

# Technical Document

## **Niagara Enterprise Security Reference**

**March 25, 2025**



## Legal Notice

### Tridium, Incorporated

3951 Western Parkway, Suite 350  
Richmond, Virginia 23233  
U.S.A.

### Confidentiality

The information contained in this document is confidential information of Tridium, Inc., a Delaware corporation (Tridium). Such information and the software described herein, is furnished under a license agreement and may be used only in accordance with that agreement.

The information contained in this document is provided solely for use by Tridium employees, licensees, and system owners; and, except as permitted under the below copyright notice, is not to be released to, or reproduced for, anyone else.

While every effort has been made to assure the accuracy of this document, Tridium is not responsible for damages of any kind, including without limitation consequential damages, arising from the application of the information contained herein. Information and specifications published here are current as of the date of this publication and are subject to change without notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia.

### Trademark notice

BACnet and ASHRAE are registered trademarks of American Society of Heating, Refrigerating and Air-Conditioning Engineers. Microsoft, Excel, Internet Explorer, Windows, Windows Vista, Windows Server, and SQL Server are registered trademarks of Microsoft Corporation. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Mozilla and Firefox are trademarks of the Mozilla Foundation. Echelon, LON, LonMark, LonTalk, and LonWorks are registered trademarks of Echelon Corporation. Tridium, JACE, Niagara Framework, and Sedona Framework are registered trademarks, and Workbench are trademarks of Tridium Inc. All other product names and services mentioned in this publication that are known to be trademarks, registered trademarks, or service marks are the property of their respective owners.

### Copyright and patent notice

This document may be copied by parties who are authorized to distribute Tridium products in connection with distribution of those products, subject to the contracts that authorize such distribution. It may not otherwise, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Tridium, Inc.

Copyright © 2025 Tridium, Inc. All rights reserved.

The product(s) described herein may be covered by one or more U.S. or foreign patents of Tridium.

For an important patent notice, please visit: <http://www.honpat.com>.

# Contents

<b>About this reference</b>	11
Document change log	11
Related documentation	12
<b>Chapter 1. Home</b>	13
Standard control buttons	13
Column Chooser view	15
Controller (System) Setup views	18
User interface	18
Graphics configuration	20
Standard properties	22
<b>Chapter 2. Monitoring views</b>	25
Alarm Console — ConsoleRecipient view	25
Alarm Console control buttons	26
Alarm Console columns	27
Alarm Console Info icons	28
Alarm Console links	29
Show Alarm Details window	29
Notes window	31
Alarm Filter window	32
Multi Source View Options window	34
AX Alarm console	35
Console Layout window	37
Activity Monitor view	38
Edit (configure) Activity Monitor view, Activity Monitor tab	40
Activity Monitor Alarm Classes tab	41
Activity Monitor Filter window	42
Video monitoring views	43
Surveillance viewer	44
Playback viewer	44
<b>Chapter 3. Personnel views</b>	49
People view	49
Quick Edit window	51
People View Filter window	51
Add New (or edit) Person view	52
New person Summary tab	55
New Person Access Rights tab	56
Change Assignment Properties window	57
Access Rights Summary window	58
Add Access Rights filter window	59
Badges tab	60
Badges Summary tab	61

Badges view .....	62
Quick Edit window .....	63
Badges Filter window .....	65
Enroll New Badge view .....	66
Enroll New Badge Summary tab .....	67
Add (or edit) New Badge view .....	68
Add New Badge Summary tab .....	70
Badge tab .....	70
Batch Enroll Badges view, Badge tab .....	72
Batch Enroll Summary tab .....	73
Range Create Badges view, Badge tab .....	74
Range Create Badges Summary tab .....	76
Access Rights view .....	77
Access Rights Summary tab .....	79
Quick Edit window .....	80
Filter window .....	82
Add New (and edit) Access Rights view, Access Right tab .....	83
People tab .....	85
Readers tab .....	86
Readers tab, Summary window .....	88
Readers tab, Filter window .....	89
Floors tab .....	89
Floors tab, Filter window .....	91
Tenants view .....	91
Tenants Summary window/tab .....	93
Filter window .....	93
Add (or edit) a New Tenant view .....	94
Tenants Niagara Integration IDs tab .....	94
Tenants Intrusion Pins tab .....	95
Tenants People tab .....	97
Tenants Badges tab .....	98
Tenants Threat Level Groups tab .....	99
Tenants Access Rights tab .....	100
Additional Personnel Data view .....	101
Additional Personnel Data Summary window/tab .....	102
Additional Personnel Data Filter window .....	102
Add (or edit) an Info Template view .....	103
<b>Chapter 4. Reports views .....</b>	<b>105</b>
Advanced Time Range Options window .....	106
Access History Report and Summary window .....	107
Purge Config window (simple) .....	108
Purge Config window (expanded) .....	109
Access History Filter window .....	110
Manage Reports window .....	111
Add (or edit) Report window .....	112



Schedule Emailed Report window .....	113
Alarm History report .....	114
Alarm history Summary window .....	115
Review Video view .....	117
Alarm history Filter window .....	117
Attendance History Report and Summary window .....	119
Manual Add (attendance record) window .....	120
Manual Hide (confirmation) window .....	121
Attendance History Filter window .....	121
Intrusion History report and Summary window .....	122
Intrusion History Filter window .....	124
Audit History Report and Summary window .....	125
Log History Report and Summary window .....	127
Log history Filter window .....	128
Hardware reports .....	129
Doors Report and Filter window .....	129
Readers Report and Filter window .....	130
Inputs Report and Filter window .....	131
Outputs report and Filter window .....	132
Elevators Report and Filter window .....	132
Remote Modules Report and Filter window .....	133
BACnet Points and Filter window .....	135
Intrusion Displays Report and Filter .....	136
Consolidated Intrusion Displays report .....	137
LDAP Audit History report .....	137
Miscellaneous reports .....	138
Person Access Right Report .....	138
Person Reader Report .....	139
Access Right Reader Report and Filter window .....	141
Personnel Changes report and Summary window .....	142
Personnel Changes Filter window .....	142
<b>Chapter 5. Controller (System) Setup-Schedules .....</b>	<b>145</b>
Schedules view .....	145
Add a new Schedule window .....	146
Schedules Quick Edit window .....	147
Schedules Filter window .....	148
Add New (edit or duplicate) Schedule view .....	148
Schedule, Summary tab .....	150
Scheduler tab .....	151
Schedule Setup (weekly schedules) tab .....	152
Special Events tab .....	155
Access Rights tab .....	163
Intrusion Pins tab .....	164
Calendar Schedules view .....	166
Calendar Schedules Filter window .....	167

	Add New (or edit) Calendar Schedule view .....	168
	Events tab .....	169
	Schedule Setup (calendar schedules) tab .....	170
<b>Chapter 6.</b>	<b>User management .....</b>	<b>173</b>
	View Graphic .....	173
	Graphic Editor view .....	174
	About the Graphic Editor canvas .....	174
	About Graphic Editor objects (widgets) .....	176
	About the Graphic Editor toolbar .....	177
	About the side bar pane .....	177
	Graphic Editor pop-up menu - available video cameras .....	179
	Images view .....	181
	Add New Image view .....	181
	Display Image view .....	182
	Navigation Groups view .....	182
	Add New (or edit) Nav Group view .....	183
<b>Chapter 7.</b>	<b>Controller (System) Setup–Backup views .....</b>	<b>185</b>
	Backups view .....	185
	System Backup/Local Backup window .....	186
	Backup Archive tab Summary window .....	187
	Backup Archive tab Restore windows .....	187
	Backup Schedule tab .....	188
	Recent Backup History tab .....	190
	Recent Backup History tab Filter window .....	190
	Restore from Backup Distribution File or System Backup File views .....	191
<b>Chapter 8.</b>	<b>Controller (System) Setup–Access Setup .....</b>	<b>193</b>
	Access Zones views .....	193
	Add New (or edit) Access Zone view .....	194
	Add new Access Zone Summary tab .....	197
	Access zone Activity Alerts Ext tab .....	198
	Occupants tab .....	199
	Access Zone Supervisors tab .....	200
	Entry Readers tab .....	201
	Exit Readers tab .....	202
	Grouping tab .....	203
	Card Formats view .....	204
	Wiegand Format Editor view, Wiegand Format tab .....	205
	Wiegand Format Summary tab .....	209
	Access Control Setup view .....	210
	Additional Personnel Entry — Import Info tab .....	211
	Data to import .....	212
	Export Personnel Records window .....	214
<b>Chapter 9.</b>	<b>Controller (System) Setup–Intrusion Setup .....</b>	<b>217</b>
	Intrusion Pins view .....	217

Add New (or edit) Intrusion Pin view, Intrusion Pin tab .....	218
Intrusion Pins Summary tab .....	219
PIN Intrusion Zones tab .....	219
Intrusion Zones views .....	221
Add New (or edit) Intrusion Zone view .....	221
Manual Override window .....	224
Intrusion Zone Summary tab .....	225
Intrusion Displays tab (learn mode) .....	225
Readers tab .....	227
Points tab .....	227
Grouping tab .....	229
Recipients tab .....	229
Escalation Level tabs .....	230
Relay Links tab .....	231
Edit Existing Intrusion Pin view .....	233
Intrusion Displays views .....	234
Add New (or edit) Intrusion Display view .....	234
Virtual Display tab .....	237
Intrusion Display tab (configuration) .....	238
Intrusion displays Activity Alert Exts tab .....	239
Display Intrusion Zones tab .....	239
<b>Chapter 10. Controller (System) Setup–Alarm Setup .....</b>	<b>243</b>
Alarm Classes views .....	243
Add New (or edit) Alarm Class view .....	244
Recipients tab .....	246
Relay Links tab .....	248
Alarm Instructions view .....	249
Edit Instructions window .....	250
Master Instructions window .....	251
Alarm Relays view (Alarm Count Relays) .....	251
Add New (or edit) Alarm Count To Relay view .....	252
Alarm Classes tab .....	253
Relays tab .....	254
EmailService view (Email Accounts) .....	255
Outgoing Account tab .....	256
Incoming Account tab .....	260
Email Recipients view .....	262
Add New (or edit) Email Recipient view .....	263
Alarm Classes tab .....	266
Alarm Consoles view .....	267
Add (or edit) Alarm Console view, Alarm Classes tab .....	268
Add (or edit) Alarm Console view, Alarm Classes tab .....	269
Video Alarm Classes (Video Alarm Recipient) view .....	271
Alarm Classes tab .....	272

Station Recipients views .....	274
Add New (or edit) Station Recipient view .....	274
Alarm Classes tab .....	275
Power alarm Setup (PlatformServices) view .....	277
Alarm Extensions view .....	279
Edit Alarm Extension properties (Alarm Source Info tab) .....	280
<b>Chapter 11. Controller (System) Setup–Miscellaneous .....</b>	<b>283</b>
Keypad Formats (Keypad Configuration) view .....	283
Add New (or edit) Keypad Format view .....	284
Pdf Styles view .....	285
Add New (or edit) PDF Styles view .....	285
License Manager view .....	287
Network TCP/IP Settings view .....	288
Maintenance view (Server) .....	294
Update Reader Count window .....	298
Get Corrupt Pin Numbers window .....	299
Configure Database view, Database Services tab .....	300
Database Configuration tab (HsqliteDatabase) .....	302
Database configuration tabs (MySQL and SqlServer databases) .....	303
Web Service view .....	305
HTTP Header Providers view .....	309
Job Service view .....	314
System Date Time Editor view .....	315
End User Licenses Agreement view .....	316
Third Party Licenses view .....	316
Controller TimeServers Settings .....	316
<b>Chapter 12. Controller (System)–Miscellaneous Graphics .....</b>	<b>321</b>
Graphics view (Graphics Management) .....	321
Add a graphic window .....	323
Modify Settings window .....	323
Edit Nav window .....	324
Types of bindings .....	324
About bound label bindings .....	325
About value bindings .....	326
About spectrum bindings .....	328
About set point bindings .....	330
About Increment Set point bindings .....	330
About spectrum set point bindings .....	331
Relative and absolute bindings .....	332
About action bindings .....	333
View Graphic .....	333
Graphic Editor view .....	334
About the Graphic Editor canvas .....	335
About Graphic Editor objects (widgets) .....	337

