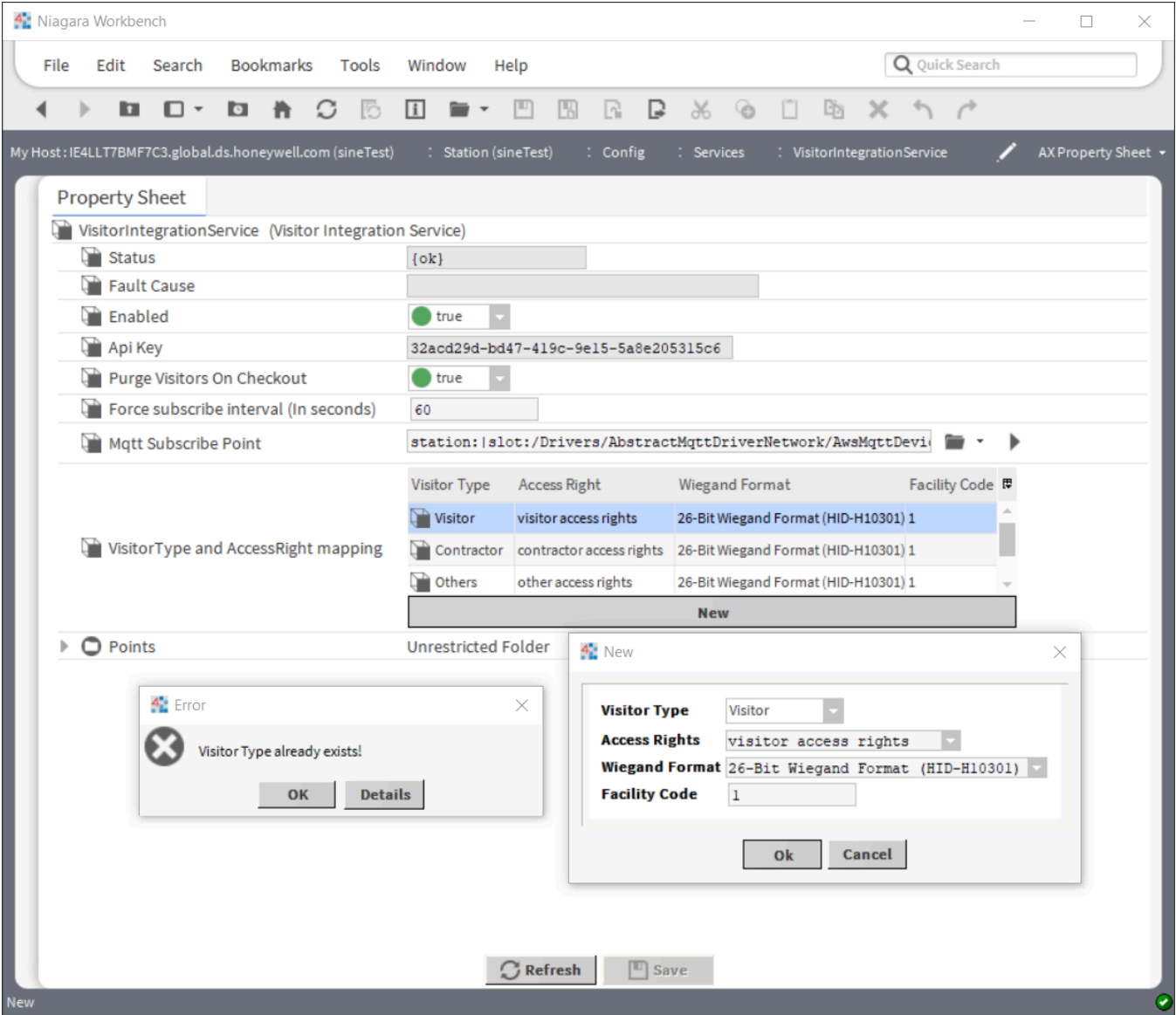
Error: No access rights in system or No Wiegand formats in system.



The user receives this error when trying to add a visitor while no access rights or Wiegand formats are set up in the system.

Solution: First add access rights to the system, then refresh the service. If this issue persists even after you add an access right and Wiegand format, , invoke the **Load Values** action.

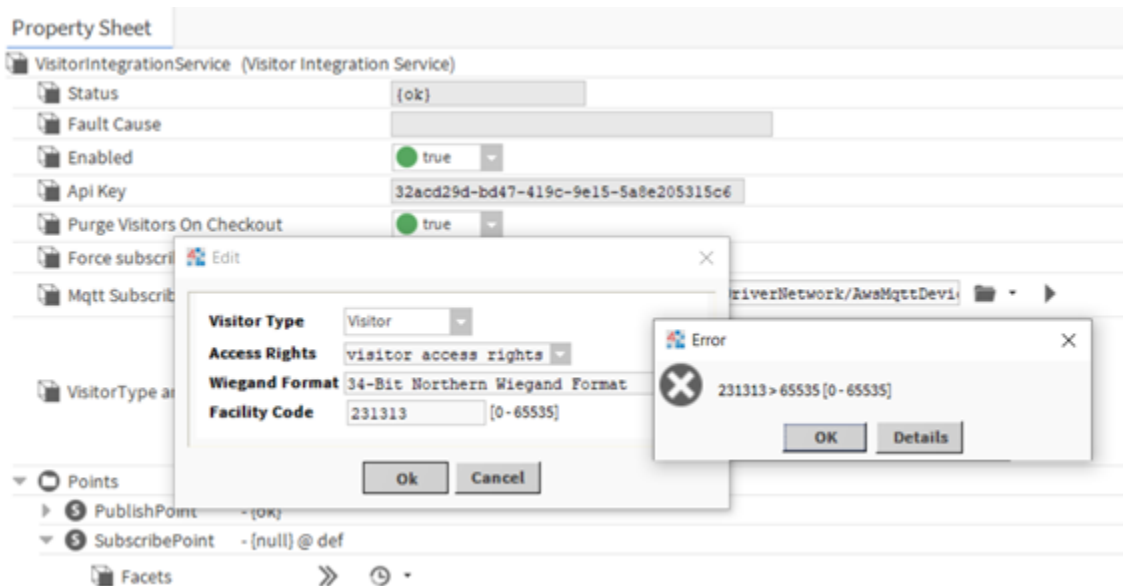
Error: Visitor Type already exists.



The user receives this error when trying to create a new visitor type while there is already a row in the table with the same visitor type.

Solution: To configure the visitor type, edit the previously existing row as visitor type must be unique in this mapping.

Facility code out of range.



The user receives this error when they enter the facility code, which is not in the range with the Wiegand formats for the badges.

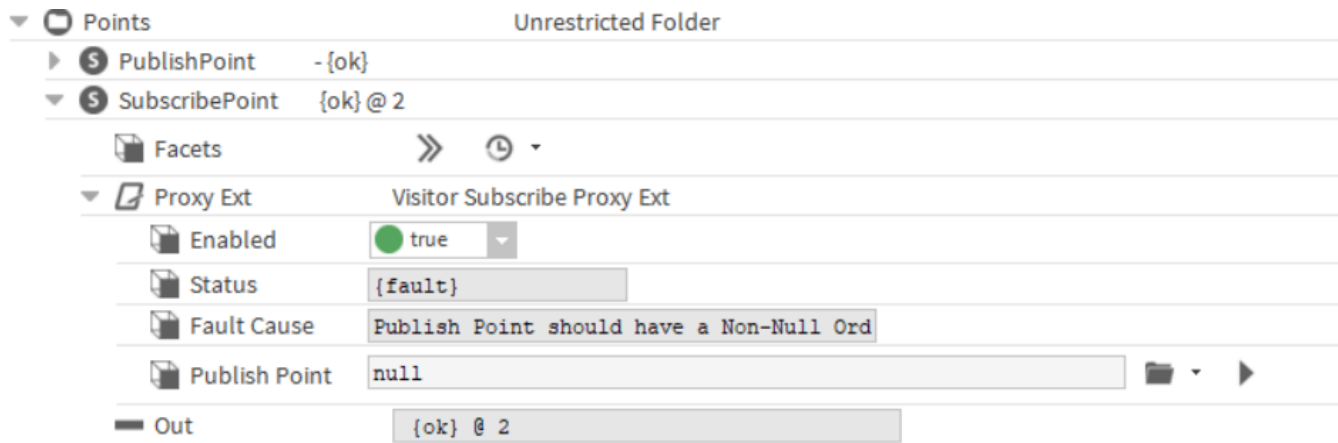
Solution: Provide a facility code that is in range with respect to the Wiegand format you are planning to use.

Access right and Wiegand format are not available in the drop-down list.

Even though the user has added at least one access right and one Wiegand format to the system, those options are not available in the drop-down list.

Solution: Right-click **VisitorIntegrationService**, navigate to **Actions** and Invoke action **Load Values** and then refresh the service once.

Visitor Subscribe Proxy Ext Failure:



The Visitor Subscribe Proxy Ext (under **Points > SubscriptionPoint > Proxy Ext**) is at Fault due to Publish Point should have a Non-Null Ord:

Solution: In the Publish Point property of the visitor proxy ext, set the value as the ord for the publish point in the **Visitor Integration Service > Points**.

The Visitor Subscribe Proxy Ext **Points > Subscribe Point > Proxy Ext** is at Fault due to Publish Point type should be a StringPoint:

▼ **SubscribePoint** - {null} @ def

Facets >> ⌚ ▼

▼ **Proxy Ext** Visitor Subscribe Proxy Ext

Enabled ☒ true ▼

Status {fault}

Fault Cause Publish Point type should be a StringPoint

Publish Point station:|slot:/Sweta/NumericWritable

Out - {null} @ def

Solution: In the Publish Point property of the visitor proxy ext, the ord should be pointing to a String Point. Change the ord to the publish point provided in the palette for visitorintegration.

The Visitor Subscribe Proxy Ext under (**Points > Subscribe Point > Proxy Ext**) is at Fault due to Input to proxy extension is not JSON.

▼ **Proxy Ext** Visitor Subscribe Proxy Ext

Enabled ☒ true ▼

Status {fault}

Fault Cause Input to proxy extension is not a JSON.

Publish Point station:|slot:/Services/VisitorIntegrationService/Points/Pub

Out - {null} @ def

In1 - {null}

The Visitor Subscribe Proxy Ext (under Points->SubscriptionPoint->Proxy Ext) is at Fault due to "Input to proxy extension is not JSON"

Solution: If you get this fault just after the initial setup of visitor integration or when you restart the station, don't worry about your setup. It is working fine. This is an extra validation. The fault goes away after one successful check in happens. If this is not your initial setup of visitor integration, check all the input slots for the Subscribe point. There should be one link mark from the MQTT subscribe point. Apart from that, if there are any link marks, then this error may occur.

Chapter 4. Badge management

Making and assigning badges is documented in this guide as well as in the *Operator's Guide*.


Each employee requires a badge. In most companies, each visitor also requires a badge. In addition, one or more badges may be used to initiate a threat level.

Creating a single badge (manual entry)

Manually entering a badge should be done when you need to create only one badge.

Prerequisites:

You are working at the Supervisor station with admin privileges.


- Step 1. Select **Personnel > Badges**.
The Badges view opens.
- Step 2. Click the Add button ().
The Add New Badge view opens.
- Step 3. Complete the properties and click the **Save** button.
The system saves the badge and opens the Edit Existing Badges view, Summary tab.
- Step 4. Make any additional edits and click the **Save** button.

Creating multiple badges (batch-create)

You can batch-create a group of badges that can have common values the following properties: **status**, **format**, **tenant**, **issue date**, **expiration date**.

Prerequisites:

You are working at the Supervisor station.


- Step 1. From the home view, select **Personnel > Badges**.
The Badges view opens.
- Step 2. Click the Batch Enroll button ().
The Batch Enroll Badges view opens.
- Step 3. Complete the properties that are to be shared for all badges scanned, including **Description**, **Wiegand Format**, **Status**, **Issue Date**, **Expiration Date**, **Owner**, **Tenant**, and **Enrollment Reader**.
- Step 4. Swipe a set of cards (a batch) one at a time.
As you swipe each card, the card data displays in the **New Badges** property.
NOTE: If badge numbers do not appear, the corresponding Wiegand format has not been defined.
- Step 5. To complete the batch-badge creation process, click the **Save** button.
The system saves the badges, and opens the Edit Badges view. The new badges appear in the table of badges.

Manually assigning a new badge

This procedure describes how to assign a badge that is not already created (new badge), without using the reader to scan it in.

Prerequisites:

You are working at the Supervisor or badge creation station with admin privileges.


- Step 1. Select **Personnel**.
The People view opens.
- Step 2. Select the person record that the badge is to be assigned to and click the Hyperlink button ().
The edit view for the person opens with the person's name at the top of the view.
- Step 3. Select the Badges tab and click the **Assign New Badge** button.
The Add New Badge view opens. This tab is the active tab, by default, when the view initially opens. The tab includes the following properties to enter or choose information that applies to the new badge record:
- Step 4. Fill in the properties.
- Step 5. To assign the new badge with the current settings, click the **Save** button.
The system assigns the badge to the person and displays the new badge in the edit existing badge view.

Enrolling from a reader to assign a new badge

This procedure describes how to assign a badge that is not already created (a new badge), using a reader to scan it in.

Prerequisites:

You are working at the Supervisor station.



- Step 1. Select **Personnel**.
The People view opens.
- Step 2. Select the personnel record that the badge is to be assigned to and click the Hyperlink button ().
The Edit Person view opens with the person name at the top of the view.
- Step 3. Select the Badges tab and click the **Enroll New Badge** button.
The Enroll New Badge view opens.
- Step 4. Complete the properties.
NOTE: You have to assign an Enrollment Reader before you can scan a badge to complete some of the properties.
- Step 5. Scan the badge at the designated enrollment reader.
The badge Id number appears in the **Scanned Badge** property and one or more format options appear in the format pane.
NOTE: If the badge number does not appear, the corresponding Wiegand format has not been defined.
- Step 6. Click the **Save** button.
- Step 7. Click the **OK** button to assign the badge.
The badge is assigned to the person and the new badge displays in the Edit Existing Badge view.