About the Graphic Editor toolbar .....	338
About the side bar pane .....	338
Graphic Editor pop-up menu - available video cameras .....	340
Images view .....	342
Add New Image view .....	342
Display Image view .....	343
Navigation Groups view .....	343
Add New (or edit) Nav Group view .....	344
<b>Chapter 13. Threat Levels .....</b>	<b>347</b>
Threat level groups view .....	347
Threat Level Group filter .....	348
Activate Threat Level window .....	349
Retrieve Active Level Activation Status window .....	349
Add New (or edit) Threat Level Group view .....	350
Summary Tab .....	352
Activation Badges tab .....	353
Access Rights tab .....	353
Remote Stations tab .....	354
Threat Level Setup view .....	355
Activation alerts .....	357
Add (or edit) threat level window .....	359
Edit instructions window .....	360
Edit metadata windows .....	360
<b>Chapter 14. LDAP network driver views, tabs and windows .....</b>	<b>363</b>
LDAP Network view .....	363
Ldap Servers tab .....	366
New (and Edit) LDAP server window .....	368
Import Preferences window .....	370
Ldap Server view .....	372
Attributes tab .....	381
Add attribute window .....	384
Groups tab .....	385
LDAP Audit History view .....	387
Periodic Purge Schedule .....	388
Ldap Driver Device Manager .....	388
<b>Chapter 15. Nrio Driver views, tabs and windows .....</b>	<b>391</b>
Nrio Device Manager view .....	391
Nrio Module view .....	392
Nrio Point Manager, Analog Points tab .....	394
Manage Nrio Points windows .....	395
Go to Module window .....	396
Digital Points tab .....	396
Nrio Point Edit view .....	397
Voltage Input points properties .....	398

Temperature Input points .....	403
Resistive Input points .....	410
Digital input points .....	416
High Speed Counter .....	421
Relay Output points (digital) .....	428
Voltage Output points .....	433
Manage Extensions windows .....	439
History Setup tab .....	439
Active Schedule tab .....	440
Link to tab .....	441
Link From tab .....	442
History Extension view .....	443
Set COM Port window .....	446
Upload window .....	447
Download window .....	448
Filter window .....	448
<b>Chapter 16. Obix Network view .....</b>	<b>451</b>
Obix links .....	451
<b>Chapter 17. Photo ID management .....</b>	<b>453</b>
Photo ID Network view .....	453
Photo ID Add device window .....	454
Settings window .....	455
Configure window .....	456
Asure ID Client Device view .....	457
Templates tab .....	459
Asure ID Device.[template] view .....	460
Tenants tab .....	460
Badges tab .....	460
Edit Photo ID Template Data view .....	461
Photo ID Viewers view .....	461
Photo ID Viewer (surveillance) view .....	462
<b>Chapter 18. Components NAC Driver Module .....</b>	<b>465</b>
nacDriver-NACNetwork .....	465
nacDriver-NACController .....	467
nacDriver- Nac Point .....	468
nacDriver nacDoor .....	470
nacDriver-nacReader .....	473
nacDriver-NACFirmwareInstanceContainer .....	474
nacDriver-nacDoorModeSchedule .....	475
nacDriver-nacActivityAlertView .....	476

## About this reference

Niagara Enterprise Security Niagara Enterprise Security (the system) is a fully-featured product designed to manage building access control in both small and large installations. This reference supports the Niagara Enterprise Security browser interface and is especially valuable for learning about individual properties, views, windows and reports as they appear in a browser.

### Audience

The information in this reference is for Systems Integrators and Facility Managers who are responsible for configuring the tools used to manage complex building systems.

### Document Content

This reference explains each property and system component.

### Product Documentation

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

## Document change log

This topic provides a summary list of the changes made to this document.

### March 25, 2025

- Added Components-Nac Driver Module Chapter.
- Removed "Password" property and added the new property description for "privileged UserName" in the "Database Configuration tab" topic.
- Removed references to Assure ID.

### February 16, 2023

Updated reused property descriptions across all topics.

### June 28, 2022

Updated LDAP network driver chapter.

### October 6, 2021

Removed the Supervisor TimeServers Settings topic. LDAP network driver

### February 22, 2021

Removed the Workbench module, plugin and window chapters from this reference to a separate document.

### January 21, 2021

Added the topic "Http Header Providers view" to the "Controller (System) Setup-Miscellaneous" chapter.

Added component topics for the entsec module.

### April 23, 2020

- Added component chapter to document the accessDriver module.
- Added video controls to Video Playback topic.
- Removed reference to view title on Add New User view (not included in this version of software)
- Added missing property descriptions.
- Removed references to the passkey, which is no longer supported.
- Reorganized video views in the Remote Devices chapter in a more logical order.

- Reused a number of property descriptions, expanded some descriptions and added missing descriptions.
- Added the Maxpro video driver.
- Updated Milestone topics.
- Updated the WebService Web Launcher properties.

#### August 8, 2019

- Updated procedure for creating MySQL database to include creating a user other than "root."
- Removed references to the system passkey, which is no longer required.

#### December 13, 2018

- Added two topics for NTP server views.
- Added content to the Milestone DVR and video camera topics. Changes are in the Controller (System) SetupRemote Devices
- Made general edits to several additional topics throughout the document.

#### September 17, 2018

- Initial release.

### Related documentation

Several documents provide additional information about this software.

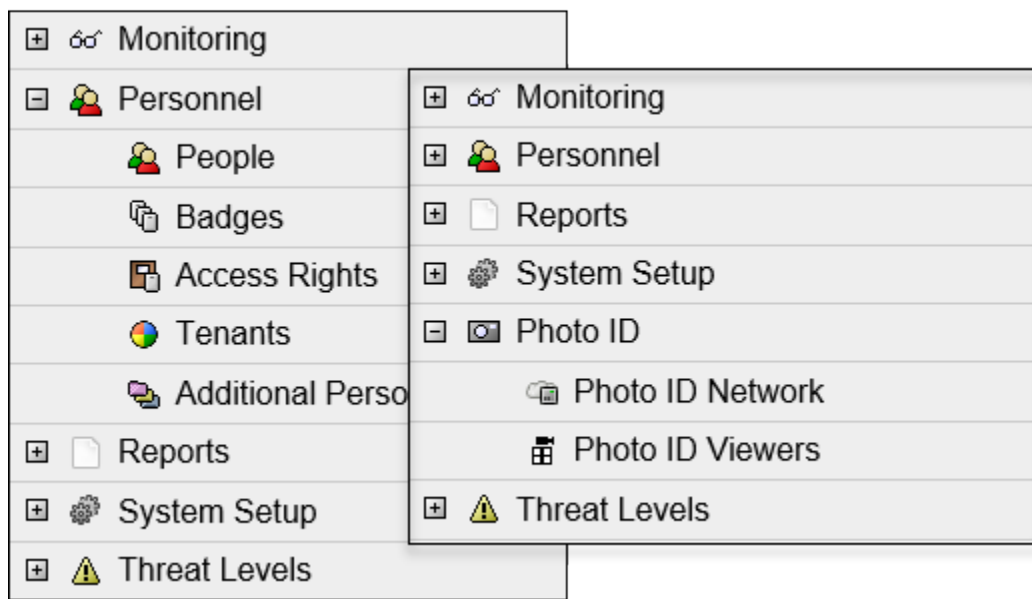
- *Niagara Enterprise Security Operator's Guide* provides procedures for daily activities including badge creation and alarm management.
- *Niagara Enterprise Security Facility Manager's Guide* provides procedures for managing personnel and system components.
- *Niagara Enterprise Security Installation and Maintenance Guide* serves the needs of the system integrator who is responsible for setting up and configuring the system.
- *Niagara Station Security Guide*
- *Niagara FIPS 140-2 Configuration Guide*
- *Niagara Video Framework Guide*



# Chapter 1. Home

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

**Figure 1.** Home menu with Personnel expanded



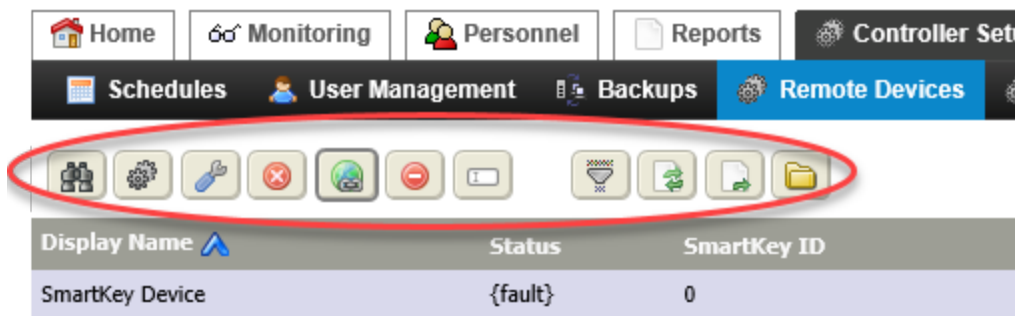
The screen capture shows examples of two home menus. The one on the right includes the Photo ID network.

- **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)** provides access to a wide variety of configuration menus that you can use to setup hardware, alarms, access and intrusion zones, and other functions.
- NOTE:** For Supervisor stations, the **Controller Setup** menu is titled **System Setup**.
- **Photo ID Network** manages the components used to create photo IDs.
  - **Threat Levels** configures how the system responds to external threats.

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











## Standard control buttons

Many views include a row of almost square, control buttons along the top of the view. While some control buttons in each view serve specific, view-related functions, a number of these buttons are present in almost every view. The documentation for an individual view may or may not include a description of these buttons.

**Figure 2.** Control buttons example

Control buttons are context sensitive to the data and type of view. Tool tips identify the function of each control button. Buttons are dimmed when the function is unavailable. These are the most common buttons that may not be defined in the topics that follow:

- Add opens a view or window for creating a new record in the database.
- Assign Mode buttons open and close the Unassigned pane.
- Column Chooser opens the **Columns for...** view from which you can add data columns to, remove them from, and reorder them in the current table.
- Delete removes the selected record (row) from the database table. This button is available when you select an item.
- 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 point values as well as properties provided by the database.
- Duplicate opens a **New** window and populates each property with properties from the selected item. Using this button speeds the item creation.
- Edit opens the component's Edit window/
- Export opens the Export window for creating a PDF or CSV formatted report of the current table.
- Filter buttons open the Filters window, which defines a query action for limiting the output visible in tables and reports. The gray version indicates unfiltered data. The red version indicates filtered data.
- Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.

-  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.).
-  Manage Devices/Drivers opens the Manage Drivers or Manage Devices window, which is used to Add, Delete, Rename, Duplicate, Copy, and Cut system drivers or devices.
-  Manage Reports opens the Manage Reports window from which you can add a report or schedule a report to be emailed.
-  or  Ping (or wink) sends a command to the remote device or server.
-  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.
-  Refresh updates the table, clearing row selections in all panes.
-  Rename opens the Rename window with which to change the name of the selected item.
-  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.
-  Move Up and Move Down change the sequence of rows in the direction indicated one selected row at a time.

## Column Chooser view

This view configures the columns to include in a table view. The columns to choose depend on the particular target view.

**Figure 3.** Example of a Column Chooser view

Home

Monitoring

Personnel

Reports

Controller S

People

Badges

Access Rights

Tenants

Additional I

Columns for People

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

entsec:Person

Report Type

Optimized


Pre-Filtering

false

Add Column

Default Table


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	

To open this type of view, click the Column Chooser button () at the top of a table.

The table at the top of this view lists the columns currently included on the target table view. The table at the bottom of this view provides the mechanism for choosing the properties to include as table columns.


**Control buttons**

In addition to the standard control buttons (Save, Edit, Delete, Column Chooser and Export) these buttons provide specific functions:

-  Move Up and Move Down change the sequence of rows in the direction indicated one selected row at a time.

## Links

- Add Column** adds the selected column to the table, which appears as a row in the table at the top of the view.
- Default Table** removes any added or reorganized table columns and returns the table to the default columns.

Property	Value	Description
Row Type	read-only	
Pre-Filtering	true or false (default)	<p>Controls the availability of filtering options.</p> <p><b>true</b> opens the Filter window each time the system opens a Person page.</p> <p><b>false</b> opens the Filter window only when you click the Filter button (  ).</p>
From column	drop-down list	Selects the source tables from which to select additional columns for the current table.
Property column	drop-down list	<p>Lists the source table's properties from which to choose an additional column. Clicking Add Column adds this property to the current table.</p> <p>Some properties are linked to the additional properties. Clicking a property in the <b>Property</b> column populates the <b>Linked Property</b> column.</p>
Linked Property	drop-down list	<p>Displays the properties of another table that is linked to this table. Clicking Add Column adds a property from the related table to the current table.</p> <p>For example, Person is linked to the Access Rights and Tenant. When you select Person in the From Column, it displays the properties of Person in the Property Column. When you</p>

Property	Value	Description
		select Tenant in the Property Column, it displays the properties of Tenant in the Linked Property column.

Controller (System) Setup views

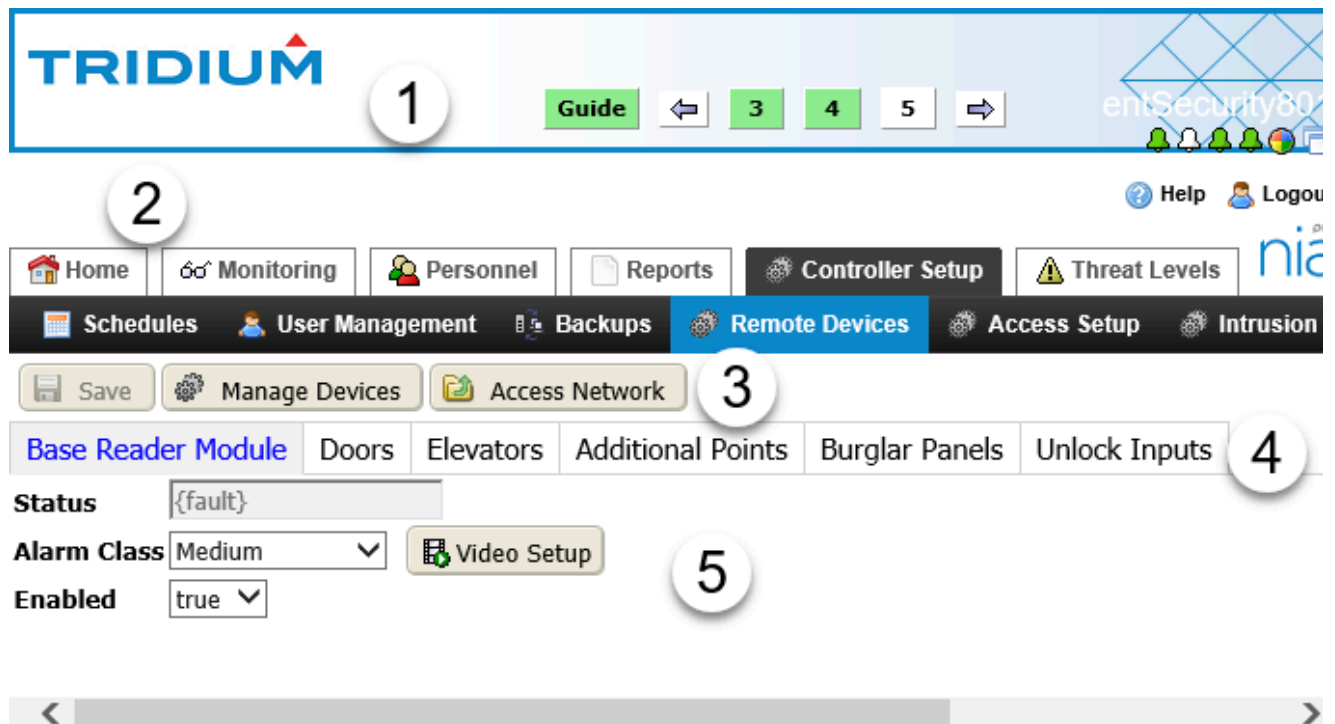
Setup views configure system components and network properties, as well as user preferences and other variables.

In a Supervisor station, the views are part of **System Setup**, whereas, in a remote host controller station, these views are part of **Controller Setup**. The differences have to do with configuring Supervisory components vs. configuring the devices connected to each controller. Many functions are available in both interfaces.

Supervisor System Setup views	Controller Setup views
Schedules	Schedules
User Management	User Management
Backups	Backups
Remote Devices	Remote Devices
Access Setup	Access Setup
Intrusion Setup	Intrusion Setup
Alarm Setup	Alarm Setup
Miscellaneous	Miscellaneous

User interface

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

**Figure 4.** Example user interface

1. Title bar
2. Menu bar
3. Links
4. Tabs
5. 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.

## Graphics configuration

A graphic provides a visual display of an access control area, can simulate actions including: doors opening and closing, readers scanned, intrusion zones enabled, etc., report on current conditions, and include buttons for implementing area-wide controls, such as turning on video surveillance and triggering threat level actions. A graphical representation of reality enables operational personnel to respond quickly to threats in real time.

### Target media

Prior to Niagara 4.9, no custom Px graphics ran in a browser (required by the web UI). Instead, they used the Java Web Start applet, which ran outside of the browser. The release of Niagara 4.9 replaced Web Start with Java Web Launcher for Px graphics that still require an external applet. Other Px graphics support HTML5, which runs in a browser.

The Graphic Editor supports two client-side, Px **Target Media** technologies:

- **HxPxMedia** are designed for the web UI. Three widgets render in a browser using HTML5: LiveVideoPlayer, Control Panel and CameraWidget. The remaining widgets: PanTiltJoystick, ZoomSlider, MouseDownButton and VideoMultistreamPane require Web Launcher and render outside of the browser.
- **WorkbenchPxMedia** are designed for the Workbench interface. When used in the web UI, all widgets require the Web Launcher (applet).

The Graphic Editor advises you if you use a feature in a widget that is not supported by the target technology.

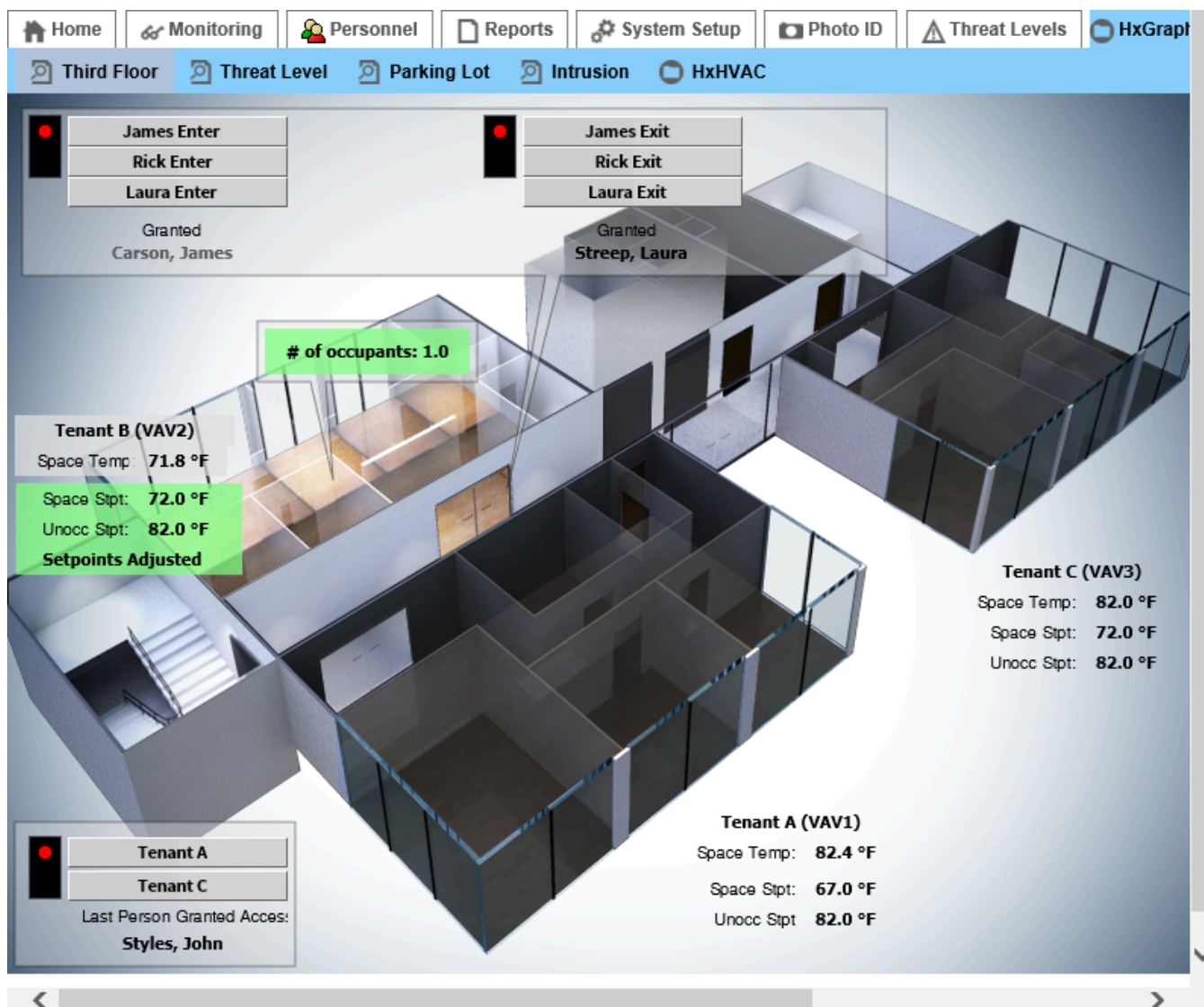
Consider carefully the basic capabilities and limitations of each technology. Obviously, a mobile phone is limited as to what it can useably display when compared to a graphic viewed in a web browser running on a computer. Keep this in mind, and test your views in all target media as you develop them.

The *Niagara Graphics Guide* documents in detail the capabilities of Hx and Px graphics. The *Niagara Video Framework Guide* documents the videoDriver module and palette.

### Summary steps

Configuring a graphical representation of a facility begins by hiring a graphics artist to create a set of three-dimensional images to represent the building, including all areas, such as the parking lot or garage, to be monitored. The images should be readily recognizable as belonging to the facility, looking down from above each floor.



**Figure 5.** A 3D image of a floor in a building

The screen capture shows an image of a single floor in a building with overlaid controls for visually monitoring access control.

The general process of creating presentation views for access control follows these general steps:

1. **Create a view**

Creating a view sets up a canvas on which to construct a representation of your facility. This view establishes a relationship between a Px file and one or more components of various types, such as folders, doors and readers.

2. **Add widgets**

A widget is a graphic visualization of an access component. You add widgets to the canvas.

3. **Bind your data to the widgets**

Data binding passes data collected from the access components to the widgets. These bound data

objects animate (update) the widgets in real time.

#### 4. Create a nav file

A .nav file sets up a customized tree structure so that users can easily access your views. You edit the .nav file using the Nav File Editor and assign a particular nav file to a user in the user's profile (using the User Manager view).

#### 5. Create and distribute a report

Reports display and deliver data to online views, printed pages, and for distribution via email.

## Standard properties

Many system property sheets include a set of common properties that provide status and other information.