Assigning an existing badge

A badge is required at most facilities to enter and exit buildings. This procedure describes how to assign a badge that is already created (existing badge), without using the reader to scan it in.

Prerequisites:

You are working at the Supervisor station with admin privileges. The badge to assign to the person exists in the database. You just created the new person record and are continuing with setting up the new person or you are editing an existing person and have already double-clicked the person's name in the People view.

- Step 1. Click the Badges tab.
The Badges discovery view opens.
- Step 2. Click the Assign Mode button ().
The system populates the Unassigned pane with all available unassigned badges.
- Step 3. Select the badge to assign to the person and click the Assign button ().
The system assigns the badge to the person by moving it from the Unassigned pane to the Newly Assigned pane.
- Step 4. To update the person's record in the database, click the **Save** button at the top of the view.
The Summary tab opens with a summary of the properties you just updated.

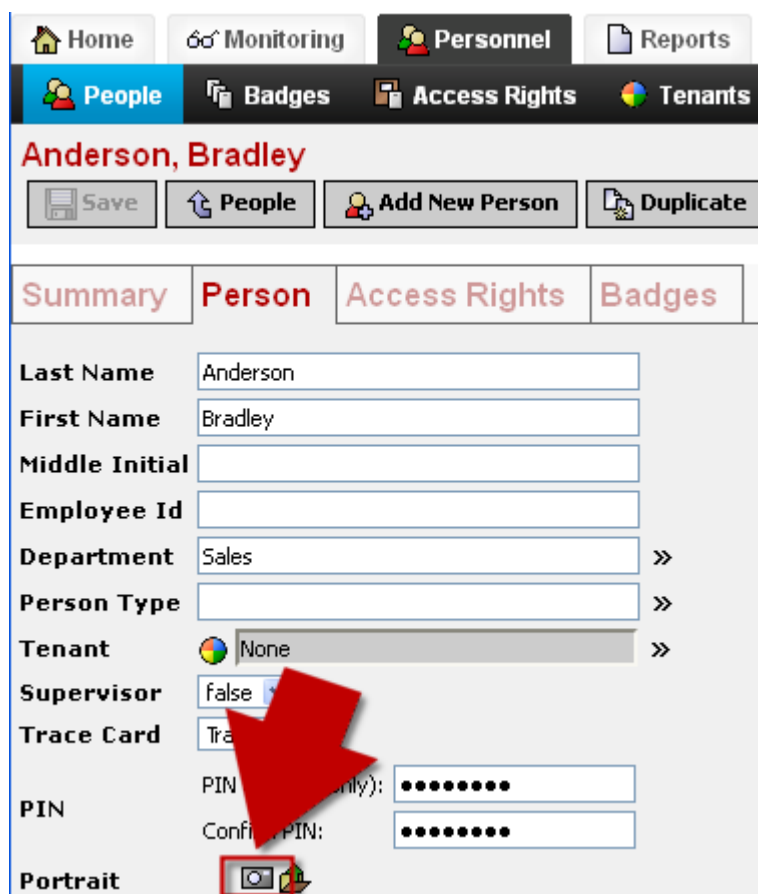
Capturing a photo and associating it with a person

You may capture a photo using a portrait camera connected to the Photo ID station, or use any photo taken by any camera and located anywhere as long as it is stored as a .jpg or .png file.


Prerequisites:

The browser used to run the system must be running in the Photo ID station to which the USB portrait camera is connected.

- Step 1. From the home view, click **Personnel > People**, double-click a person's row in the table, and click the Person tab.
The Person view opens.



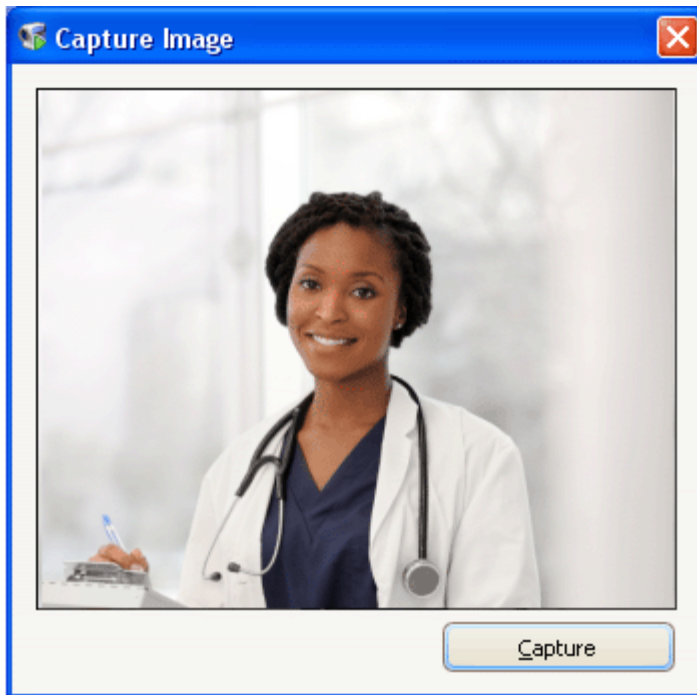
The screenshot shows the 'Personnel > People' view in the Niagara Enterprise Security Facility Manager. The 'Person' tab is selected, displaying the details for Bradley Anderson. The form includes fields for Last Name, First Name, Middle Initial, Employee Id, Department, Person Type, Tenant, Supervisor, Trace Card, PIN, and Portrait. A red arrow points to the 'Portrait' field, which contains a camera icon and a document icon.

- Step 2. At the bottom of the view, click the capture icon ().

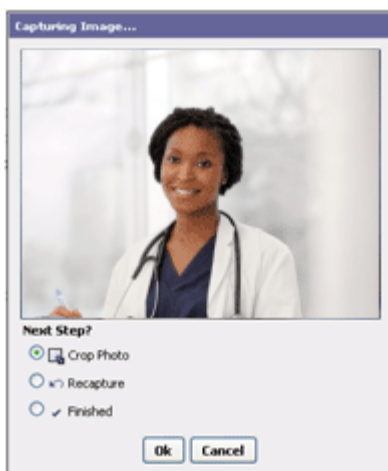
NOTE: If you do not have a **capture** button, check for the native badge design device added under the photo ID network that needs to be added to the station.

A waiting-for-capture window opens.

- Step 3. If you have more than one Photo ID station, the software asks you which Photo ID station you are using.
- Step 4. Select the station and click **OK**.
The Capture Image window opens.

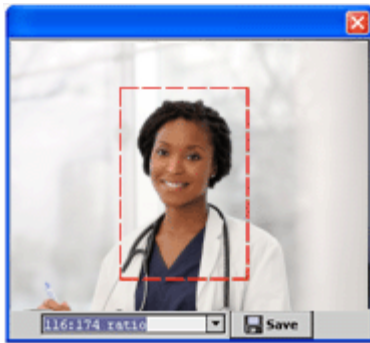


- Step 5. Focus the image and click the **Capture** button.
The **Next Step** window opens.



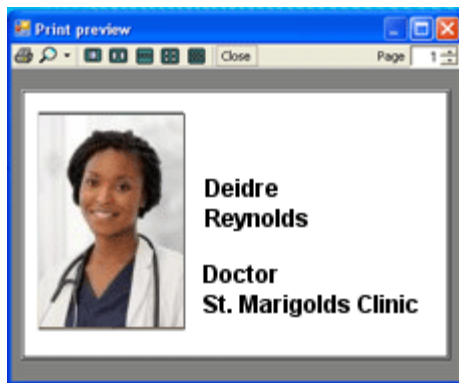
- Step 6. To crop the photo, click **OK**.

The crop tool opens.



Step 7. Enter the aspect ratio (width: height) from the template, adjust the crop box and click the **Save** button.

The **Print Preview** window opens.



The system places the photo in the persons portrait section within the database.

Importing a photo

This procedure allows you to use an existing photo on a badge.

Prerequisites:

Before you can import a photo, the person must exist in the database.

Step 1. From the home view, click **Personnel > People**, double-click a person's row in the table, and click the **Person** tab.

The Person view opens.

The screenshot shows the 'Personnel' view for a person named Bradley Anderson. The interface includes a top navigation bar with 'Home', 'Monitoring', 'Personnel', and 'Reports'. Below this is a sub-navigation bar with 'People', 'Badges', 'Access Rights', and 'Tenants'. The main header displays the person's name 'Anderson, Bradley' and buttons for 'Save', 'People', 'Add New Person', and 'Duplicate'. A tabbed interface shows 'Summary', 'Person', 'Access Rights', and 'Badges'. The 'Person' tab is active, displaying a form with fields for 'Last Name' (Anderson), 'First Name' (Bradley), 'Middle Initial', 'Employee Id', 'Department' (Sales), 'Person Type', 'Tenant' (None), 'Supervisor' (false), 'Trace Card' (Trace), 'PIN' (with fields for PIN and Confirm PIN), and 'Portrait'. A red arrow points to the 'Portrait' section, specifically highlighting the 'File Open' icon (a green house with a red 'x') among other icons like 'Camera' and 'Delete'.

NOTE: If file open icon is not available, create and save the person first.

Step 2. Click the File Open icon (), browse for the photo file and click the **Save** button.

Cropping a photo

Use this procedure to crop a captured or uploaded photo.

Step 1. From the home view, click **Personnel** > **Person**.

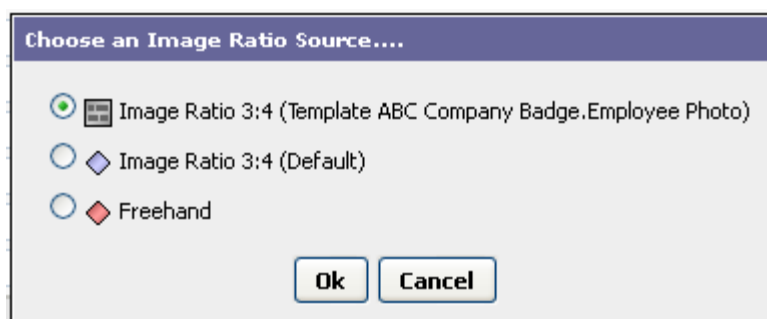
The Person view opens.



The screenshot shows the 'Personnel' tab in the Niagara Enterprise Security Facility Manager's Guide. The 'Person' view is open for 'Reynolds, Diedre'. The form includes the following fields:

- Last Name:** Reynolds
- First Name:** Deidre
- Middle Initial:**
- Employee Id:**
- Department:**
- Person Type:**
- Tenant:** None
- Supervisor:** false
- Trace Card:** Trace Off
- PIN:** PIN (number only): , Confirm PIN:
- Portrait:** A photo of a woman in a white lab coat. A red arrow points to the 'Crop Image' icon (a square with a crop symbol) in the bottom right corner of the portrait area.

- Step 2. Click the Crop Image icon ().
The Choose an Image Ratio Source.... window opens.



The 'Choose an Image Ratio Source....' dialog box is shown. It contains the following options:

- ☒ Image Ratio 3:4 (Template ABC Company Badge.Employee Photo)
- ☐ Image Ratio 3:4 (Default)
- ☐ Freehand

Buttons: Ok, Cancel

Step 3. Choose one of the following :

- **Image Ratio width: height (template name) where:**
 - width is the width as defined by the template.
 - height is the height as defined by the template.
 - templatename is the name of the template.
- **Image Ratio width: height (default) where:**
 - width is the default width.
 - height is the default height.
- **Freehand** lets you use the freehand tool alone to crop the image.

NOTE: Although this may seem the easiest way to crop the photo, it may result in a distorted image. The best option is to use the aspect ratio as defined in the template.

The photo capture window opens with a cropping box set to the largest size possible.



Step 4. Grab any corner or edge and drag the cropping box smaller, then click and drag the center of the cropping box to move it to the desired position.

Step 5. When the cropping box is centered over the face, click the **Save** button.

The photo is cropped to the smaller size while maintaining the aspect ratio.



Step 6. Click **OK** and click the **Save** button.

Printing badges

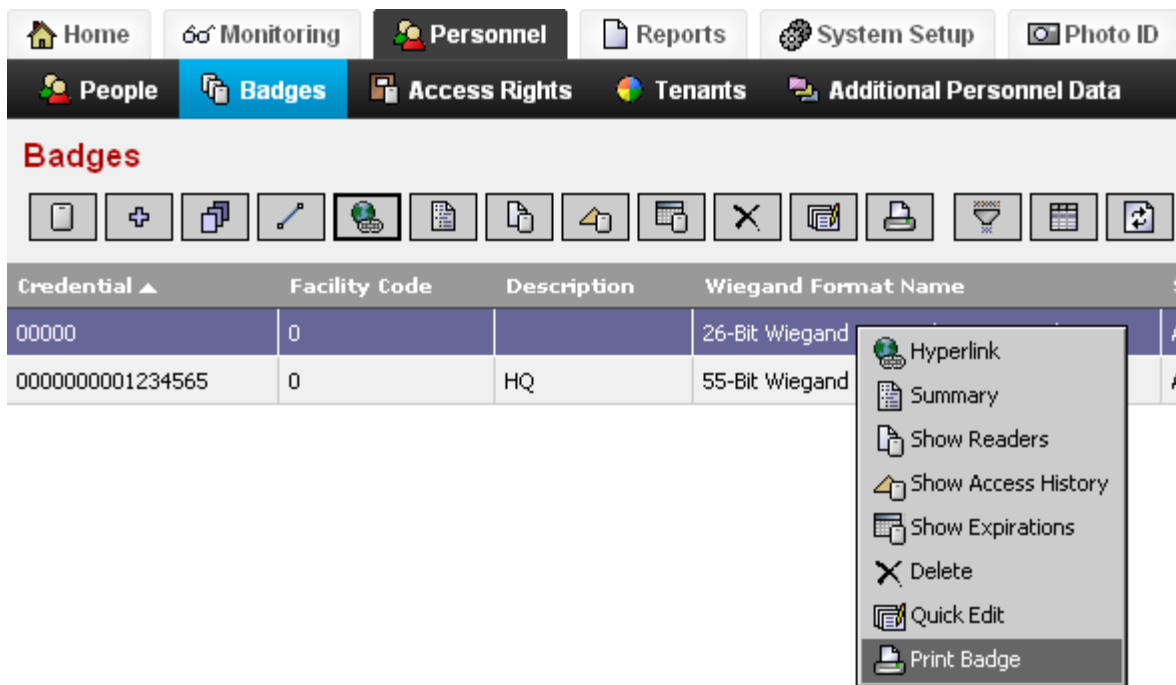
This procedure explains how to print one badge or a group of badges.

Prerequisites:

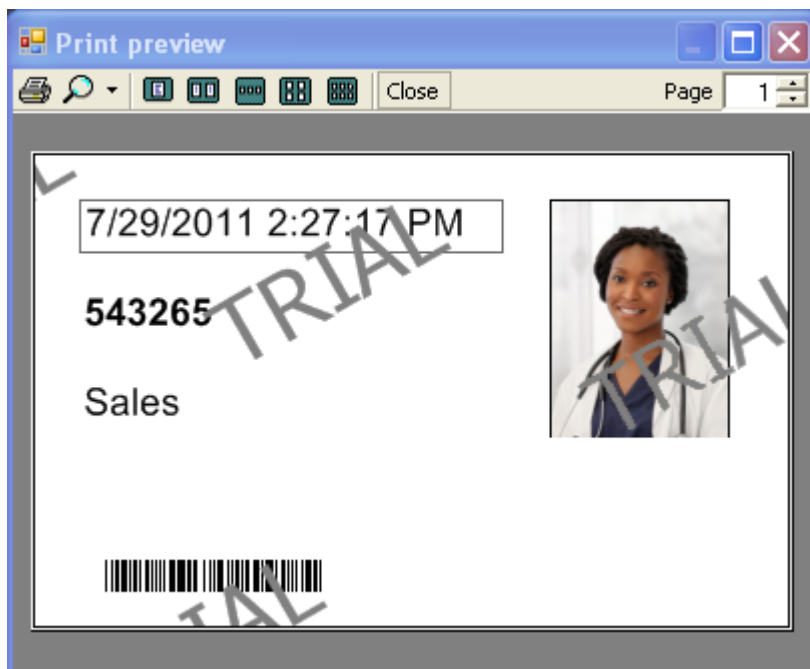
To print a dual-sided badge you follow the same procedure. A dual-sided template and printer capable of printing on both sides are required.

- Step 1. Beginning from the home view, click **Personnel > Badges**.
- Step 2. Select the badge(s) to print, right-click and click **Print Badge**. You can also click the **Print Badge** button.


The action drop-down list opens.



The Print Preview view opens.



NOTE: When more than one badge is selected, you can use the **Print Badge** button to skip the **Print Preview** and print all selected badges in one print operation.

- Step 3. Click the print icon ().
The badge prints.

Chapter 5. Threat-level management

Threat Level management is a licensed feature that provides a way to quickly initiate broad-scale changes to building access based on one or more predefined operational levels (threat Levels) and facility spaces (threat level groups).

Authorized persons use the application interface, an activation badge, or a hardware device to activate the threat level in response to a situation that requires a change to the scheduled access requirements for one or more specific facility areas.

Configuring a system for threat levels involves these primary tasks:

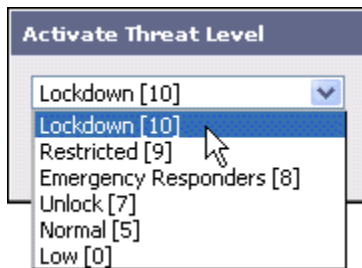
- Setting up threat levels and threat level groups
- Setting up access rights, doors and readers to respond to threat levels
- Assigning access rights, readers, door strikes and activation badges to threat level groups

Threat levels

Threat levels and threat level groups form the core of threat level management. The procedures outlined in the related topics require an understanding of how threat levels work and involve configuring system properties.

By default, the system provides a set (or range) of active threat levels, which are available as enumerated options.

Figure 17. Activate Threat Level window



Assuming you have appropriate administrative privileges, you may rename or supplement this set of threat levels. Each threat level definition includes a number within a range up to a maximum of 255. This number indicates relative degrees of building access.

The default level for normal operation is [5]. This relaxes the restrictions in certain cases, such as when an evacuation is needed, or emergency response teams need general access.

Generally, each successively higher number within the range is more restrictive, so that the higher the threat level, the higher the access privilege that is required to enter the building.

NOTE: If the Access Right is associated with NAC Readers, the threat level changes would be automatically replicated to NAC Controllers. This replication occurs through the NAC Threat Level Replication Job.

Threat level groups

Threat level groups apply and manage active threat levels in a facility's physical space.

If you intend each access right, card reader, and door strike to be affected by threat levels, configure each with

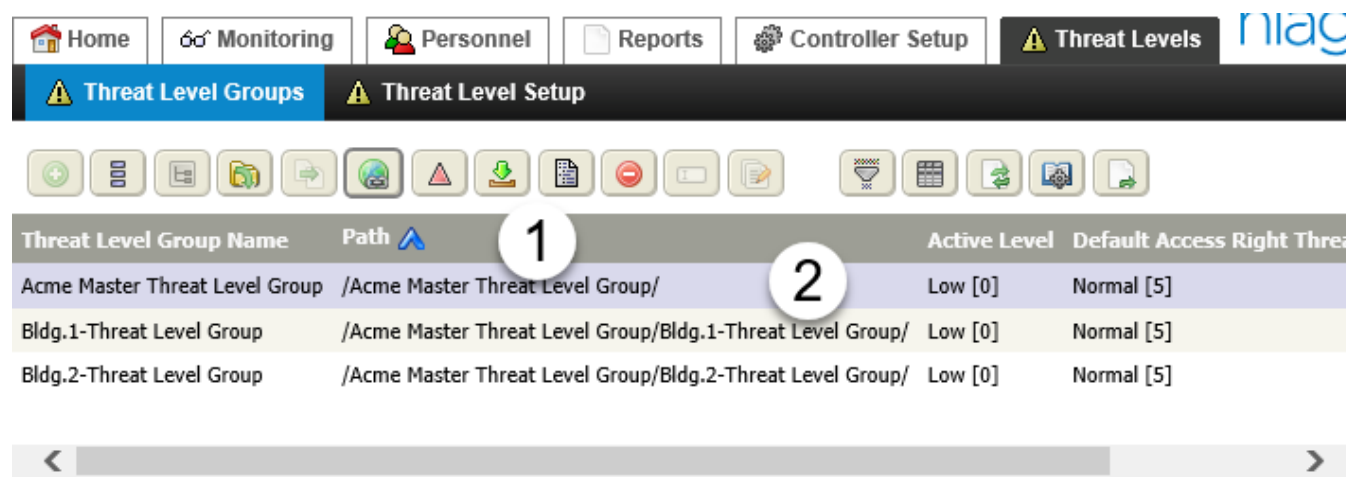
a threat level group. Without a threat level group assigned, an access right or device cannot respond to or interact with threat levels. Only those access rights and devices with a threat level group assigned are threat-level aware.

To assign a threat level to a person, you assign an access right with an associated threat level. By default, the threat level assigned to the access right is also assigned to the person. You may change this and directly assign a threat level to a person.

Threat level group hierarchy

You can arrange threat level groups in a parent-child hierarchy that makes sense for your facility.

Figure 18. Threat Level Group parent, child hierarchy



- 1. Parent group
- 2. Child groups

Changing the parent threat level group’s active threat level automatically changes the threat level associated with the its child threat level groups. You may change the active threat level assigned to the child without affecting the active threat level assigned to the parent or other children under the parent.

Threat levels and people

Threat level assignment, for people, is initially accomplished using access rights. When a person is assigned an access right, the **Default Assigned Threat Level** on that access right becomes the assigned threat level associated with the person. While this automates the initial assignment of threat levels to people, you can specifically change a person’s threat level without changing the person’s assigned access right.

You would use this method of assigning threat levels if you have a large number of people assigned to an access right, but only certain people assigned should be granted access in special situations.

What to do when the threat has passed

The threat level does not change automatically when the condition clears. You can override a thread level through the web UI, a hardware input, or by u sing a threat-level card. These methods return the threat level to the level designated for normal conditions.

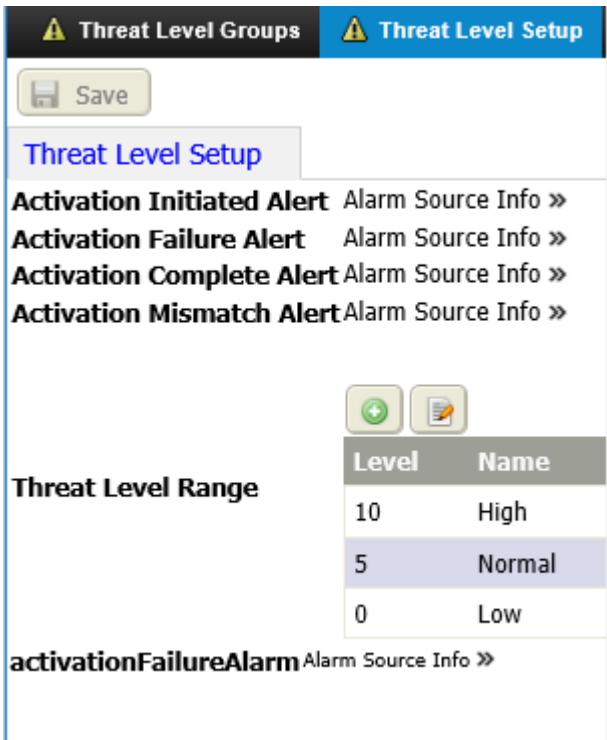
Setting up threat levels

The system comes with three default threat levels in a range from 0 to 10: High [10], Normal [5], and Low [0]. You may change and add to these default threat levels up to a maximum of 255 levels. When setting up threat levels, consider leaving gaps in the numeric assignment so that you can insert levels later if needed.



Prerequisites:

You must have sufficient administrative privileges. For systems with a Supervisor, after you join a controller to the Supervisor, you must add all threat level groups at the Supervisor. Threat levels for systems without a Supervisor may be configured at a controller.

- Step 1.
- From the main menu, expand or click **Threat Levels > Threat Level Setup**.
The Threat Level Setup view opens.



the example shows an expanded list of escalating threat levels.

- Step 2.
- Start by defining the situations that require modifications to the building’s access or that will trigger events, and order them from least to most severe.
Remember to leave gaps in the numeric assignment so that you can insert additional levels later.
- Step 3.
- Do one of the following:
 - To edit one of the default levels, select the level and click the Edit button ().
 - To add levels, click the Add button ().The **Edit Display** or **Add** window opens.
- Step 4.
- Pick a number, create a name and click **Ok**.

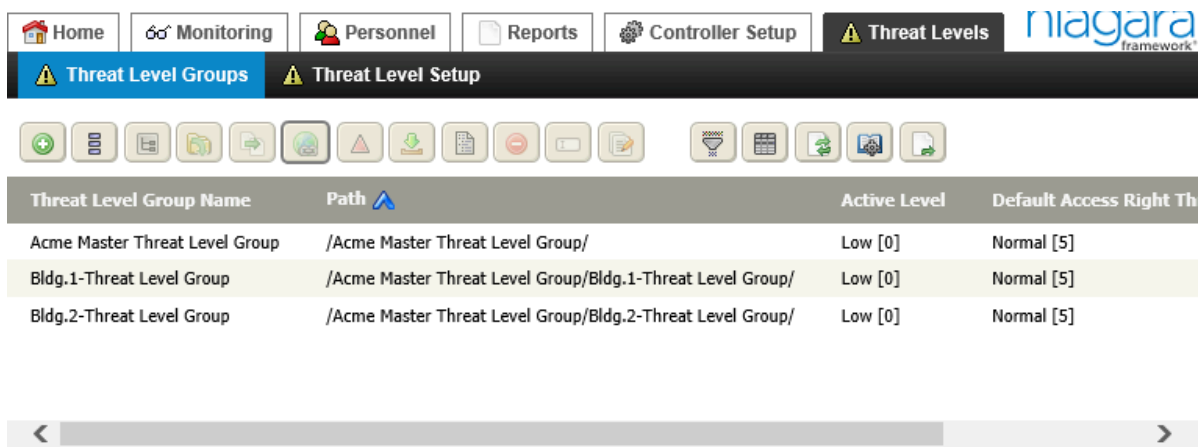
Adding (or editing) a threat level group


A threat level group anticipates what to do in a specific type of emergency. For example, by invoking a threat level group when a child is reported lost, all doors may be automatically locked. You configure the activation method for the various levels: hardware inputs that may trigger various levels, hardware outputs that may be triggered at various levels, and access rights that are modified when the threat level changes. Specific activation cards (badges) may be associated with a threat level group to activate predetermined threat levels.

Prerequisites:

You are working in the Supervisor station. The access rights and badge(s) to assign to parent and child threat level groups already exist in the system.



- Step 1. From the main menu, click **System Setup > Threat Levels**.
The Threat Level Groups view opens.






- Step 2. To create a new group, click the Add button ().
Threat level groups may be related to one another as parent is to child. Child threat level groups inherit the attributes configured for the parent.
- Step 3. Do one of the following:
- To create a parent threat level group, give the group a **Display Name**, but leave **Parent** blank.
 - To create a child group, give it a **Display Name** and identify its **Parent**.

The Add New Threat Level Group view opens.

The illustration shows the view when adding a new threat level group, and when editing an existing threat level group.

- Step 4. If you are editing multiple parent and child threat level groups, clicking the Show Top Level button () filters the table to display only parent threat level groups.
- Step 5. To remove this filter, click the Filter button ()
The Filter window opens.

- Step 6. To see all threat level groups, clear the **Path** property.
- Step 7. To assign access rights to a parent or child group, click the Access Rights tab; to discover unassigned rights, click the Assign Mode button (); select the right in the Unassigned pane and click the Assign button ().
- Step 8. To assign one or more badges, which staff can use to activate the group, click the Activation Badges tab; discover the badges in the system; select one or more badges and click the Assign button ().
- Step 9. To configure the system to pass threat level group information to one or more remote stations, click the Remote Stations tab; discover the remote station(s) to receive the threat level group

information; and assign the remote station(s) to the threat level group.