Property	Value	Description
Status	read-only	<p>Reports the condition of the entity or process at last polling.</p> <p>{ok} indicates that the component is licensed and polling successfully.</p> <p>{down} indicates that the last check was unsuccessful, perhaps because of an incorrect property, or possibly loss of network connection.</p> <p>{disabled} indicates that the <b>Enable</b> property is set to <code>false</code>.</p> <p>{fault} indicates another problem. Refer to <b>Fault Cause</b> for more information.</p>
Enabled	true or false	<p>Activates (<code>true</code>) and deactivates (<code>false</code>) use of the object (network, device, point, component, table, schedule, descriptor, etc.).</p>
Fault Cause	read-only	<p>Indicates the reason why a system object (network, device, component, extension, etc.) is not working (in fault). This property is empty unless a fault exists.</p>
Health	read-only	<p>Reports the status of the network, device or component. This advisory information, including a time stamp, can help you recognize and troubleshoot problems but it provides no direct management controls.</p>

Property	Value	Description
		The <i>Niagara Drivers Guide</i> documents the these properties.
Alarm Source Info	additional properties	<p>Contains a set of properties for configuring and routing alarms when this component is the alarm source.</p> <p>For property descriptions, refer to the <i>Niagara Alarms Guide</i></p>



# Chapter 2. Monitoring views

The Monitoring menus provide access to three system monitoring functions: Alarm Console, Activity Monitor and Video Monitoring.

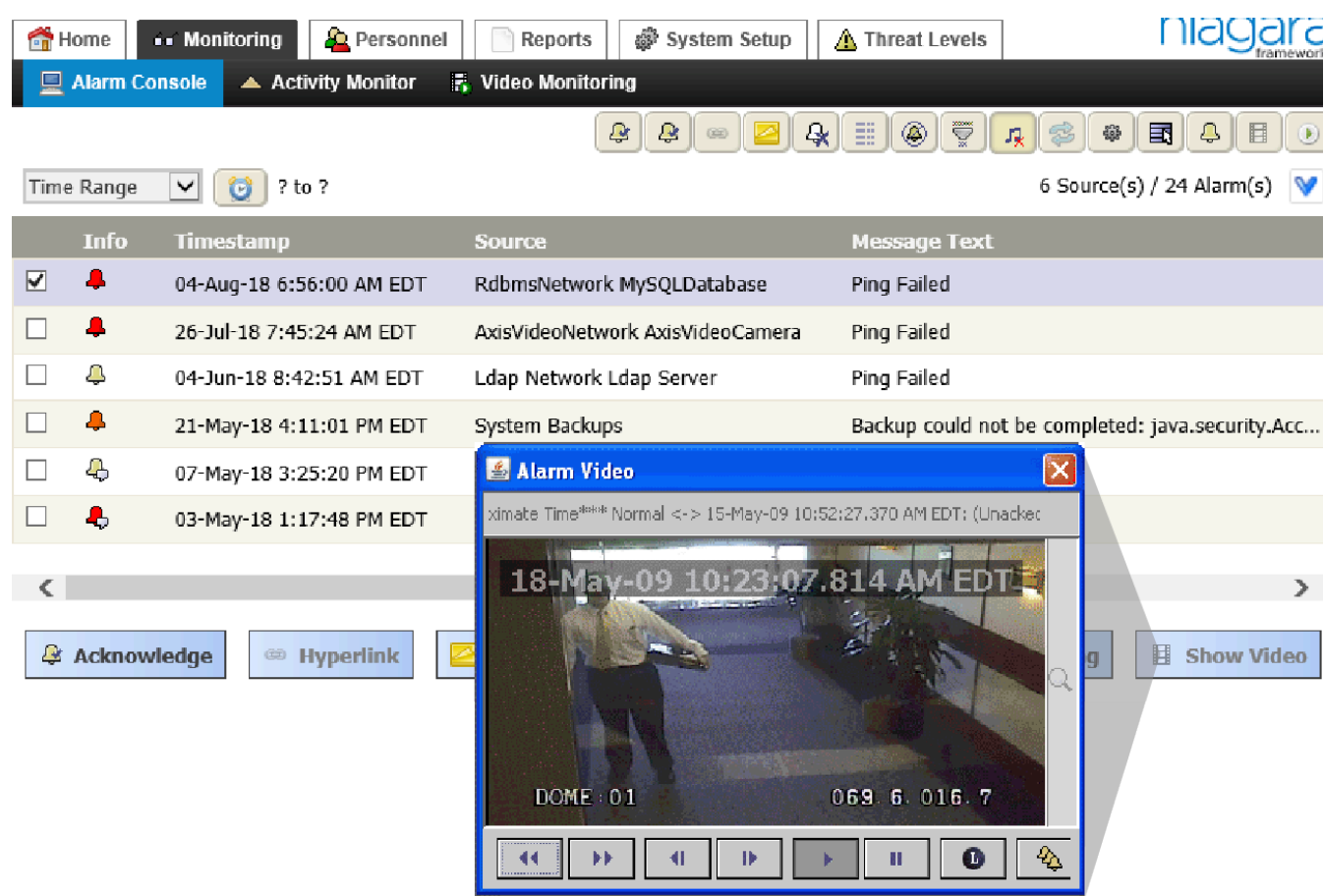
The monitoring views include the:

- Alarm console views: Alarm Console and Recurring Alarms. The latest alarms are listed at the top.
- Activity Monitor views
- Video monitoring views

## Alarm Console — Console Recipient view


This multi-source view provides a real-time alarms table to manage alarms on a per-point basis.

**Figure 6.** Open alarm sources view (Alarm Console with video alarm)



You access this view by clicking the **Monitoring** in the menu tree or by expanding **Monitoring** and clicking **Alarm Console**.

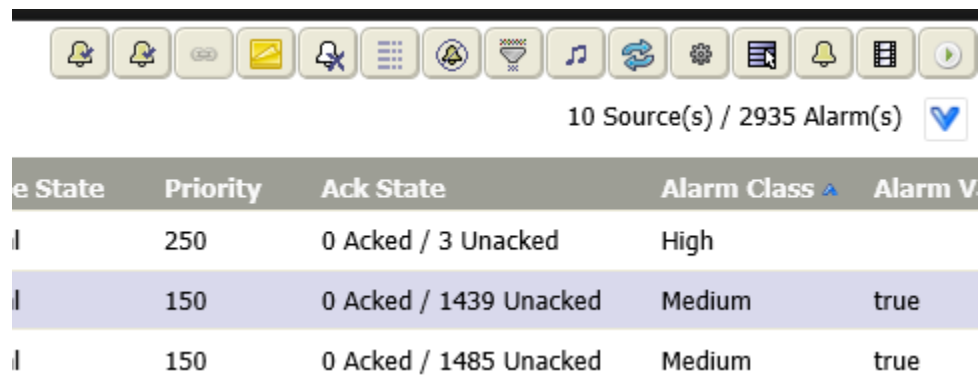
This view displays all the current alarms with constant live updates from a single, specific point. The latest alarms are listed at the top of the view. Each row represents an alarm source. The **Time Range** drop-down list









and time picker button (  ) to the left about the table columns filter the table by date and time.










Alarm Console control buttons

You work with the alarms in the **Alarm Console** view by selecting one or more rows and clicking a control button

**Figure 7.** Alarm Console row of buttons



-  Acknowledge the selected alarm(s) recognizes that an alarm state exists at the point(s) represented by the selected row(s) in the table. This button displays on the Alarm Console view and on the Recurring Alarms view.
-  Acknowledge most recent alarm from selected source(s).
-  Go to alarm URL opens a hyperlink to the location that generated the alarm.
-  Notes opens the Alarm Notes window, which provides a text field for adding descriptive information to one or more alarms.
-  Remove alarm from console deletes all selected alarms from the table. This button is available to users who have invoke permission. Otherwise, this button does not appear.
-  Show Alarm Details opens the Alarm Details window, which provides additional information about the selected alarm.
-  Silence all alarm sounds turns off the audible alarm sounds.
-  Show Alarm Details opens the Alarm Details window, which provides additional information about the selected alarm.

-  Silence all alarm sounds turns off the audible alarm sounds.
-  The Filter alarms buttons open and close the **Filter Results** window from which you can limit the number of alarms based on alarm class, priority, etc.
-  The Toggle Sound buttons enable and disable the alarm sound.
-  Plays alarm sounds continuously until silenced. For systems with critical alarms, such as those related to building security, you may want to have a continuous alert sound to be sure that the alarm is noticed and acknowledged.
-  Set alarm console options opens the Multi Source View Options for the alarm console.
-  Selects all visible rows.
-  Show open alarms for the selected source opens a view that includes all alarms for the source of the alarm you selected in the Alarm Console.
-  Shows a video applies to video alarms. With a video alarm selected, clicking this button opens a video playback window that automatically plays the associated video.
-  Shows AX Alarm Console opens the alarm console provided by earlier versions of the system.

Alarm Console columns

An event related to a device or point occurs. If the event generates a value that is outside of normal, the event triggers an alarm. The table provides a set of basic columns of information about the event, which triggered the alarm.

Clicking the down arrow to the right under the control buttons provides a list of columns you can include in the alarm console. The ones with check marks next to them are the ones currently in view on Alarm Console. To include or exclude columns, click the column name in the list. This toggles column inclusion on and off.

To sort the information in any alarm console, click a column title.

The **bold** column entries in the table identify the default columns.

Column	Description
Source	Reports the component that transitioned from normal to offnormal, fault, or alert. If defining search criteria, you can use wild cards here.
Message Text	Describes the condition that generated the alarm.
Source State	Reports the component state transition:

Column	Description
	<ul style="list-style-type: none"> <li>• Offnormal (normal to offnormal)</li> <li>• Alert (normal to alert)</li> <li>• Fault (normal to fault)</li> <li>• Normal (offnormal, alert, or fault to normal)</li> </ul>
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to Offnormal, from normal to Fault, from offnormal, fault or alert to Normal, and from normal to Alert). The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1. The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Ack State	Reports the state of the alarm (unacknowledged, acknowledged).
Alarm Class	Reports the Display Name of the alarm class associated with the point, recipient or other component.
UUID	Universally Unique Identifier
Ack Required	Indicates if the alarm must be acknowledged (true) or not (false).
Normal Time	When displayed, shows a null value until the point returns to a normal state, then it displays the time that the point status returned to normal.
Ack Time	Displays the time that the alarm was acknowledged (if applicable).
User	If the alarm was triggered by an access control violation, identifies the person associated with the badge. If the alarm was generated by malfunctioning equipment, identifies the system user, if known.
Alarm Data	Refer to <a href="#">Alarm Data</a> .
Alarm Transition	Shows the initial source state that caused the alarm to be generated. The Alarm Transition may not be the current state of the alarm source. Once an Alarm Transition is created, it does not change for a single alarm record. For example, if the source state returned to "Normal" after an "Offnormal" status, this value remains at "Offnormal".
Last Update	Displays the time the system most recently updated the alarm.
Alarm Value	Reports the point value that triggered the alarm.
Notify Type	Indicates if the alarm is an alarm, alert, or an acknowledgement notification.
Add Alarm Data Column	Opens the Add Alarm Data Column window, which provides a drop-down list of additional data columns you can add to the console. These columns are not documented in this <i>Niagara Enterprise Security Reference</i> .
Remove Alarm Data Column	Opens the Remove Data Column window, which provides a drop-down list of the additional data columns you may have added to the alarm console. The purpose of this list is to delete any added columns from the console.
Reset Table Settings	Opens a confirmation window. Clicking Yes returns the console columns (multi-source view) to their defaults.


### Alarm Data

These data identify the source of the alarm and what caused the alarm (message text).









Name	Description
Message Text	Displays the customized message created for this alarm.
Source Name	Reports the component that transitioned from normal to offnormal, fault, or alert. If defining search criteria, you can use wild cards here.
Time Zone	Reports the time zone where the alarm occurred.

### Alarm Console Info icons

These icons appear under the Info column in the alarm console. Color coding and symbolic images represent the state of each alarm.

-  A red alarm icon in the table indicates that the current state of the alarm source is offnormal and not acknowledged.