If a remote controller has an access right that is already assigned to the threat level group, the system notifies the remote controller of the threat level change.

Step10. To confirm the configuration, click **Save** and review the Summary tab.

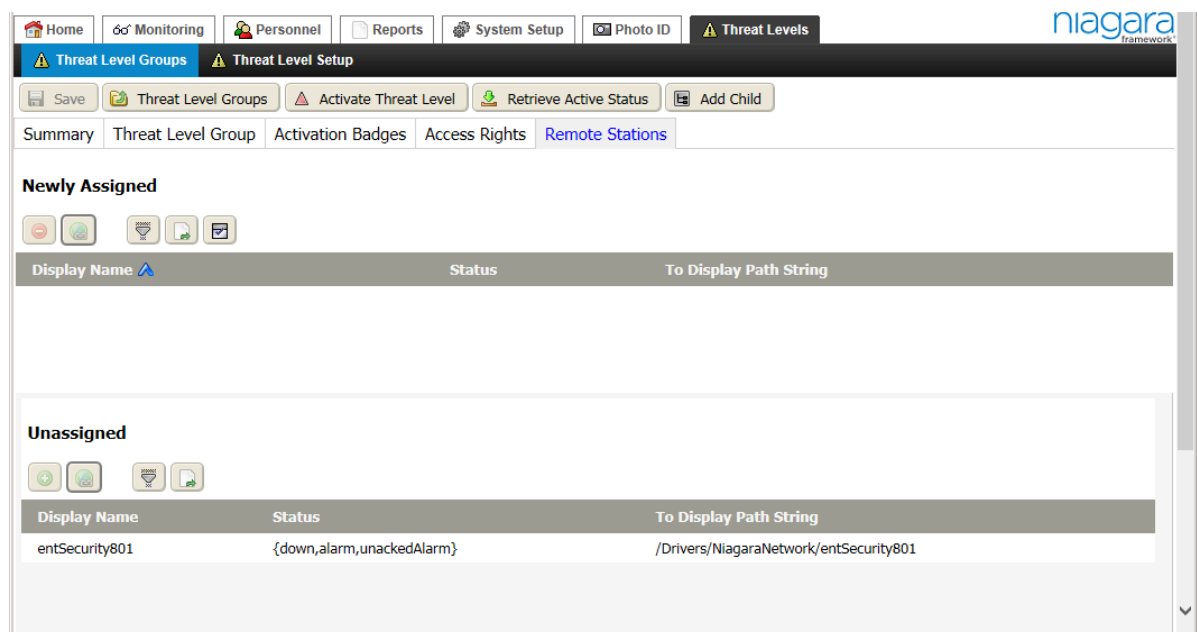
Assigning a remote station to a threat level group



If a remote controller uses an access right that has been configured with a threat level group, the replication process propagates the threat level group to the remote station. If the remote controller access right is not configured with a threat level group, you must assign the remote station to the threat level group. This ensures that the system passes threat level group information to the remote station.

Prerequisites:

This procedure assumes you are working in the Supervisor station.

- Step 1. From the main menu click **Threat Levels**.
- Step 2. Double-click an existing threat level group.
The threat level group view opens.
- Step 3. Click the Remote Stations tab.
The Remote Stations tab opens.




- Step 4. Click the Assign Mode button ().
The system discovers and displays the available (unassigned) remote stations.
- Step 5. Select the station and click the Assign button ().

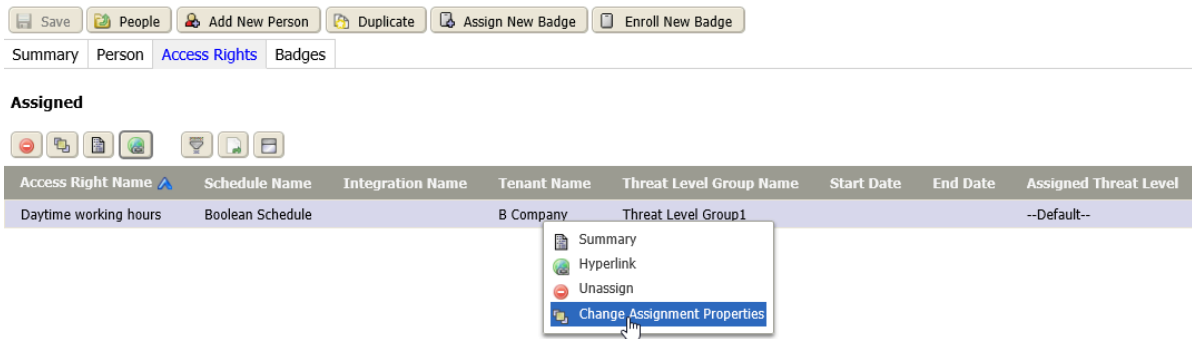
Directly assigning a threat level to a person

Once you specify a specific threat level, the person's threat level is no longer linked to the person's access right and will not change if the threat level group defined in the access right changes.

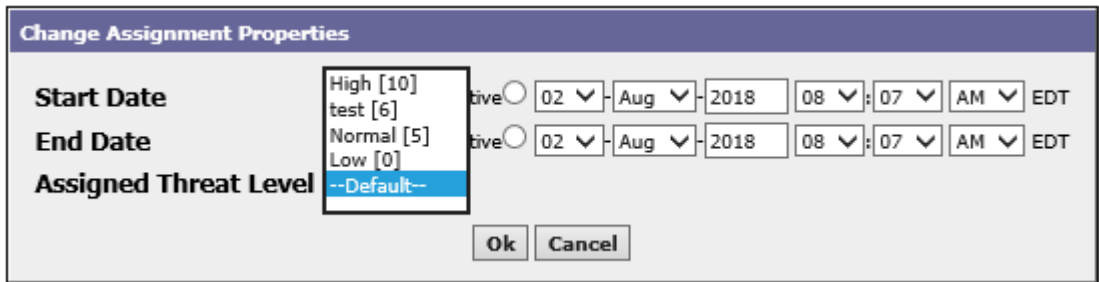
Prerequisites:

The person to whom you are directly assigning a threat level exists in the system database.

- Step 1. From the main menu click **Personnel**.
The People view opens.
- Step 2. Double-click the person row in the table or select the person to edit and click the Hyperlink button ().
The person's view opens.
- Step 3. Click the Access Rights tab.
The Access Rights tab displays the assigned rights.



- Step 4. Select one or more access rights, right-click the selection, and click **Change Assignment Properties**.
The **Change Assignment Properties** window opens.



- Step 5. Select a threat level and click **Ok**.
This assignment overrides and breaks the link to an assigned access right's default threat level. A person may have more than one access right assigned. You can edit each access right to directly assign the threat level.

Assigning access rights to threat level groups

Assigning access rights to threat level groups creates the link between the threat level group and each access right, such that, the access right threat level defaults to the threat level of the threat level group. This procedure is not required if your access rights are configured with threat levels.

Prerequisites:


If your system is configured with a Supervisor, this operation must be done at the Supervisor station.

- Step 1. From the main menu, expand or navigate to **Threat Levels > Threat Level Group** and double-click a threat level row in the table.

Step 2. Click the Access Rights tab.

Step 3. Click the Assign Mode button ().

The system discovers all unassigned access rights. You may assign an access right to only one threat level group. If an access right is already assigned to a threat level group, and you assign it to a different threat level group, the system removes the access right from the previously-assigned group.

Step 4. Select an access right, and click the Assign button ().

The access right is now assigned to the threat level group.

Threat level response

Access rights, doors and readers must be prepared to respond when a threat level is activated. The information in these topics involves configuring system properties on access rights, door strikes and readers.

When setting up access rights, one must determine what type of person will need access in various situations, and what type of person should have access inhibited in these situations. For example, contract workers may have their access to a lab area denied if there is a chemical spill in the area. If the access right assigned to a contract worker has a default threat level set at normal [5], and the threat level is set to 10, the system denies access to the contract worker, but it allows access to everyone whose access right is configured with a threat level of 10 or higher.

The threat level for the area could be further increased to 15. This would restrict access to everyone with an access right and threat level of 14 and below. It would allow access to everyone with an access right and threat level of 15 and higher.

Inhibiting those assigned an access right with a threat level below the active threat level, while granting access to those assigned an access right with a threat level above the active threat level represents the normal mode of threat level operation for an access right. An access right may also be set to be active only at a specific threat level, or to be active in reverse mode. In this mode, the meaning of the scale flips. Reverse mode grants access when the assigned access right's threat level is below the active threat level, and prohibits access with the access right's threat level is above the active threat level. You may use this type of action for non-internal emergency responders that need access for certain situations (Fire fighters need access to the fire. Normal workers need to flee the fire.)

Access rights are based on a schedule that specifies where and when a person may enter a building. To support threat levels, each access right should also be configured with a unique threat level group. When a person attempts to gain access using an access right configured with a threat level group, the system compares the currently active threat level with the threat level contained in access right's threat level group. If the threat level group validates, the system authorizes the person to enter the building.

Adding a threat level group to an access right

Associating a threat level group with an access right is how you configure the system to assign threat level groups to individual people.

Step 1. From the main menu expand or navigate to **Personnel > Access Rights** and either create a new access right, or double-click an existing access right.

Step 2. If you are editing an existing access right, click the Access Right tab.

Step 3. Click the chevron to the right of the **Threat Level Group** property. A **Ref Chooser** opens with the list of available threat level groups.








Step 4. Select a threat level group and click **Ok**.

Step 5. To update the database, click the **Save** button at the top of the view.

Directly assigning a threat level to an access right

This procedure makes it possible to define a unique threat level for an access right independently of the threat level defined in the threat level group.

- Step 1. From the main menu click **Personnel > Access Rights >** , double-click an access right in the table and click the Access Right tab.
The access right view opens with the Access Right tab selected.

Summary	Access Right	People	Readers	Floors
Access Right Name	access Right1			
Schedule	 Boolean Schedule >> 			
Niagara Integration ID	 None >>			
Tenant	 None >>			
Threat Level Group	 Threat Level Group >>  			
Threat Level Operation	Normal ▼			
Default Assigned Threat Level	Normal [5] ▼			
Description	<div style="border: 1px solid #ccc; height: 40px; position: relative;"> <div style="position: absolute; top: -10px; right: 0;"> <div style="position: absolute; top: -10px; left: 0;">^</div> <div style="position: absolute; top: -10px; right: 0;">v</div> </div> </div>			

- Step 2. Select an assigned threat level other than --Default--.
- When a threat level group is associated with an access right, the system determines the actual threat level based upon how you configure the **Default Assigned Threat Level** on the access right. If you leave this property set to --Default--, the system uses the **Default Access Right Threat Level** as defined for the threat level group. This is convenient. It means that to change the threat level for all access rights, all you have to do is change the **Default Access Right Threat Level** on the threat level group. To break this threat-level-group-to-access-right link you may change the **Default Assigned Threat Level** from --Default-- to a specific threat level.

Configuring a threat level on a door strike

The way that a threat level affects a door depends on the way that you configure the door's strike.

Prerequisites:

You are working in the controller station that manages the door.

- Step 1. From the main menu, click **Controller Setup > Remote Devices > Remote Modules > Remote Module Setup** and double-click the door device (module), click the door name, and click the Strike tab.

The Module Setup view opens to the Strike tab.

Strike	Sensor	Exit Request
Locked State	Open ▾	
Status	Locked {fault}	
Auto Relock	Relock On Door Open ▾	
Schedule Operation	Normal ▾	
Unlock Schedule	None »	
Override Schedule	None <small>schedule.override.chooser.label</small>	
Access Unlock Time	00 m 05 s [1sec - 59mins]	
Log Exit Requests	None ▾	
Log Schedule Activity	true ▾	
Threat Level Group	⚠ None »	
Door Lock Output	Relay Output 1 ▾	

- Step 2. Configure the **Schedule Lockdown Threat Level** property to something other than **None**. The system keeps the door locked as long as the active threat level is at or above the level specified here.

NOTE: This value must be greater than the value of the **Unlock Threat Level** property. If not, a warning message displays next to the property when you try to save the changes.

- Step 3. Configure the **Unlock Threat Level** property to something other than **None** and to a lower threat level than that configured for **Schedule Lockdown Threat Level**. Typically, the **Unlock Threat Level** would be lower than the level defined for normal operation (less than 5 in our example). The system keeps the door unlocked, no matter what the associated schedule state is.

NOTE: This value must be less than the value of the **Schedule Lockdown Threat Level** property. If not, a warning message displays next to the property when you try to save the changes.

Configuring a threat level for a reader

Assuming your reader has the required features, at a normal threat level a reader can require a reader-only card swipe for validation. However, at a higher active threat level, a reader may require a card swipe and the entry of a PIN to provide valid access.

Prerequisites:

You are working in the controller station that manages the reader.

- Step 1. From the main menu, click **Controller Setup > Remote Devices > Remote Modules > Remote Module Setup** and double-click the remote module that supports the door device, click the **Doors** tab, click the door name, and click the **Strike** tab. The Module Setup view opens to the Strike tab.
- Step 2. Configure the **Elevated Threat Level** property to something other than **None**. Setting this value to **None** causes the system to ignore the threat level.
- Step 3. Configure the **Elevated Threat Reader Config** property. This tells the system what to enable when the active threat level matches or exceeds the **Elevated Threat Level** value.

Activation level input

On a controller (not a Supervisor) the **Manage Devices** button adds a boolean activation level input to a particular threat level group. This **In** property selects a controller Digital Input (DI) or Supervised Digital Input (SDI) as the initiating event. The **Active Threat Level** property defines what active level the threat level group changes to when the input is active.

The input triggers a specific threat level. You would set up one input for a lockdown, and another input for the all clear.

Figure 19. Activation Level Input tab

Acme Enterprise Master Threat Level Group/Bldg.2-Threat Level Group

Save

Threat Level Groups

Activate Threat Level

Retrieve Active Status

Manage Devices

Summary	Threat Level Group	Activation Level Input	Activation Level Output	Access
Out	Active {ok}	Active Threat Level	Emergency Responders [8]	
In	<div><div></div>Base Reader Module.Sdi6</div>			
Inactive State	open			

For example, imagine a duress or panic device located near a reception desk. When someone activates the device, it sets the threat level of the associated threat level group to a high level, such as 10 or higher. An activation badge, Boolean input, or command from the console can be used to reset the threat level group back to normal.

Activation level output

On a controller (not a Supervisor) adding a Boolean activation level output to a particular threat level group assigns a controller relay to the **Relay Out** property. The **Manage Devices** button adds this tab.

When the active level matches or exceeds the **Assigned Threat Level** property, the relay responds according to the **Threat Level Operation** property. If the **Out** property is active, the system energizes the relay.

For example, initiating a high threat for a threat level group can activate a relay output, which is connected to an alarm dialer. This causes the dialer to initiate a call to a central monitoring station.

Access rights and activation badges assigned to threat level groups

Assigning access rights and components to threat level groups uses a discovery process, which makes it possible to assign multiples at a time.

Activation badge

Rather than grant access, an activation badge activates a specific threat level for a specific threat level group. An activation badge uses access rights to implement an active threat level at the desired access points. Access rights are assigned to people. There are two ways to create an activation badge.

- Create a fictitious threat level person; assign that person access rights that allow the activation badge to work; then assign all activation badges to that person. The system recognizes these badges as activation

badges for activating the designated threat level at the access points associated with the threat level group. Activation badges do not provide access to the door associated with the reader.

- Assign an access right to a real person with sufficient default levels to allow the person to initiate a threat level.

When you assign an access right to a person for the purpose of creating an activation badge, be aware of the access right's threat level. A person with an access right configured for a threat level of three [3] cannot use their badge to change an active threat level that is a level four [4] or higher. A good practice may be to create a threat level just for the person with the activation badge and set its **Default Access Right Threat Level** property to the highest threat level.




Creating an activation badge

You create an activation badge the same way you create any other badge, but, instead of providing access to a facility, you configure this badge to activate one specific threat level for one specific threat level group.

Prerequisites:

The person (fictitious or real) exists with an access right assignment for a valid schedule. All readers for which this badge is to activate the threat level exist. If your system is configured with a Supervisor, you are currently working in the Supervisor station.

NOTE: To make it easier to set up the activation badges, you may want to create a threat level person and assign all activation badges to that person.

- Step 1. From the main menu click **Personnel > Badges**, and click the Add button ().
The Add New Badge view opens to the Badges tab.
- Step 2. Configure the basic badge properties.
- Step 3. For **Owner**, enter the person with the access right assignment that is valid for activating a threat level on desired readers.
- Step 4. When you complete configuring the badge, click the **Save** button.
- Step 5. Navigate to **Threat Levels**, double-click the threat level group to assign to the badge, and click the **Activation Badges** tab.
The Activation Badges tab opens.
- Step 6. Click the Assign Mode button ().
The system discovers all unassigned badges. The activation badge may be assigned to only one threat level group. Once it is assigned to a group, it is not available from the Unassigned pane to be assigned to any other badge in the Activation Badges view.
- Step 7. Select the activation badge and click the Assign button ().
The system assigns the badge to the threat level group.

Assigning a threat level to an activation badge

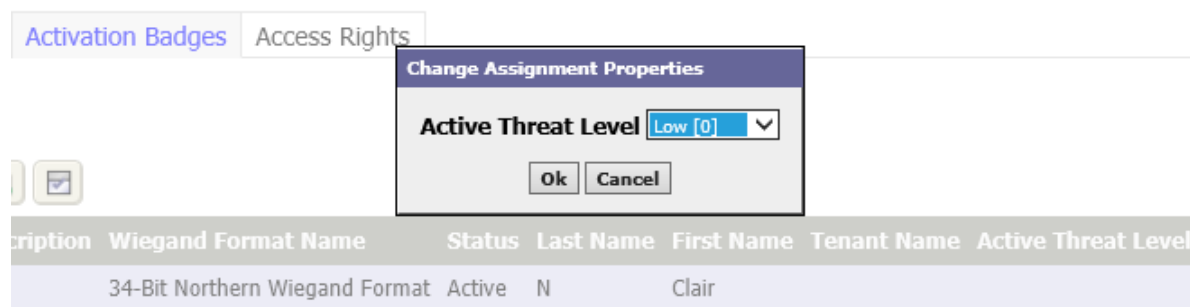
After you have assigned an activation badge to a threat level group, you need to assign the threat level that the activation badge will initiate.

Prerequisites:

NOTE: Threat level jobs, such as Activate Threat Level and Retrieve Active Status, cannot be canceled from the browser once they start.

- Step 1. Navigate to **System Setup > Threat Levels**, double-click the threat level group, and click the **Activation Badges** tab.
The Activation Badges tab opens.
- Step 2. Select and right-click on one or more listings in the displayed table.
- Step 3. Click **Change Assignment Properties** from the popup menu.

The **Change Assignment Properties** window opens.



- Step 4. Choose the desired threat level from the **Active Threat Level** drop-down list and click the **Ok** button.

The system changes the active threat level for the badge.

Chapter 6. Reports

Reports provide information about the data stored in the station database. The system provides a set of pre-configured (default) reports and the ability to create custom reports. You can save custom-configured reports as well as schedule any report for automatic generation and email forwarding.

Default reports are optimized for quick processing. These reports return only one row for the data in each column. If a report request can return multiple answers in any one column, you see only data for the first answer found.

Full reports return all data, but are much slower to compile. The data in any one column can display multiple, semi-colon-separated results.

For example, an optimized report on people with a column showing their assigned badges only returns one badge per person. A full report of the same data shows every card assigned to each individual.

History reports

The default history reports include:

- The Access History report displays a table of all access activity.
- The Alarm History report provides a time-stamped table with a row for each alarm that includes: timestamp, description, acknowledgment, source, credential number and owner name.
- The Intrusion History report displays a time-stamped table that lists each time the intrusion zone was armed and disarmed.
- The Attendance History report displays a table of badge transactions with arrival and departure times.
- The Audit History report displays a table of records of all system operations.
- The Log History report displays a table of all log entries.

Hardware reports

The default hardware reports include:

- Doors report lists all doors.
- Readers report lists all readers connected to the network.
- Inputs report lists digital inputs that are on the network.
- Outputs report lists all digital outputs on your network.
- Elevator report lists all elevators.
- Modules report lists all hardware modules on the network.
- BACnet report lists all BACnet points in the system.

Miscellaneous reports

This set of default reports includes the following:

- Person Access Right report.
- Person Reader report.
- Access Right Reader report shows the access rights and their assigned readers.
- Personnel Changes report.

Custom reports

You can configure a custom report to appear anywhere in the navigation path and schedule the emailing of a

report at a time you designate. Emails are initiated by a transition from false to true using a Boolean Schedule.

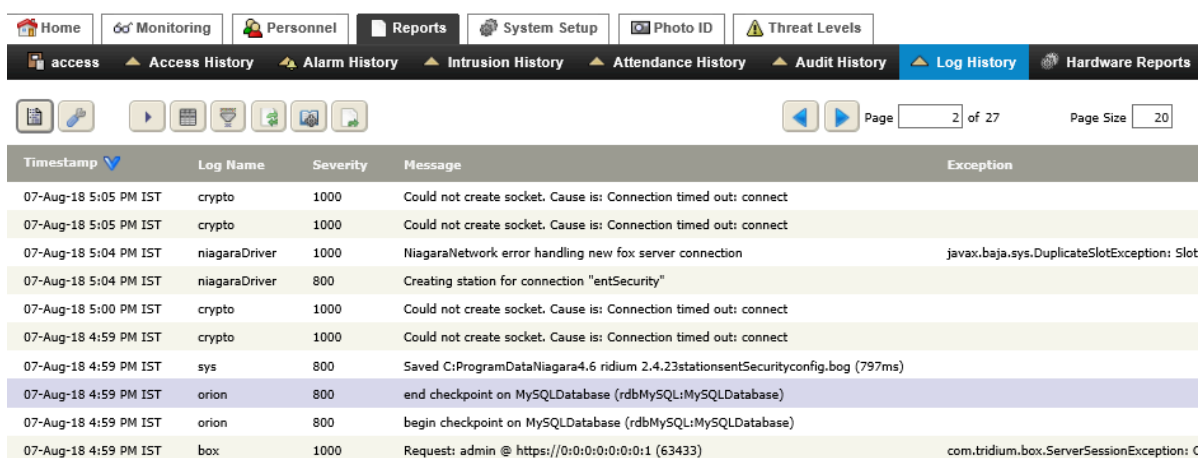
Viewing a report

A default report is one that is available under the **Reports** menu in the navigation tree. Custom reports may appear anywhere in the menu hierarchy.

Step 1. Do one of the following:

- To view a default report, from the Home view, click **Reports**, and click a report name, such as **Alarm History**, Audit History, etc.
- To view a custom report, navigate to the report and click its name in the menu structure.

Hardware Reports and Miscellaneous Reports are further organized into report sub-groups. The report table opens.




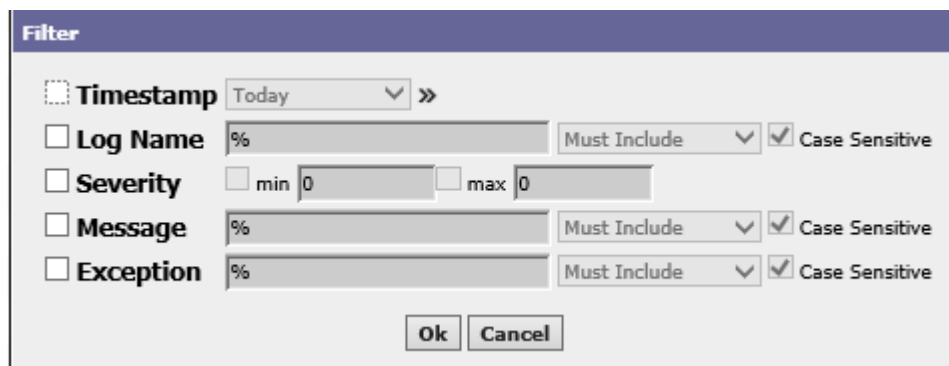
The screenshot shows the Niagara Enterprise Security Facility Manager interface. The top navigation bar includes Home, Monitoring, Personnel, Reports, System Setup, Photo ID, and Threat Levels. The Reports menu is expanded, showing sub-menus like Access History, Alarm History, Intrusion History, Attendance History, Audit History, Log History (selected), and Hardware Reports. Below the navigation bar is a toolbar with icons for various functions. The main area displays a table with the following columns: Timestamp, Log Name, Severity, Message, and Exception. The table contains several rows of log entries, including connection timeouts, network errors, and database checkpoints.

Timestamp	Log Name	Severity	Message	Exception
07-Aug-18 5:05 PM IST	crypto	1000	Could not create socket. Cause is: Connection timed out: connect	
07-Aug-18 5:05 PM IST	crypto	1000	Could not create socket. Cause is: Connection timed out: connect	
07-Aug-18 5:04 PM IST	niagaraDriver	1000	NiagaraNetwork error handling new fox server connection	javax.baja.sys.DuplicateSlotException: Slot
07-Aug-18 5:04 PM IST	niagaraDriver	800	Creating station for connection "entSecurity"	
07-Aug-18 5:00 PM IST	crypto	1000	Could not create socket. Cause is: Connection timed out: connect	
07-Aug-18 4:59 PM IST	crypto	1000	Could not create socket. Cause is: Connection timed out: connect	
07-Aug-18 4:59 PM IST	sys	800	Saved C:\ProgramData\Niagara4.6\ridium 2.4.23stationsentSecurityconfig.bog (797ms)	
07-Aug-18 4:59 PM IST	orion	800	end checkpoint on MySQLDatabase (rdMySQL:MySQLDatabase)	
07-Aug-18 4:59 PM IST	orion	800	begin checkpoint on MySQLDatabase (rdMySQL:MySQLDatabase)	
07-Aug-18 4:59 PM IST	box	1000	Request: admin @ https://0:0:0:0:0:0:1 (63433)	com.tridium.box.ServerSessionException: C

The example is of the Log History report table.

Step 2. If the report contains more than one page, navigate to the additional pages.

Step 3. To filter the report, click the Filter button (). The Filter window opens.




The screenshot shows the Filter window for the Log History report. It has a title bar labeled "Filter". The window contains several filter criteria:

- Timestamp**: A dropdown menu set to "Today" with a right arrow button.
- Log Name**: A text input field with a percentage sign, a "Must Include" dropdown, and a "Case Sensitive" checkbox.
- Severity**: A range selector with "min" and "max" input fields, both set to "0".
- Message**: A text input field with a percentage sign, a "Must Include" dropdown, and a "Case Sensitive" checkbox.
- Exception**: A text input field with a percentage sign, a "Must Include" dropdown, and a "Case Sensitive" checkbox.

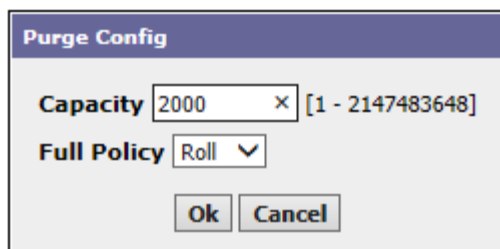
 At the bottom of the window are "Ok" and "Cancel" buttons.

The screen capture above is for log history. Each report provides a different set of filter criteria.

Step 4. Select and define the filter criteria and click **Ok**.

Step 5. To print the report, click the Export button (), select PDF for **File Type** and click **Ok**. The system creates a PDF, which you can use to create a hard copy.

- Step 6. If the report contains a large number of records, only a few of which are needed, click the Purge Config button.
The **Purge Config** window opens.


The image shows a dialog box titled "Purge Config". It has a purple header bar. Below the header, there are two fields: "Capacity" with a text input containing "2000" and a range "[1 - 2147483648]" to its right, and "Full Policy" with a dropdown menu showing "Roll". At the bottom of the dialog are two buttons: "Ok" and "Cancel".

- Step 7. Define the **Capacity** and **Full Policy** and click **Ok**.
The system removes the records that exceed the defined capacity from the database.