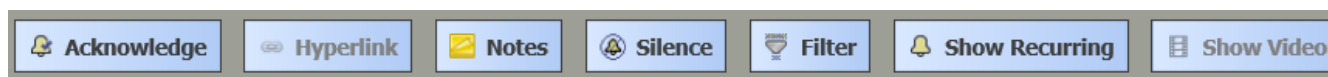


-  An orange alarm icon in the table indicates that the current state of the alarm source is alert and is not acknowledged.
-  A yellow alarm (gold) icon in the table indicates that the current state of the alarm source is offnormal but is acknowledged.
-  A green alarm icon in the table indicates that the current state of the alarm source is normal and not acknowledged.
-  A white alarm icon in the alarm history table indicates that the current state of the alarm source is normal and acknowledged.
-  A note alarm icon (it may be any color) in the table indicates that there is a note associated with the alarm.
-  A link icon in the table indicates that the alarm has a link associated with it. When an alarm displays this icon, the **Hyperlink** button is also active.
-  A video alarm icon may display if video is available with the associated alarm. If included, this graphic appears at the left end of the alarm record row.
-  An optional icon may display if it is setup in the alarm properties. If included, this graphic appears at the left end of the alarm record row.

## Alarm Console links

These links along the bottom of the window provide the essential alarm management functions.

**Figure 8.** Alarm Console links



- **Acknowledge** recognizes that the alarm state exists.
- **Hyperlink** opens the target link for the alarm, if one exists.
- **Notes** opens the **Notes** window, which is used to add a note to one or more selected alarms.
- **Silence** stops any audible notification associated with an alarm.
- **Filter** opens the **Filters** window used to define a query for the purpose of limiting system output to only selected criteria.
- **Show Recurring** opens the Recurring Alarms view for a single, selected point, and changes to the **Show All** returns to the Alarm Console view, which reports alarms on all points.
- **Show video** opens any video associated with the alarm for viewing.

## Show Alarm Details window

This summary window displays the details of a specific alarm record in the database.

Figure 9. Show Alarm Details window

Name	Value
Timestamp	29-May-18 5:13:28 PM EDT
UUID	3aa740d9-fea8-41f8-855c-8b3ae055805e
Source State	Offnormal
Ack State	Unacked
Ack Required	true
Source	NiagaraNetwork entSecurity802 local: station: slot:/Drivers/NiagaraNetwork/entSecurity802
Alarm Class	Medium
Priority	150
Normal Time	null
Ack Time	null
User	Unknown User
Alarm Transition	Offnormal
Last Update	04-Jun-18 12:02:57 PM EDT
▼Alarm Data	
Message Text	Ping Failed
Source Name	NiagaraNetwork entSecurity802
Time Zone	America/New_York (-5/-4)

Back


Forward

Acknowledge

Hyperlink

Notes

Close

This window opens from the Alarm Console view when you click the Show Alarm Details button (  ) or double-click an alarm row in the table.

Alarm information

These data describe when the point generated the alarm and the current state of the alarm.

Name	Description
Timestamp	Reports when the record was written to the database.
UUID	Unique Universal Identifier
Source State	Reports the component state transition:

Name	Description
	<ul style="list-style-type: none"> <li>Offnormal (normal to offnormal)</li> <li>Alert (normal to alert)</li> <li>Fault (normal to fault)</li> <li>Normal (offnormal, alert, or fault to normal)</li> </ul>
Ack State	Reports the state of the alarm (unacknowledged, acknowledged).
Ack Required	Indicates if the alarm must be acknowledged ( <code>true</code> ) or not ( <code>false</code> ).
Source	Reports the component that transitioned from normal to offnormal, fault, or alert. If defining search criteria, you can use wild cards here.
Alarm Class	Reports the <code>Display Name</code> of the alarm class associated with the point, recipient or other component.
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to Offnormal, from normal to Fault, from offnormal, fault or alert to Normal, and from normal to Alert). The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1. The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Normal Time	When displayed, shows a null value until the point returns to a normal state, then it displays the time that the point status returned to normal.
Ack Time	Displays the time that the alarm was acknowledged (if applicable).
User	If the alarm was triggered by an access control violation, identifies the person associated with the badge. If the alarm was generated by malfunctioning equipment, identifies the system user, if known.
Alarm Transition	Shows the initial source state that caused the alarm to be generated. The Alarm Transition may not be the current state of the alarm source. Once an Alarm Transition is created, it does not change for a single alarm record. For example, if the source state returned to "Normal" after an "Offnormal" status, this value remains at "Offnormal".
Last Update	Displays the time the system most recently updated the alarm.
Alarm Data	Refer to <a href="#">Alarm Data</a> .

### Alarm Data

These data identify the source of the alarm and what caused the alarm (message text).

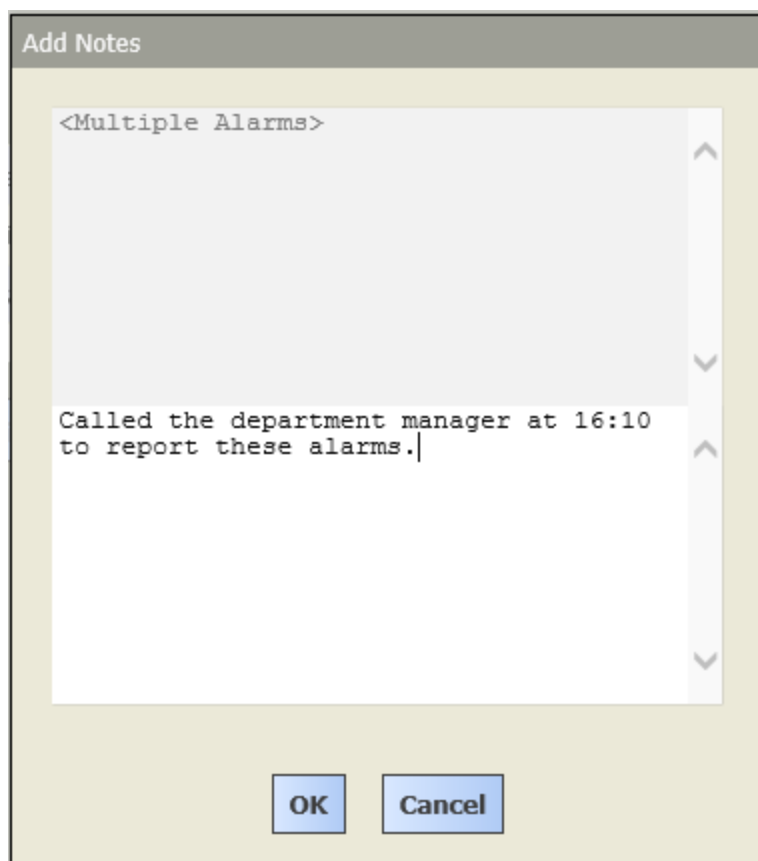
Name	Description
Message Text	Displays the customized message created for this alarm.
Source Name	Reports the component that transitioned from normal to offnormal, fault, or alert. If defining search criteria, you can use wild cards here.
Time Zone	Reports the time zone where the alarm occurred.


### Links

- Back** and **Forward** displays previous and next alarm data.
- Acknowledge** recognizes that the alarm state exists.
- Hyperlink** links to the edit view associated with the selected item. If no hyperlink exists, the button is grayed out.
- Notes** opens the **Notes** window, which is used to add a note to one or more selected alarms.
- Close** returns to the Alarm Console view.

### Notes window

This window provides a place to record comments about the alarm on a specific point.

**Figure 10.** Notes window

You open this window by selecting an alarm in the table and clicking the Notes button () on the Alarm Console view.

The upper pane reports the alarm. You use the lower pane to enter your note.

### Alarm Filter window


This window defines the criteria used to include or exclude alarms from the Alarm Console view.

Alarm Filter search criteria

Figure 11. Alarm Filter window

Filter

☐ Timestamp

Time Range  ? to ? >>

☐ Source Name

%

Must Include

☒ Case Sensitive

☐ Source State

☐ Ack State

☐ Priority

☐ min 0

☐ max 0

☐ Alarm Class

%

Must Include

☒ Case Sensitive

☐ Message

%

Must Include

☒ Case Sensitive

☐ Badge

%

Must Include

☒ Case Sensitive

☐ User


%

Must Include

☒ Case Sensitive

Ok

Cancel

You open this window by clicking the Filter button () on the Alarm Console view.

Criterion	Value	Description
Timestamp, Time Range	drop-down list and time chooser	Sets up start and end dates and times, days of the week or a schedule to use as filter criteria. The time in each alarm record identifies when the point's status changed from normal to offnormal.
Source Name	text	Reports the name of the alarm source. If you use the default script setting (%parent.displayName%), the source name property shows the display name of the alarm extension parent. You can edit this script, or type in a literal string.
Source State	read-only	Reports the component state transition:  Offnormal (normal to offnormal)

Criterion	Value	Description
		<p>Alert (normal to alert)</p> <p>Fault (normal to fault)</p> <p>Normal (offnormal, alert, or fault to normal)</p>
Ack State	text	Reports the state of the alarm (unacknowledged, acknowledged).
Priority	number for each of four component states	<p>Define the priority level to assign to the alarm class for each component state transition (from normal to offnormal, from normal to fault, from normal to alert, from offnormal to fault and from alert to normal.</p> <p>The lower the number, the more significant the alarm. The highest priority alarm is number 1.</p>
Alarm Class	text	Defines alarm routing options and priorities. Typical alarm classes include <i>High</i> , <i>Medium</i> and <i>Low</i> . An alarm class of <i>Low</i> might send an email message, while an alarm class of <i>High</i> might trigger a text message to the department manager.
Message	text	Limits the search based on the customized message created for this alarm. The result reports only alarms that contain this specific message text.
Badge	text	Limits the search to specific badge number(s).
User	text	Limits the search to specific user(s).

## Multi Source View Options window

This window configures the Alarm Console features.

Properties

**Figure 12.** Multi Source View Options window

Multi Source View Options

Notes Required On Ack

☐false

Sound Delay

0h

0m

10s

Sound File

module://alarm/com/tridium/alarm/ui/sound

Disable Row Highlight

☐false

OK

Cancel

Reset to Defaults

You open this window by clicking the Set alarm console options button () on the alarm console.

Property	Value	Description
Notes Required on Ack	defaults to true; option box for false	Opens the Notes window when a user acknowledges an alarm.
Sound Delay	hours, minutes, seconds	Configures an amount of time to wait between a transition to offnormal and the sounding of the audible alarm.
Sound File	filepath	Identifies the file that contains the alarm sound.
Disable Row Highlight	defaults to true; option box for false	Turns on and off the row highlight.

AX Alarm console

This view is an optional view you can configure or disable for each user. It provides a split-screen view with the Alarm Console on the top and two video camera panes below.

**Figure 13.** Alarm Popup window

The screenshot shows the 'Security Alarm Console' window. At the top right, there are configuration buttons: 'Auto Video Loading is ON', 'Auto Video Loading', 'Alarm Popup Setting', and 'Change Layout' (callout 1). The main area is a table of alarm sources. Below the table are buttons for 'Acknowledge', 'Show Recurring', 'Notes', 'Silence', 'Filter', and 'Review Video' (callout 3). The bottom section has two panes: 'Live Video' and 'Video Playback'. The 'Live Video' pane shows a camera feed with a timestamp '15-Sep-18 9:24:13.000 AM EDT'. The 'Video Playback' pane shows a message 'Video Playback not supported by camera' (callout 4). At the bottom of the video panes are buttons for 'Previous Video', 'Next Video', 'Most Recent Video', and 'Acknowledge' (callout 5).

Timestamp	Source State	Ack State	Source	Alarm Class	Priority	Normal Time	User	Message Text	Badge
15-Sep-18 6:57:15 AM EDT	Normal	0 Acked / 1438 Unacked	AXIS 210A - 00408C836221 MotionDetected1	Medium	150	15-Sep-18 6:57:15 AM EDT	Unknown User		
15-Sep-18 6:57:15 AM EDT	Normal	0 Acked / 1484 Unacked	AXIS 210A - 00408C836221 Motion Detected	Medium	150	15-Sep-18 6:57:15 AM EDT	Unknown User		
14-Sep-18 4:29:11 PM EDT	Alert	0 Acked / 1 Unacked	Remote Reader Module1.Reader 1	Medium	150	null		Badge Does Not Exist	000029954924 [0]
14-Sep-18 4:29:05 PM EDT	Alert	0 Acked / 1 Unacked	Remote Reader Module1.Reader 2	Medium	150	null	Sanders, Randy	No Access Right	00003744372 [0]
14-Sep-18 3:52:37 PM EDT	Alert	0 Acked / 1 Unacked	Remote Reader Module1.Reader 1	Medium	150	null	Sanders, Randy	No Access Right	00003744372 [0]
14-Sep-18 3:52:30 PM EDT	Alert	0 Acked / 1 Unacked	Remote Reader Module1.Reader 2	Medium	150	null		Badge Does Not Exist	000029954924 [0]
14-Sep-18 11:12:56 AM EDT	Offnormal	0 Acked / 1 Unacked	NiagaraNetwork EnterpriseSecurity2_4	Medium	150	null	Unknown User	Ping Failed	
12-Sep-18 4:24:59 PM EDT	Normal	0 Acked / 2 Unacked	Axis Video Network AXIS 210A - 00408C836221	Medium	150	12-Sep-18 4:30:00 PM EDT	Unknown User	Ping Success	
12-Sep-18 3:06:52 PM EDT	Normal	0 Acked / 1 Unacked	Axis Video Network	Medium	150	12-Sep-18 3:08:04 PM EDT	Unknown User	Ping Success	
14-Sep-18 4:29:20 PM EDT	Normal	0 Acked / 3 Unacked	Access Network Remote Reader Module1	High	250	14-Sep-18 4:32:21 PM EDT	Unknown User	Ping Success	

1. Window configuration controls
2. Alarm console
3. Alarm controls
4. Video panes
5. Video alarm controls

Before you can access this view you must enable it for a user. Click **Controller (System) Setup > User Management > Users**, add a new user or edit an existing user, and set the **Alarm Console Popup** property to **All Alarms** or **Video Alarms Only**.

Then, open this view from the Alarm Console view by clicking the Show AX Alarm Console button ( ). This button is the furthest to the right in the row of buttons at the top, right side of the view. The console pane displays open alarm sources. The video panes display real-time and recorded video.

#### Window configuration controls

These control buttons are in the top right corner of the view configure view options.

- **Auto Video Loading** is a play and pause button for the video panes.
- **Alarm Popup Setting**



- **Change Layout** opens the Select Layout window, which configures the alarm console.

#### Alarm controls

- **Acknowledge** recognizes that an alarm state exists at the point represented by the selected row in the table. This button displays on the alarm console views and on the Recurring Alarms view.
- **Show Recurring** opens the Recurring Alarms view for a single, selected point, and changes to the **Show All** button. Clicking this button returns to the Alarm Console view, which reports alarms on all points.
- **Notes** opens the **Notes** window, which is used to add a note to one or more selected alarms.
- **Silence** stops any audible notification associated with an alarm.
- **Filter** opens the **Filters** window used to define a query for the purpose of limiting system output to only selected criteria.
- **Review Video** opens the Alarm Video viewer for reviewing video that is recorded as a result of an alarm. This link is only available when an alarm video is available.

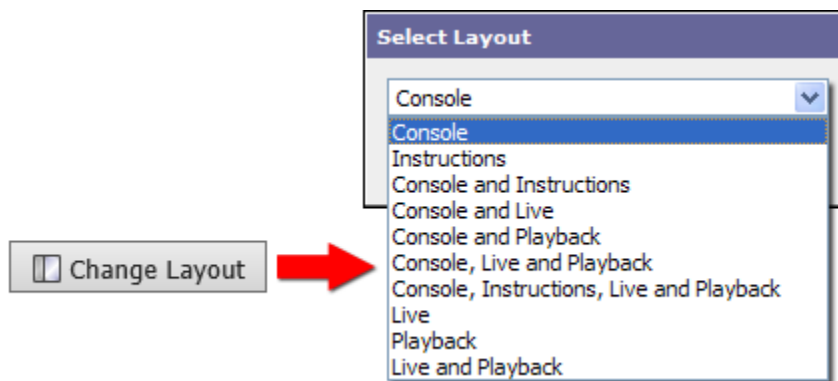
#### Video alarm controls

- **Previous** loads and plays back the previously-recorded video.
- **Next** loads and plays back the next recorded video (if one exists).
- **Most Recent Video** loads and plays back the video captured most recently.
- **Acknowledge** recognizes that an alarm state exists at the point represented by the selected row in the table. This button displays on the alarm console views and on the Recurring Alarms view.

### Console Layout window

When you use the Alarm Console view, or when you use the Alarm Popup window, you have several layout options available.

**Figure 14.** Console Layout window



This window opens when you click the Console Layout link at the top of the AX Alarm Console view.

Each option provides a unique display with pane combinations that include up to four of the following panes:

- Alarm Console pane
- Instructions pane
- Live Video pane
- Video Playback pane

Each pane displays information pertaining to an alarm. When a video alarm is selected in the console, the video panes display Live Video or Video Playback. When no video is associated with an alarm, "No Video Available"

displays in the Live Video and Video Playback panes. You can configure settings for each individual user so that video alarms are selected (and displayed) automatically or so that they require manual selection.

Activity Monitor view

This view, under the **Monitoring** main menu, lists all system activity (history records and alarms) that occurred during the last seven days. Activities include events, such as badge access traffic, system user audits, and so on.

The Activity Monitor view can show all the types of system activity recorded at the designated controller or you can customize it to show only specific activities.


Figure 15. Activity Monitor view

Home Monitoring Personnel Reports System Setup Threat Levels						
Alarm Console Activity Monitor Video Monitoring						
Page 1 of 3 Page Size 20						
Timestamp	Record Type	Activity	Station	Authority	Object	Description
11-May-18 10:21 AM EDT	Log	box.serverSession	MyEntsecSupervisor	1000	Exception processing unsolicited BOX message	java.lang.NullPoint
11-May-18 10:14 AM EDT	Log	sys	MyEntsecSupervisor	800	Saved C:\ProgramData\Niagara4.6\ridiumstations\MyEntsecSupervisorconfig.bog (422ms)	
11-May-18 10:14 AM EDT	Log	orion	MyEntsecSupervisor	800	end checkpoint on MySQLDatabase (rdBMySQL:MySQLDatabase)	
11-May-18 10:14 AM EDT	Log	orion	MyEntsecSupervisor	800	begin checkpoint on MySQLDatabase (rdBMySQL:MySQLDatabase)	
11-May-18 10:14 AM EDT	Log	sys	MyEntsecSupervisor	800	Saving station...	
11-May-18 10:06 AM EDT	Audit	Login	MyEntsecSupervisor	admin	/Services/WebService	Slot Name: 0:0:0:0
11-May-18 9:14 AM EDT	Log	sys	MyEntsecSupervisor	800	Saved C:\ProgramData\Niagara4.6\ridiumstations\MyEntsecSupervisorconfig.bog (328ms)	
11-May-18 9:14 AM EDT	Log	orion	MyEntsecSupervisor	800	end checkpoint on MySQLDatabase (rdBMySQL:MySQLDatabase)	
11-May-18 9:14 AM EDT	Log	orion	MyEntsecSupervisor	800	begin checkpoint on MySQLDatabase (rdBMySQL:MySQLDatabase)	
11-May-18 9:14 AM EDT	Log	sys	MyEntsecSupervisor	800	Saving station...	
11-May-18 8:14 AM EDT	Log	sys	MyEntsecSupervisor	800	Saved C:\ProgramData\Niagara4.6\ridiumstations\MyEntsecSupervisorconfig.bog (266ms)	
11-May-18 8:14 AM EDT	Log	orion	MyEntsecSupervisor	800	end checkpoint on MySQLDatabase (rdBMySQL:MySQLDatabase)	
11-May-18 8:14 AM EDT	Log	orion	MyEntsecSupervisor	800	begin checkpoint on MySQLDatabase (rdBMySQL:MySQLDatabase)	

You access this view from the main menu by clicking **Monitoring > Activity Monitor**.

Buttons

In addition to the standard control buttons (Summary, Auto Refresh, Column Chooser, Filter, Refresh, Manage

Reports, and Export), the Configure button () opens a view for configuring the information to include in the Activity Monitor view.

Columns

Table 1. Activity Monitor columns

Column	Description
Timestamp	Reports when the record was written to the database.
Record Type	Reports the type of information the record represents: Access, Audit, Log, Alarm, Alert, Unacked, Intrusion. Refer to <a href="#">About record types</a> .
Activity	Identifies the event (for example, Login, Exit Request) that prompted the system to generate the record. Refer to <a href="#">About activities</a> .
Station	Reports the station in which the event occurred.
Authority	Identifies the person responsible for the event.

Column	Description
Object	Reports the door at which the event occurred.
Description	Provides additional information.

## About record types

The type of activity record in the database provides additional information about the event.

**Table 2.** Record types

Record type	Description
Access	Indicates a record created when a person accessed the building.
Audit	Indicates a record that provides an audit trail.
Log	Indicates a record created in a system log.
Alarm	Indicates an alarm record.
Alert	Indicates a record created by an alert.
Unacked	Indicates a record that reports an alarm, which has not been acknowledged.
Intrusion	Indicates a record created when an intrusion event occurred.

## About activities

An activity explains an event. For example, the system may grant access while an additional condition is required. Or the system may deny access for a reason. The activity value identifies the reason.

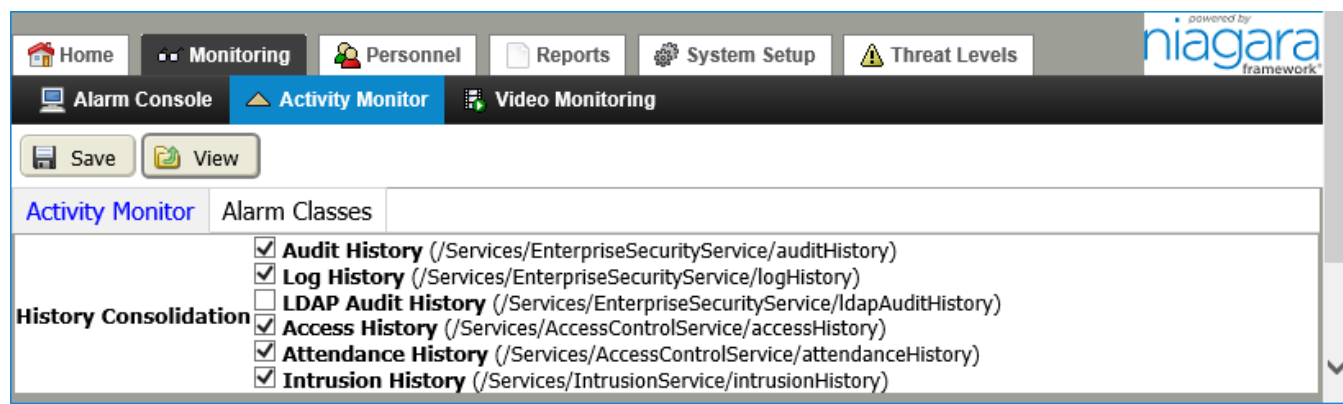
Activity value	Description
Granted	Normal access event.
Badge Does Not Exist	Access denied because the system cannot find the badge in the database.
Badge is Lost	Access denied because the badge has been disabled.
Badge is Disabled	Access denied because the badge is not active. Badges can be disabled usually by a manager using the Supervisor station.
Badge Not Assigned	Access denied because the badge exists, but has not yet been assigned to a person.
No Active Schedule	Access denied for lack of a schedule.
No Access Right	Access denied because the person lacks the right to access the location.
Unknown Wiegand Format	Access denied because the format of the badge does not conform to a known Wiegand format.
Invalid PIN	Access denied because the person entered a Personal ID Number that does not match the badge.
No PIN Number Entered	Access denied because the person did not submit a PIN.
Access Zone Disabled	Access denied because the access zone is not active.
Occupancy Violation	Access denied because more or fewer people are in the zone than required.
Supervisor Required	Access denied because supervisor is required and none is currently in the access zone.
Anti Passback Violation	Access denied because the person entered, exited, and is attempting to enter again (pass back) immediately. Access configuration ( <b>Controller (System) Setup &gt; Access Setup &gt; Access Zones</b> ) defines the <b>Passback Timeout</b> value (the amount of time required before the person can pass back).
Granted But Not Used	Access granted, but the person did not enter.
Granted But PIN Duress	Access granted, but there is a problem with either the badge or the PIN.  If PIN duress is set up in the controller, then, when a person uses a PIN with the offset specified in the controller, the system grants access but issues a duress alert. This allows a person to enter a space under duress, but causes an alert.
Granted But Anti	Access permitted, but the person is attempting to enter again (pass back) before the <b>Passback Timeout</b> expired.