Adding a custom report

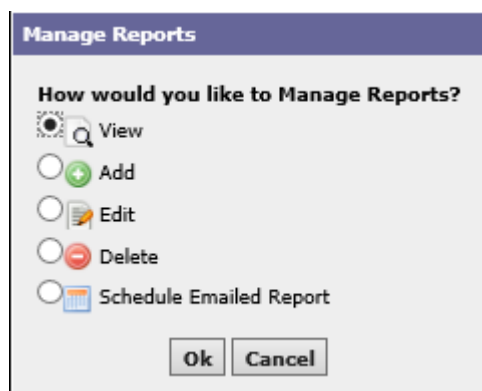
You create a custom report by basing it on an existing default or custom report. The report you create may appear anywhere in the system menu structure.

- Step 1. Do one of the following:
- To base your report on a default report, from the **Home** view, click **Reports**, and click a report name.
 - To base the new report on a custom report, navigate to the report in the menu structure.
- The report table opens.

- Step 2. Click the filter button  .
The **Filter** window opens.

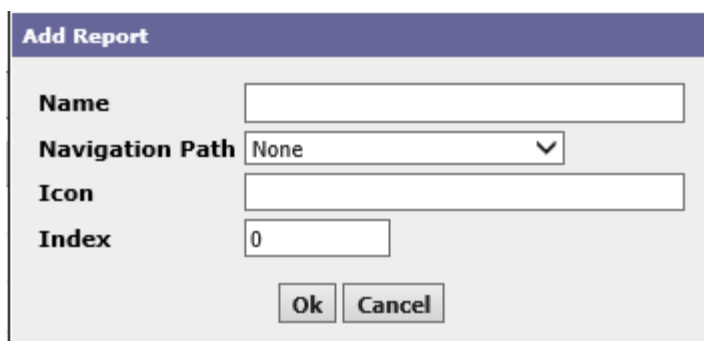
NOTE: Any filters that are active when you add the report become read-only for the new custom report. For example, if you add a report that is filtered using the Timestamp property, you cannot then change the Timestamp property value. You can, however, change other properties in the Filter window to further filter the custom report.

- Step 3. With the filtered report information displaying, click on the **Manage Reports** button  .
The **Manage Reports** window opens.

The image shows a dialog box titled "Manage Reports". It has a purple header bar. Below the header, the text "How would you like to Manage Reports?" is displayed. There are five radio button options: "View" (with a magnifying glass icon), "Add" (with a green plus icon), "Edit" (with a pencil icon), "Delete" (with a red minus icon), and "Schedule Emailed Report" (with a calendar icon). At the bottom of the dialog are two buttons: "Ok" and "Cancel".

- Step 4. To add a new report, choose the **Add** option and click **Ok** .

The **Add Report** window opens.




- Step 5. Give the report a name (**Name**), choose a location to display the report on the main menu (**Navigation Path**), define an icon to appear next to the report name (**Icon**), and enter an integer (**Index**), which determines where the report appears (left to right) in the navigation path.

NOTE: If you choose **None** for **Navigation Path**, the report name does not appear in the menu but you still have access to it from the **Manage Reports** windows (for example, **View Report**, **Edit Report**, or other).

- Step 6. In the **Add Report** window, click the **Ok** button.
The new report menu item displays in the selected menu navigation path.


Editing a custom report

Editing an existing report is similar to creating it in the first place.

- Step 1. Navigate to the report table in the system's menu structure.
- Step 2. Click on the **Manage Reports** button ().
The **Manage Reports** window opens.
- Step 3. Choose the **Edit** option and click **Ok**.
The **Edit Report** window opens.
- Step 4. Edit a property and click **Ok**.
- Step 5. Select the report to edit and click **Ok**.
The **Edit Report ...** window opens. The properties you can edit are the same ones used to create the custom report.

Deleting a custom report

You may delete custom reports. You may not delete the default reports.


- Step 1. Navigate to the report table in the system's menu structure.
- Step 2. Click on the **Manage Reports** button ().
The **Manage Reports** window opens.
- Step 3. Click the **Delete** followed by clicking **Ok**.
The **Delete Report** window opens. This window lists all appropriate custom report options.
- Step 4. Choose the report to delete and click **Ok**.
The system deletes the report.

Creating an email schedule for reports

To send email reports at designated times you need to have an appropriately configured schedule. Report emails are initiated by a schedule that transitions from a `false` to `true` output. The following example illustrates how you might create an appropriate schedule using the Create Schedule view, Special Events tab. The procedure describes how to create a new schedule. You could also edit an existing schedule to create an appropriate schedule for emailing.

Prerequisites:

You have set up custom schedule options and opened the Add New Schedule view opens.

- Step 1. Type a name in the **Display Name** property and click the **Save** button.
The Summary tab opens with the name you just created as the view name.
- Step 2. Select the Special Events tab and click the Add button ().
The Add window opens.
- Step 3. Type a name to identify when to send the email in the **Display Name** property, choose an appropriate option from the **Type** option list and click the **Ok** button.
The email event displays in the Special Events table. Each event **Type** option provides different configuration possibilities. For example, to send a one-time email report on a specific date, choose the **Date** option. To send a report at the same time every week, choose the **Week and Day** option.
- Step 4. Select the newly added event, assign the **Output** property to `true` on a 15 minute block of time in the Events editor (drag on the timeline or use the **Start** and **Finish** properties), and click the **Save** button.
The system creates the new schedule and makes it available for assigning to an email report.
- Step 5. Since you need the event to transition the schedule output value from a `false` to `true` output, check on the Schedule Setup tab to make sure that the current schedule **Output** value is `false` and that the **Default Output** value is set to `false`.


Assigning a schedule to a report

This procedure describes how to designate that a report be attached to an email that is sent at a scheduled time.

Prerequisites:


This procedure requires:

- The report to email must be defined (default reports already exist, custom reports must be defined) so that it appears as an option in the Schedule Emailed Report window.
- The schedule must exist so that it appears as an option in the **Export Schedule** property of the Schedule Emailed Report window.
- A functional and accessible email account must exist so that it appears in the **Email Account** option list of the Schedule Emailed Report window.

- Step 1. Navigate to the report table and click on the Manage Reports button ().
The **Manage Reports** window opens.
- Step 2. Choose the **Schedule Emailed Report** option and click the **Ok** button.
The **Schedule Emailed Report** window opens. This window displays a list of reports from which to choose.
- Step 3. Select the report and click **Ok**.

The **Schedule Emailed Report** window opens.

Step 4. Click the browse icon (>>) next to the **Export Schedule** property.
The **Ref Chooser** window opens.

Step 5. Select the schedule in the table listing and click **Ok** or the  button to assign the schedule to the report.
The **Schedule Emailed Report** window opens again.

NOTE: The system sends scheduled reports based on a schedule transition from a `false` to a `true` output state. This means that if the schedule you are using is already in a `true` output state when you assign the schedule to the report, the system does not send the report. The assigned schedule output must transition to `false` and then to `true` for the report to be sent.

Step 6. Select the email account from the drop-down list.

Step 7. Complete the rest of the email properties as appropriate, and click **Ok**.

Step 8. Use the large text field area to include a message in the body of the email.
The **Schedule Emailed Report** window opens again.


Step 9. At a minimum, give the report a **Title**, **File Type**, **Alignment**, and **Style** and click the **Ok** button.
The report is now scheduled for delivery via email.

Printing a report

To print a report you first create a PDF and then print the PDF. Creating a PDF is an export function.

Step 1. Open the view that contains the records to export.

Step 2. Optionally, filter the table so that only the records to export are visible.


- Step 3. Click the Export button ().
The **Export** window opens.
- Step 4. Select an **Export Range** and click **Ok**.
The system opens a file chooser window.
- Step 5. Define a PDF file name and click **Ok**.
- Step 6. Open the PDF and print it.

Purging history records from a remote controller

History records can build up quickly in remote controllers, which have limited storage. Based on your audit requirements, you can configure in advance each station's purge policy.


Prerequisites:

You are connected to the remote station.

- Step 1. Click **Reports** and click a history report.
The report view opens
- Step 2. Click the Purge Config button ().
The **Purge Config** window opens.
- Step 3. Configure the number of history records to retain, what should happen when the history file reaches capacity, and click **Ok**.
The default, **Roll**, replaces the oldest records with newer ones. **Stop** ceases recording when the system reaches **Capacity**.

Purging history records from a Supervisor station

While a Supervisor PC has more room to store history records, you can configure when records expire and set up an automatic purge schedule, or purge on a specific date.

- Step 1. Click **Reports** and click a history report.
The report view opens.
- Step 2. Open a history view.
- Step 3. Click the Purge Config button ().
The **Purge Config** window opens.
- Step 4. Configure the data expiration date.
This identifies records that may be automatically deleted.
- Step 5. Configure the **Auto Purge** date and time.
This tells the system when to automatically remove expired records. In lieu of this method, **Manual** specifies a specific date and time (trigger) to purge the file of expired records.

Opening an exported CSV file in Microsoft® Excel®

When exporting a CSV file, long credential numbers may display in scientific notation. You can edit the CSV file in Notepad or similar text editor and avoid this problem, or you can import the CSV file into Microsoft® Excel®.

Prerequisites:

NOTE: The following procedure uses menus, window text, and options from Microsoft® Office Excel 2003. Other versions of Excel may have different text and interface labels.

- Step 1. Open a blank worksheet in Excel.

- Step 2. Click in the **A1** cell to designate a cell location for import.
- Step 3. From the **Data** menu, select **Import**
- Step 4. Browse to the location of the CSV file, select it, and click the **Open** button.
The import wizard, step 1 opens.
- Step 5. Click the **Next** button.
The import wizard, step 2 opens.
- Step 6. In the **Delimiters** area, click to clear the **Tab** check box, select the **Comma** check box, and click the **Next** button.
The import wizard, step 3 opens.
- Step 7. Under the **Data preview** area, click to select the Credential Number column (or the column that contains the data that is being converted incorrectly).
- Step 8. Under the **Column data format** area, select the **Text** option and click the **Finish** button.
The **Import Data** window opens (some versions) asking where to put the data.
- Step 9. With the **\$A\$1** field selected, click **OK** to complete the import.

Chapter 7. Station save, backup and restore

To keep a system healthy, periodic station saves and backups are required.

The normal controller station save captures changes to the station's object spaces (components, alarm, history) to flash memory.

A backup automatically performs a local station save first, and then, running as a standard station job, backs up all station data to the Supervisor station. This creates a .dist file, which can be later restored following a software upgrade or installation of a new controller.

Restoring a station from a backup .dist file returns the station to the state it was in when the backup job ran.

About station save

A single file defines a station database: `file:~stations/{name}/config.bog`. This bog (Baja object graph) file contains the collection of station components in an HSQL relational database management system. This database offers a fast response time in an embedded environment.

The config.bog is required to boot a station and manage its components. A station save differs from a local or system backup in that a station save backs up the config.bog to a local destination. A local or system backup saves the data collected by the system to the Supervisor PC.

Data storage in a controller is limited compared to the storage available on a PC. Each time you save a controller station, the system makes a copy of the config.bog in the controller's memory. The save station job can also compress the HSQL database to remove empty space (requiring less memory and improving performance). This de-fragmenting of the database requires time, and may or may not be needed depending on how you use the system. You can enable and disable de-fragmentation as part of a station save. You can also manually initiate a station save with de-fragmentation.

Saving a station

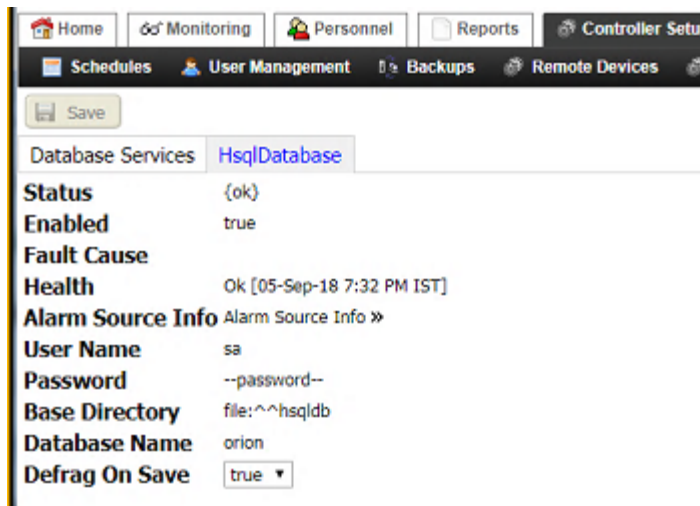
A station save captures all changes to the station's object spaces (components, alarm, history) to flash memory, saved as the files config.bog, alarm.zip and history.zip. You should save a station before upgrading and on other occasions.

Prerequisites:

You are working in the web UI.

- Step 1. Navigate to **Controller Setup > Miscellaneous > Configure Database** and click the **HsqlDatabase** tab.

The property sheet view opens.



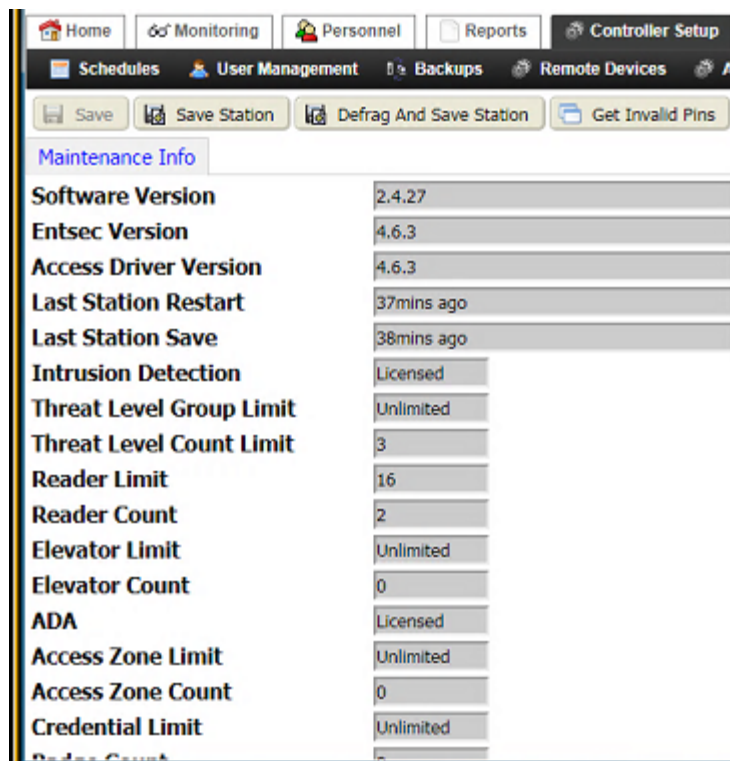
Step 2. Confirm that **Defrag On Save** is set based on your requirements.