Activity value	Description
Passback Violation	
Granted But Occupancy Violation	Access permitted even though too many or too few people are in the zone or a supervisor is not present.
Granted But Waiting On More Occupancy	Access permitted pending the arrival of more people.
Granted But Waiting On PhotoID	Access permitted, but the person must present their photo ID.
Granted But Access Zone Disabled	Access permitted even though the access zone is not active.
Granted But Supervisor Required	Access permitted even though a supervisor is not present.
Granted If Occupancy Corrected	Access permitted pending changes to overall occupancy.
Granted But Trace	Access permitted with trace provided.  If trace has been set up for a person, then, every time the person uses an assigned badge, the system issues an alert in the alarm console.
Exit Request	Normal exit from an access zone.
Manual Override	Access permitted by manually overriding the door.
Canceled	The person started to access the zone, but did not complete the action.
Connection Problem	Access may or may not be permitted due to a networking issue.
Granted But Connection Problem	Access permitted, but the system is experiencing network problems.
Validation Timeout Expired	Access denied because the maximum time allowed to receive a badge validation has expired.
Inactive Threat Level Group	The threat level group exists, but has not been activated.
Unlock Input	The controller received an input to unlock the door.
Unknown	Something happened that is not covered here.

## Edit (configure) Activity Monitor view, Activity Monitor tab

This view configures the Activity Monitor view.

Figure 16. Edit Activity Monitor view, Activity Monitor tab



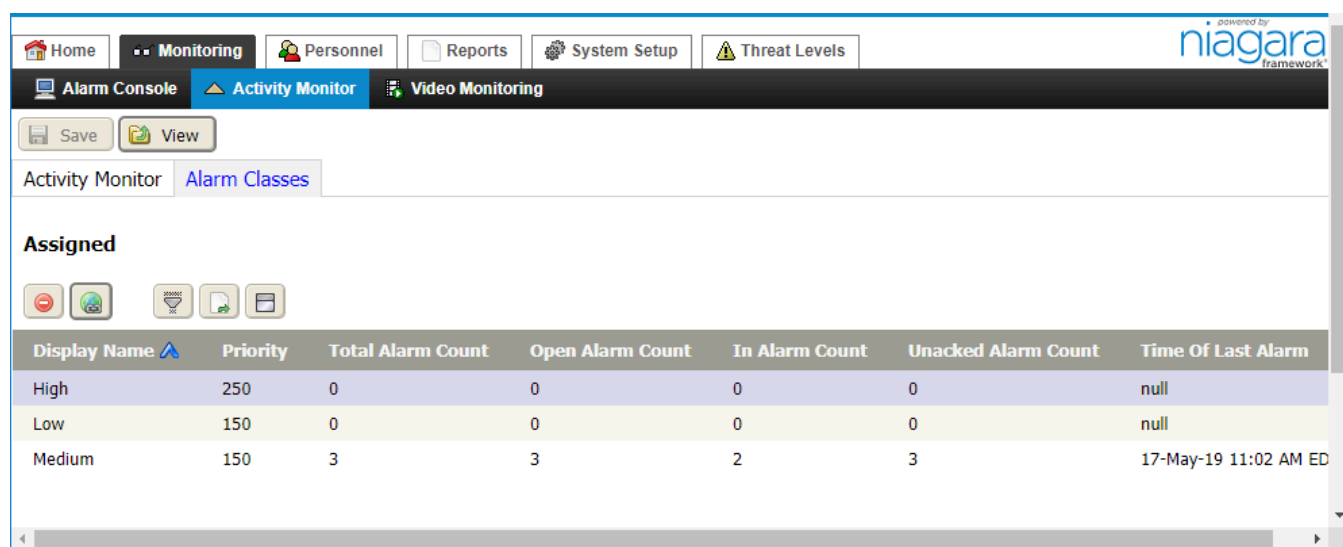
This view displays when you click the **Configure** button  in the Activity Monitor view.

The **History Consolidation** property boxes on the view configure the activity monitor table so that it includes the type of records you want to monitor. Click the **Save** button to keep any changes before navigating away from the view.

### Activity Monitor Alarm Classes tab

In addition to the seven days of history records selected on the Activity Monitor tab, the Activity Monitor view displays alarm records for all assigned alarm classes. This tab provides a way to assign or unassign alarm classes for monitoring.

Figure 17. Edit Activity Monitor view, Alarm Classes tab






You access this view by clicking **Monitoring > Activity Monitor**, clicking the **Configure** button () , and

clicking the Alarm Classes tab.

Alarm classes categorize, group, and route alarms. The alarm class settings can provide alarm priorities and designate which alarms require acknowledgment. They are also the basis for visual grouping in the alarm console view.

Control buttons

In addition to the standard Filter and Export buttons, these buttons serve this view:

-  Unassign removes the assignment.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  Assign Mode buttons open and close the Unassigned pane.

Activity Monitor columns

Column/data item	Description
Display Name	Indicates the name associated with the activity.
Priority	Indicates the significance of the alarm. The lower this number the more significant the alarm.
Total Alarm Count	Indicates the total number of alarms.
Open Alarm Count	Indicates the total number of alarms that are currently open and unacknowledged.
In Alarm Count	Indicates the total number of alarms that are currently active.
Unacked Alarm Count	Indicates the total number of alarms that have not been acknowledged.
Time of Last Alarm	Reports when the most recent alarm was saved to the database.

Activity Monitor Filter window

This window provides a series of wild cards to display only activity records of interest.

Figure 18. Activity Monitor Filter window

Filter

☒ **Timestamp**

Last 12 Hours ▾ >>

☐ **Record Type**

☐ **Activity**

%

Must Include ▾

☒ Case Sensitive

☐ **Station**

%

Must Include ▾

☒ Case Sensitive

☐ **Authority**

%

Must Include ▾

☒ Case Sensitive

☐ **Object**

%

Must Include ▾

☒ Case Sensitive

☐ **Description**


%

Must Include ▾

☒ Case Sensitive

Ok

Cancel

You open this window by clicking the Filter button () on the Activity Monitor view.

Activity monitor search criteria

Criterion	Value	Description
Timestamp	drop-down list	Limits summary data to a specific time period.
Activity	wildcard (%)	Limits summary data based on activity name.
Station	wildcard (%)	Limits summary data based on station name.
Authority	wildcard (%)	Limits summary data based on severity.
Object	wildcard (%)	Limits summary based on action: Station Stopped, Service Stopped
Description	wildcard (%)	Displays the exception stack trace if the trace exists, otherwise this value is empty.

Video monitoring views

Video monitoring is available for cameras that are licensed and added under the appropriate video networks. Use the Remote Drivers view to add video drivers to the video networks that are licensed and available to your system.

Home

Monitoring

Personnel

Reports

System Setup

Threat Levels

Alarm Console

Activity Monitor

Video Monitoring

Surveillance Viewer

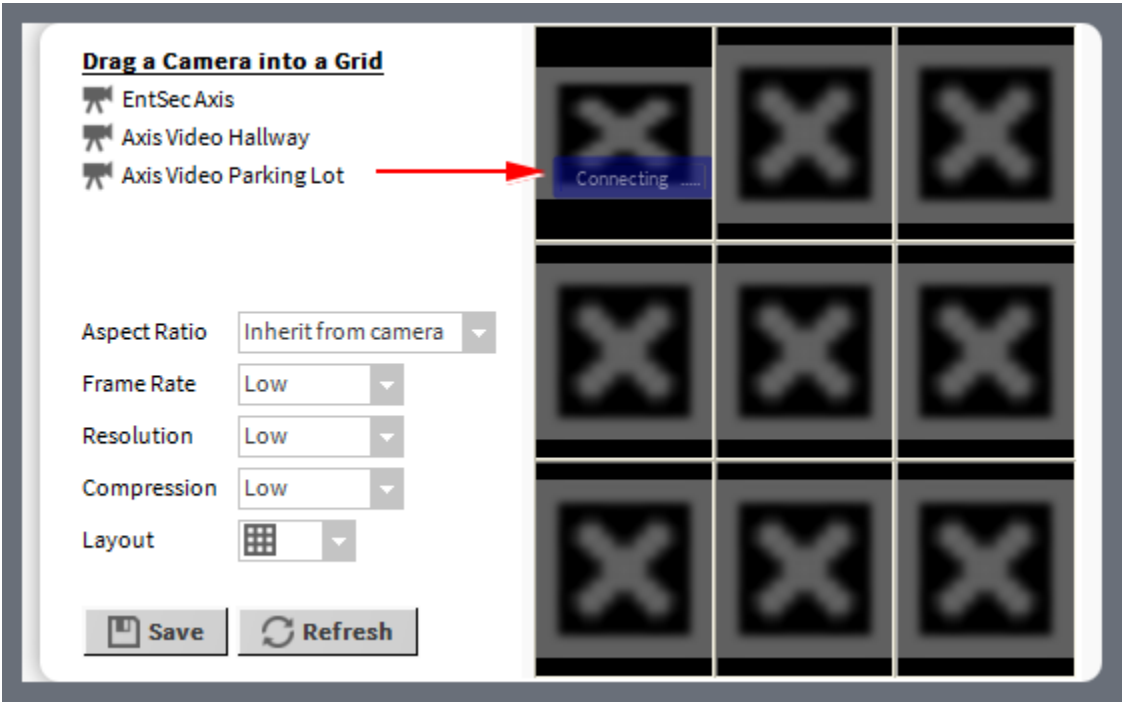
Playback Viewer

The *Video Framework Guide* contains additional information about configuring video cameras for supported camera models.

Surveillance viewer

This view supports video from up to nine video cameras. You may configure video quality and layout options from the viewer. This viewer requires the Web Launcher. Browsers do not support this viewer.

Figure 19. Video Surveillance view with 9-camera layout



You access this view from the main menu by clicking **Monitoring > Video Monitoring**.

The view consists of a four-pane grid. Each pane links to an active surveillance camera.