Selecting **true** configures the system to empty space and compress (de-fragment) the database during the save station job. In a controller station, and depending on the volatility of your database, this de-fragmentation step could take a significant amount of time.

Selecting **false** configures the system to ignore empty space in the database, and just save the database as it is. This is the quicker option, however, and, again, depending on your database, you should regularly schedule a station save with de-fragmentation.

Step 3. Navigate to **Miscellaneous > Controller Maintenance**.

The Maintenance view opens.



Step 4. Do one of the following:

- Click **Save Station**. If **Defrag On Save** is set to **true**, the system de-fragments the database as part of the save job. If it is set to **false**, the job proceeds more quickly because no de-fragmentation takes place.
- Click **Defrag And Save Station**. If the HSQL database is configured for **Defrag On Save** set to **false**, this button overrides the **false** setting and de-fragments the database along with the save job.

Result

You can also configure Defrag on Save in Workbench (expand **Drivers > RdbmsNetwork > HsqlDatabase** and view the property sheet).

Data backup

System backups are an important part of a disaster recovery plan. Software backups should be done at an interval that matches the dynamic nature of a system.

For example, if a system has just a few database changes a month and history file retention is not critical, monthly backups may be sufficient. In a very dynamic system, where database retention is critical, backups may need to be done on a daily basis.

Three backup operations are available:

- A system backup combines a Supervisor station and one or more subordinate stations in a single backup job. System backups create *.zip files. To restore a system backup you must first un-zip the file using a third-

party data compression utility.

- A local backup creates a single compressed distribution file (*.dist) of a Supervisor or controller station. The restore job requires only the .dist file.
- You can use a station copy to back up all files and subdirectories.

After creating the backup, you should download it, copy it to a thumb drive or other storage medium, and store it off site in a secure location.

Software backups need to be stored at a secure location that is isolated from the system. When choosing how and where to store a backup, remember that system backups contain information that could be used to compromise the security of a system or network. You may send the backup to the local server drive or a mapped network drive. For disaster recovery purposes, it is recommended that the backup either be sent to a network drive at another physical location, or that auto archiving of the server be setup to archive to a remote server.

Backing up a local station


This procedure backs up the station you are currently logged into. This may be the Supervisor station or a remote controller station. The file created using this procedure is a compressed distribution (.dist) file.








Prerequisites:



Workbench is available on a PC connected to the network.

- Step 1. Using Workbench, determine what to exclude from the backup by editing the property sheet of the BackupService.

Property Sheet

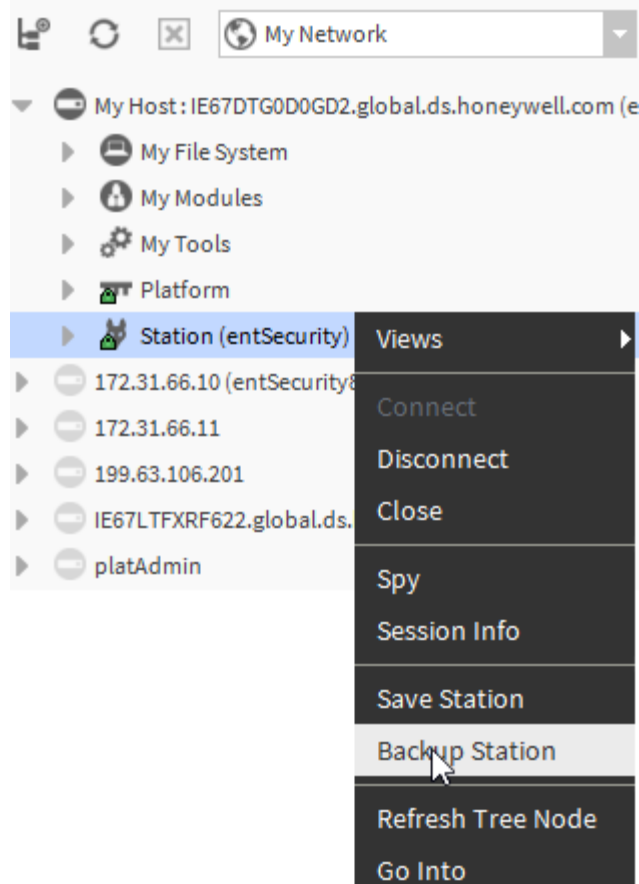
 BackupService (Backup Service)

 Status	{ok}
 Fault Cause	
 Enabled	<input checked="" type="radio"/> true
 Exclude Files	*.hdb;*.adb;*.lock;console.*;config.bog.*
 Exclude Directories	<div> file:^history file:^alarm file:^temp </div> <div>⊕ ✕</div>
 Offline Exclude Files	*.lock;console.*;config.bog.b*;config_ba
 Offline Exclude Directories	<div> file:^temp </div> <div>⊕ ✕</div>

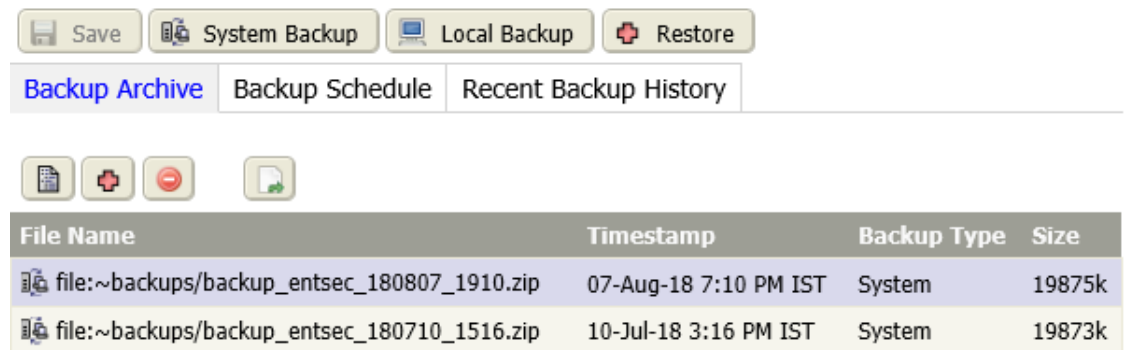
 Refresh  Save

The default settings do not back up the history files or alarm database. Access history is stored in the rdbms database so, unless you have critical trends running, there may be no need to back up the history files. The local backup files are also excluded from this backup because including previous backups in a backup file does not make logical sense and causes the backup file size to grow exponentially.

- Step 2. Do one of the following to make a distribution file backup of the existing controller station:
- If you are in Workbench, select the station in the Nav tree, right-click and click **Backup Station**.

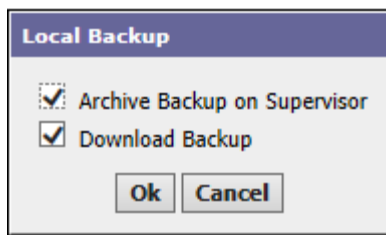


- To use the web UI, click **Controller (System) Setup > Backups**.



Step 3. Continuing with the Web UI, click the **Local Backup** button.

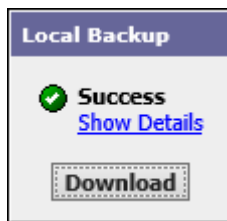
A Local Backup window opens.



The first option saves the file in the backups folder under the Supervisor station. The second option automatically downloads the backup to the computer's Downloads folder.

Step 4. To continue, click **Ok**.

The Job window displays a progress bar while the backup job runs. When the job is finished, the Local Backup window opens.



Step 5. Click the **Show Details** link to open a window that displays the history of this backup job.

Step 6. To save the backup *.dist file to a designated location, click the **Download** button. The browser prompts you to open or save the file. You cannot save it to the controller.

NOTE: You must save the file within five minutes of creating it. If you view the file, it opens from a temporary directory. You must designate a save-to location to save the file to a location other than the temporary location.

Step 7. Do one of the following:

- Choose to save the file.
- Choose to open the file.

If you chose to save the file, a browser prompts you to open the Downloads folder. If you chose to open the file, you can save it from the opening application interface (this must be a file-compression application).

Step 8. Make a note of the date and where you saved any downloaded backup files so you can find them later.

Backing up the station using station copier

This procedure is for replacing a current controller with a different model. To restore a station to a platform of a different type than the original platform on which the station was running, requires a station copy rather than the creation of a distribution file. This is because the distribution backup depends on platform files.

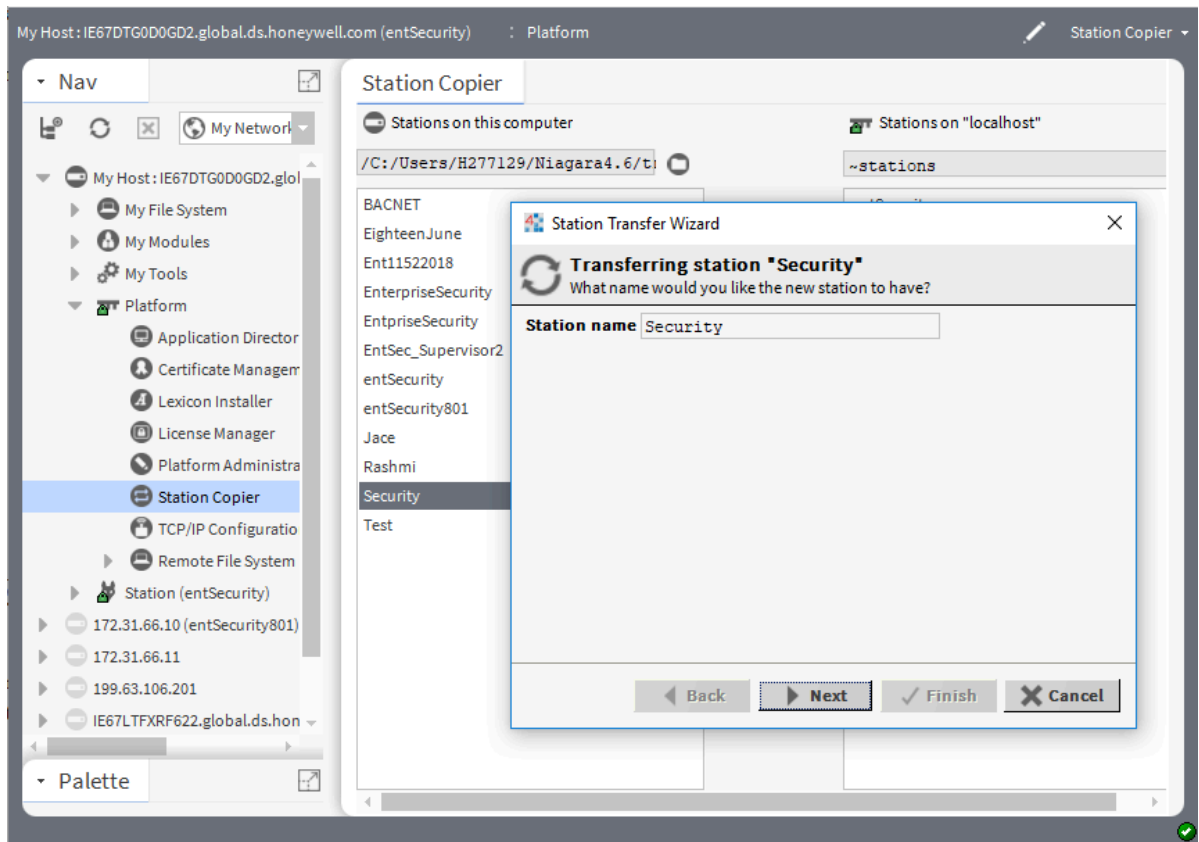
Prerequisites:

You need Workbench for this functionality. The web UI does not support a station copy.

Step 1. Connect a PC to the network and open Workbench.

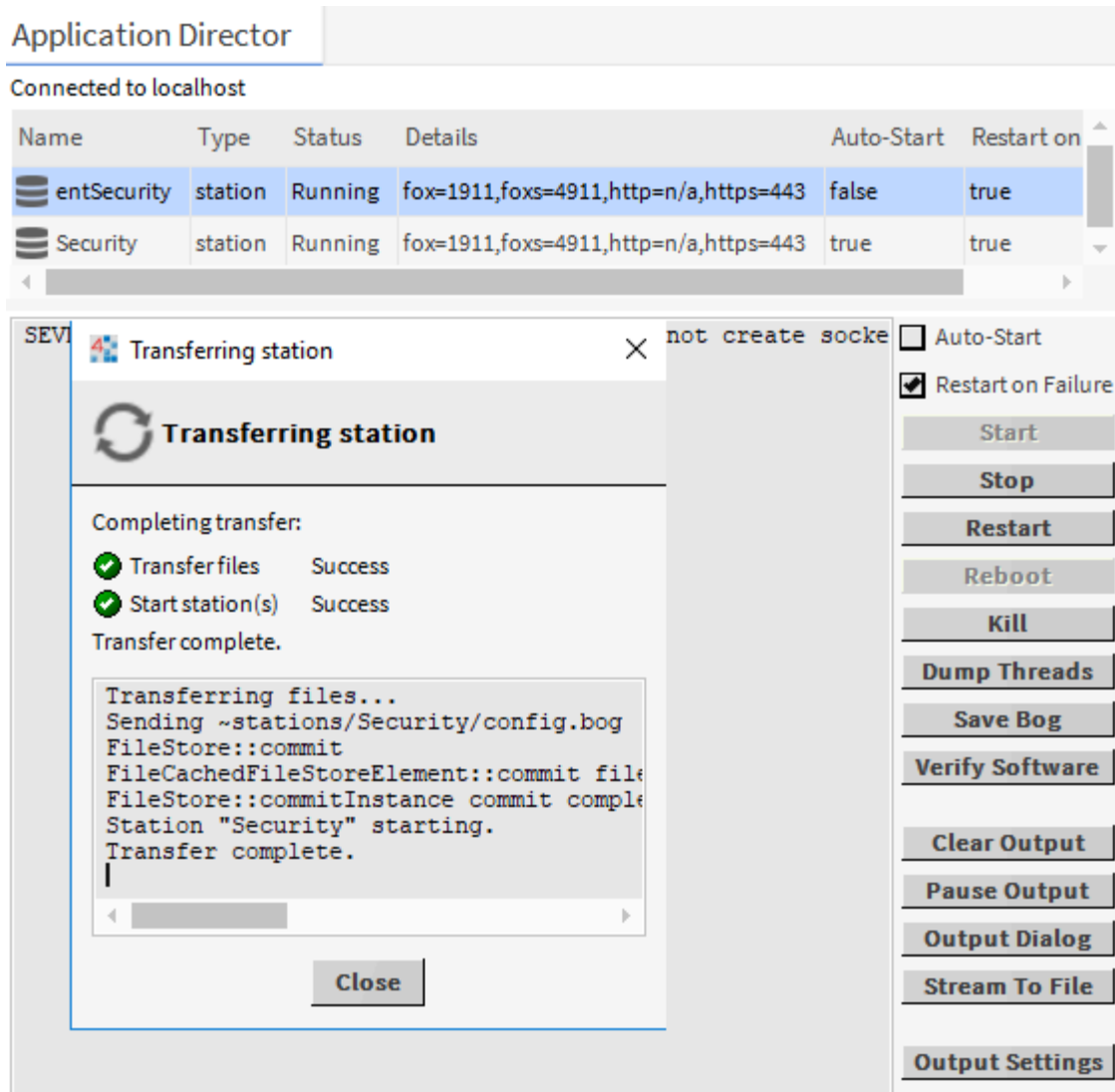
Step 2. To back up the station, expand the Platform node in the Nav tree and select the **Station Copier**.

The transfer wizard opens.



Step 3. Select the option to copy every file in the station and its subdirectories and click **Next**.

Step 4. Use the File Transfer Client to copy the `security` folder from the controller to a backup location (on your PC).



CAUTION: Do not overwrite the `security` folder in your Workbench. This folder contains encryption keys, which you will need in the new controller to decrypt user passwords.

Creating a system backup

Performing an ad hoc backup of a Supervisor station may be required if you are updating the station software or installing a new feature. System backups are available only for Supervisor stations. The system backup file contains backup files for the Supervisor station and all subordinate stations. A Local Backup backs up only the Supervisor station. The file created using this procedure is a compressed (.zip) file.

Prerequisites:

You are working in a Supervisor station.

- Step 1. From the Supervisor system main menu, select **System Setup > Backups**.
The Backups view opens.
- Step 2. Click the **System Backup** button.
A **System Backup** window opens. The first option saves the file in the backups folder under the Supervisor station. The second option automatically downloads the backup to the computer's Downloads folder.

- Step 3. To create the system backup, click **Ok**.
The **Job** window displays a progress bar while the backup job runs. When the job is finished, the **System Backup** window reports success or failure. Clicking the Show Details link opens a window that displays the history of this backup job.
- Step 4. To save the backup *.zip file to a designated location, click the **Download** button.
The browser prompts you to open or save the file.
NOTE: You must save the file within five minutes of creating it.
If you choose to open the file instead of having the browser save it, you can save it from the opening application interface (this must be a file-compression application).
- Step 5. If you chose to save the file, the browser prompts you to open the Downloads folder.
- Step 6. Click to open the folder and copy or cut and paste the file to a different location on the Supervisor's hard disk or thumb drive.
- Step 7. Should you need to restore the backup later, make a note of the date and where the file is located.

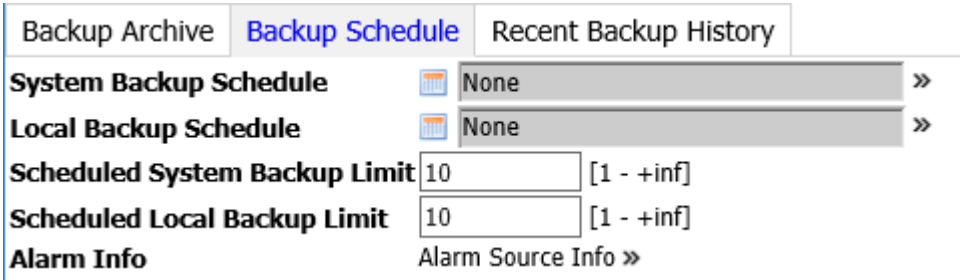
Creating a backup schedule for a system backup

Regularly backing up a Supervisor station consistently preserves data collected from all the remote controllers joined to the Supervisor. This is the recommended method to back up the system.

Prerequisites:

You are working in the Supervisor station. You chose a time when the system is least busy. The backup service may slow down system response.

- Step 1. Determine the frequency and time you want to backup the system.
- Step 2. From the main menu, select the following: **System Setup > Backups**, and click the Backup Schedule tab.
The Backup Schedule tab opens.



- Step 3. Click **System Setup > Schedules**, add a new schedule and click **Save**.

The schedule view opens.

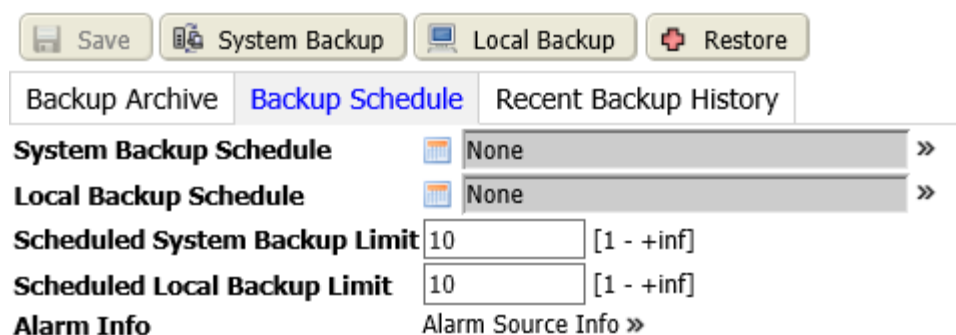
The screenshot displays the Scheduler interface with the following components:

- Navigation Bar:** Home, Monitoring, Personnel, Reports, System Setup, Photo ID, and a warning icon.
- Sub-Menu:** Schedules (selected), User Management, Backups, Remote Devices, Access Setup.
- Buttons:** Save, Schedules.
- Tabs:** Summary, Scheduler (selected), Schedule Setup, Special Events, Access Rights, Intrusion Pins.
- Tools:** A row of icons for various actions like delete, add, edit, etc.
- Schedule Grid:** A table with columns for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The rows represent time slots from 12:00 AM to 12:00 AM. A 'Granted' entry is visible in the Sunday column at 2:00 AM.
- Settings:**
 - Start:** 01:30 AM IST
 - Finish:** 03:00 AM IST
 - Output:** ☐ null ☒ Granted
- Note:** The Default Output for this Schedule is currently set to "Denied {ok}".

The example shows a backup occurring every Sunday morning at 2 AM.

Step 4. Click **System Setup** > **Backups**, and click the Backup Schedule tab.

The Backup Schedule tab opens.



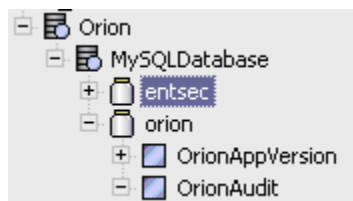
There are two backup schedules: system backup and local backup. The system backup backs up the server station and all subordinate stations, while the local backup only backs up the server station. You may want to schedule the local backup to occur more frequently than the system backup.

- Step 5. Assign the schedule to the backup job, and click **Save**.
When the backup job runs, the system saves the backup as a zip file that contains the distribution files for the Supervisor and all its subordinate controllers.

MySQL and MS SQL Database backups

The system is contained in an RDBMS (Relational Database Management System). This database contains all personnel, access right, credentials, access history, and other access information. The system supports a variety of databases: MySQL or MSSQL, HSQL, Orion.

Figure 20. MySQL database in the Workbench Nav tree



The backup does not include a MySQL database. You must make provisions to have this database backed up separately either using database tools, or system recovery backups.

If this database is lost, you can pull most of this information back up from the controllers, but any information programmed at the Supervisor level is lost.

Data restore

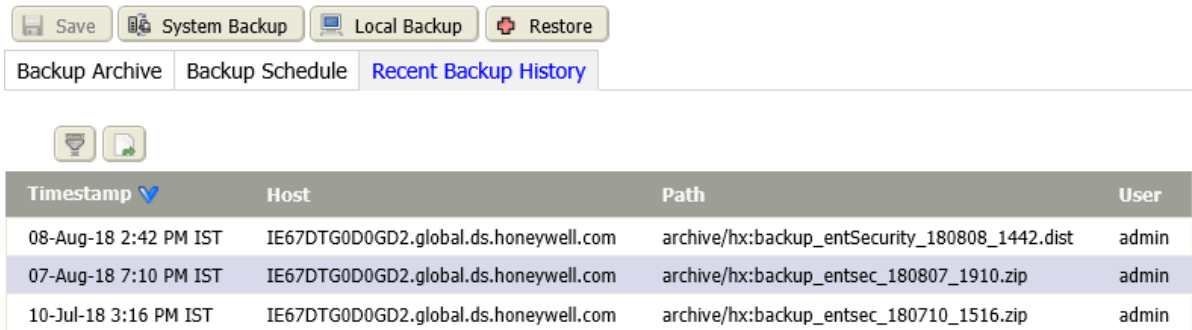
The Recent Backup History tab contains a table of all backups jobs that are run, even if the resultant backup file is not saved or downloaded to a designated location. This means that it is possible to see a file name listed in the Recent Backup History that is unavailable for restoring.

Due to stored dependencies, a distribution backup can only be restored to a like platform. To restore a station to a different platform model, rename the distribution backup to a zip file, extract the contents, and use the station copier to copy the station out of the backup without the rest of the information.

Viewing backup history

Before restoring a data backup, this procedure documents how to view the list of backups that have been made.

- Step 1. From the main menu, select **System (Controller) Setup > Backups**.
The Backups view opens.
- Step 2. Click the Recent Backup History tab.



Timestamp	Host	Path	User
08-Aug-18 2:42 PM IST	IE67DTG0D0GD2.global.ds.honeywell.com	archive/hx:backup_entSecurity_180808_1442.dist	admin
07-Aug-18 7:10 PM IST	IE67DTG0D0GD2.global.ds.honeywell.com	archive/hx:backup_entsec_180807_1910.zip	admin
10-Jul-18 3:16 PM IST	IE67DTG0D0GD2.global.ds.honeywell.com	archive/hx:backup_entsec_180710_1516.zip	admin

This tab lists all backup jobs.

NOTE: If the backup file was not saved or downloaded to a designated location, its file name may be listed in this table, but it may not be available to restore.

Restoring station(s) using the Web UI

You may need to restore a system or a local station. A system restore restores a Supervisor station and one or more subordinate stations in a single backup job. System backups are saved as *.zip files so you need to find the proper *.zip file to initiate a system restore. A local restore restores a single Supervisor or controller station. Local backups are saved as *.dist files, so you need to find the proper *.dist file to initiate a local restore.

- Step 1. From the main menu, select **System (Controller) Setup > Backups**.
The Backups view opens.
- Step 2. Click the **Restore** button.
The Restore from Backup Distribution File view opens.
- Step 3. Click the **Browse** button.
The **File Upload** window opens.
- Step 4. To initiate the restoration job, navigate to and select the file (*.zip for a system restore or *.dist for a local restore) and click the **Save** button.

NOTE: The Recent Backup History tab contains a table of all backup jobs that are run, even if the resultant backup file is not saved or downloaded to a designated location. This means that it is possible to see a file name listed in the Recent Backup History that is unavailable for restoring. The **Restore** window opens to let you select and confirm the station(s) that you want to restore.



Step 5. Confirm the identification of all selected stations and hosts.

CAUTION: Restoring the wrong station makes right station temporarily unavailable. Remember, the station is restored to its state at the time of the backup.

Step 6. To begin the restoration, click the **Ok** button.
A message prompts you to confirm the action.

Step 7. To confirm, click **Ok**.
The **Restore from Backup Distribution File** window displays a progress bar. When the job has finished, the **System Restore** window displays a message to let you know if the restoration succeeded or failed.

Step 8. If the restoration was successful, click the **Ok** button to close the **System Restore** window. If the restoration failed, lick the **View Details** link to help diagnose the problem.
The system restarts a restored station. This causes a temporary loss of communication.

NOTE: Restart takes several minutes. After a station restart, type in the login URL in the browser (a browser Refresh may not create a new station connection).

Troubleshooting

This topic identifies and documents some technical issues, error messages and provides an explanation.

While configuring a time range I got the message, "Advanced Filtering too Strict."


You have configured an illogical database inquiry. For example, you selected a specific date using a filter, then in the Advanced Time Range Options window you excluded a day of the week that corresponds to your selected date.

Change the filter or the options.

- **There is no capture button/icon on my Person view.** The capture icon (📷) requires a native badge designs device. If you see no capture button, your system has not been configured yet for the Photo ID feature.
- **I cannot find the window I am expecting to see.** Temporarily minimize your browser or other windows to see if the window is behind.
- **I cannot upload a photo to the database.** For you to upload a photo, the person must already exist in the database. Create and save the person, and then the upload icon will be available.

Badge creation troubleshooting

This topic identifies some technical issues and provides an explanation.

- **There is no capture button/icon on my Person view.** The capture icon () requires a native badge design device is added under the photo ID network be added to the station. If you see no capture button, your system has not been configured yet for the Photo ID feature.
- **I can't find the window I'm expecting to see.** Temporarily minimize your browser or other windows to see if the window is behind.
- **I cannot upload a photo to the database.** For you to upload a photo, the person must already exist in the database. Create and save the person, and then the upload icon will be available.