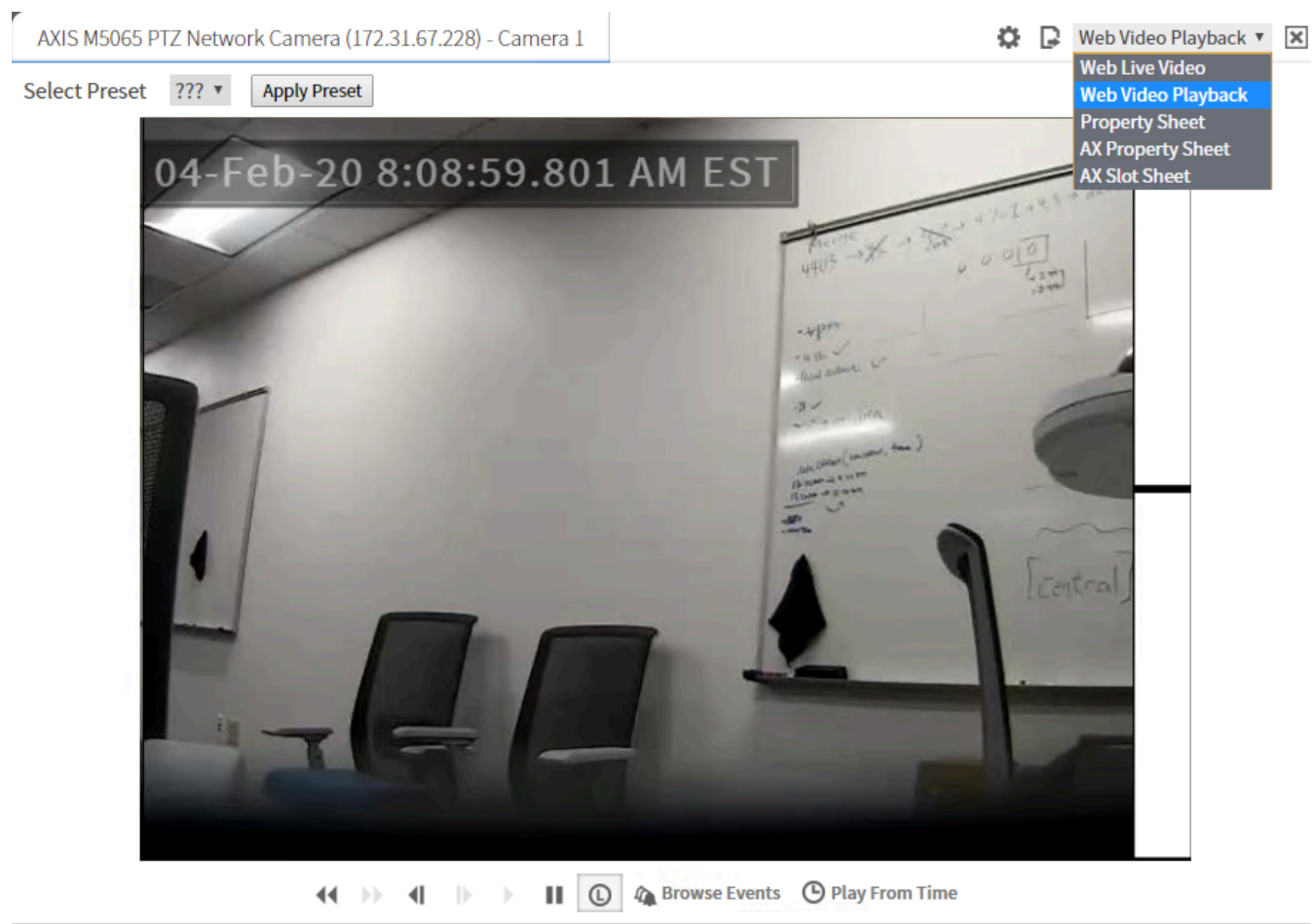
Property	Value	Description
Frame Rate	drop-down list	Defines the frequency (rate) at which an imaging device displays consecutive images called frames.
Resolution	drop-down list	Defines number of distinct pixels in each dimension that the view can display.
Compression	drop-down list	Defines the quality of the image. The more an image is compressed to reduce its file size the lower the quality of the image.
Layout	drop-down	Selects the nature of the grid.

Playback viewer

This view plays back live or recorded video from a single, selected camera.





Figure 20. Video Playback viewer



Any camera under a video network is available for selection from an option list in the top left corner of the view. Depending on the camera type, controls are available for configuring or adjusting the camera.

Table 3. Video playback controls

Control	Description
<div> Fast Play Reverse</div>	<p>Incrementally speeds up the reverse play speed with each click. The on-screen play indicator shows the current play speed while this function is being used.</p> <p>The rewind speed defaults to 4x. Use the camera's Property Sheet view to change this speed. Clicking this button once rewinds at 4x. Clicking it again increases the rewind speed to 8x. The maximum rewind speed is 16x.</p>
<div> Fast Play Forward</div>	<p>Incrementally speeds up the forward play speed with each click. The on-screen play indicator shows the current play speed while this function is being used.</p> <p>Fast forward speed defaults to 4x. Use the camera's Property Sheet view to change this speed. Clicking this button once advances at 4x. Clicking it again increases the fast forward speed to 8x. The maximum forward speed is 16x.</p>









Control	Description
 Skip Reverse/ Skip to the start or previous clip	While playing video, this function skips backward to the beginning of the current track and starts playing automatically.  The rewind speed defaults to 1x. Use the camera's Property Sheet view to change this speed. Clicking this button once rewinds at 1x. Clicking it again increases the rewind speed to 2x, 4x, etc. The maximum rewind speed is 16x.
 Skip Forward/Skip to the end or next clip	While playing back video, this function skips forward to the next recorded track and starts playing automatically.  Slow forward play back defaults to 1x. Clicking it again increases the slow forward speed to ex, then 4x, etc. The maximum forward speed is 16x.
 Play	Initiates playback and resumes playback following a pause.
 Pause	Discontinues playback at the current location.
 Live	Switches from a playback video display to a live video display (still in the <b>Video Playback</b> view).

Table 4. Event Controls

Control	Description
 Browse events	Opens the <b>Browser Events</b> window.
 Play From Time	Initiates playback from a specific time.

Video indicators

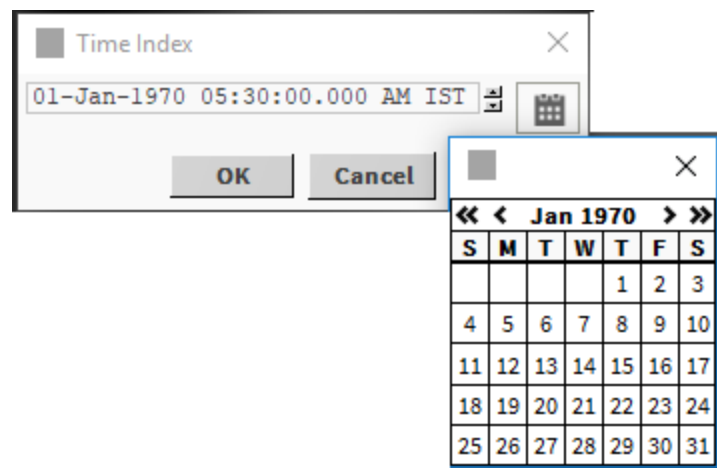
The driver displays these indicators in the video playback window:

-  (L) indicates Live Video.
- X1,X2..... indicate the play back speed.
- Fast-Forward, Skip, Play and Pause indicate the video playback mode.
- Slow- Light blue, Medium- Medium blue and Fast- Dark blue indicate the pan, tilt and zoom degrees.
- A text message displays on the screen at times to indicate the connection status.

Find Event

This function opens the **Time Index** window, which allows you to select an event according to a specific date and time in terms of day, month, year, and time. A calendar icon in the window presents an interactive calendar for browsing to and selecting the desired date.

**Figure 21.** Time Index window

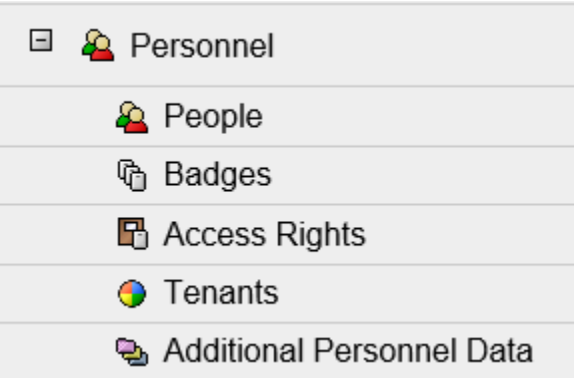




# Chapter 3. Personnel views

The **Personnel** menu item opens to the **People** view. Other views open when you add, edit, access history and show readers. The personnel views set up and manage people.

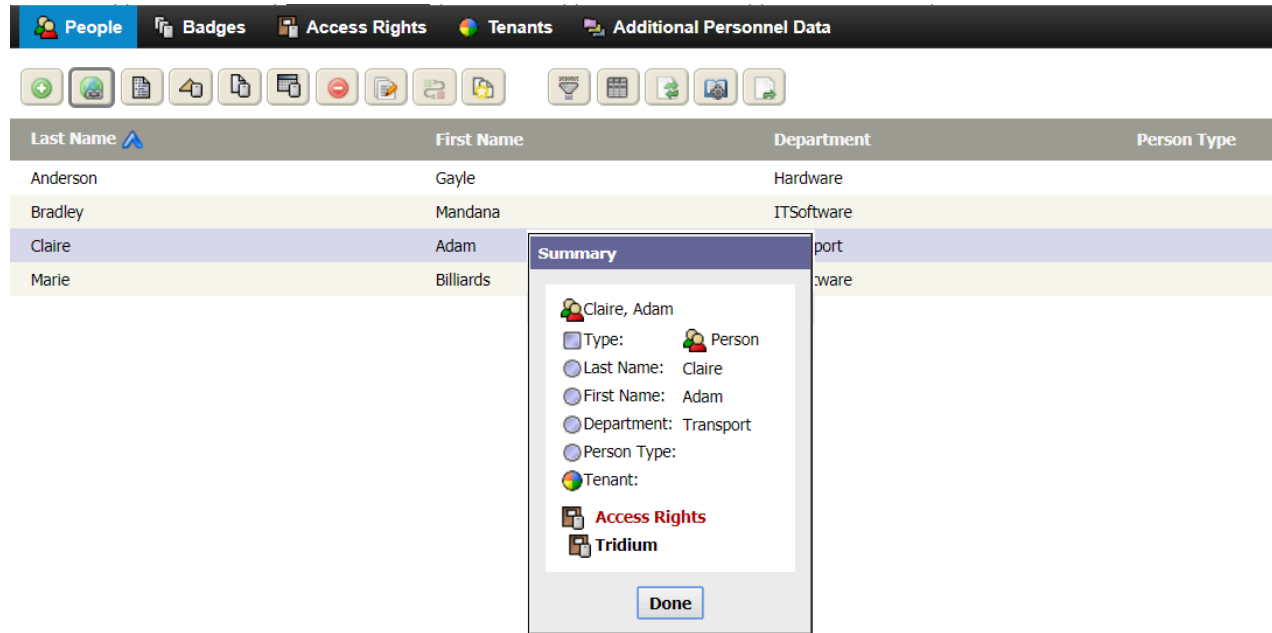
**Figure 22.** Personnel menu



## People view

This view lists all personnel in the system. The Summary view reports the same information for a specific person.

**Figure 23.** People view












To open the People view, expand **Personnel** and click **People**. To open the Summary window, select a person in

the People view.

The columns in the People view table provide key information for each employee.

### Control buttons

In addition to the standard control buttons (Delete, Column Chooser, Refresh, Reports and Export), these buttons provide personnel management functions:

-  Add opens a view or window for creating a new record in the database.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  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.
-  Show Access History opens the Access History view for the selected record.
-  Show Readers opens the Person Reader Report. The [Reports](#) chapter documents this report.
-  Show Expirations opens the Person Access Right Report view.
-  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.
-  Match with synchronize combines the properties of similar schedules (subordinate to the Supervisor) and similar personnel records under a single name.
-  Duplicate opens a New window and populates each property with properties from the selected item. Using this button speeds the item creation.

### Default People view columns

Column and summary property	Description
Last Name	Reports the family name of the person.
First Name	Reports the given name of the person.
Department	Reports where within the organization's flow chart the person works.
Person Type	Reports additional information about the person.
Tenant Name	Reports the name of the associated tenant.
Access Rights	The Summary window lists the access rights assigned to the person.

Quick Edit window

This window provides controls to batch edit one or more table records simultaneously.

Figure 24. Quick Edit window

Quick Edit

Apply to selected items: 1

Apply to all records with the current filter

Department

Human Resources

>>

Person Type

>>

Tenant

None

>>

Supervisor

true

>

Trace Card

Trace Off

>

Add Access Rights

None

>>


Remove Access Rights

None

>>

Ok

Cancel

The Quick Edit window opens when you select one or more table records and click the quick edit button (  ) at the top of a view or select the Quick Edit menu item from the right-click menu.

Property	Value	Description
Apply to selected items	radio button	Selects for update only the currently selected rows (records). The number of currently selected records displays to the right of the option.
Apply to all records with the current filter	radio button	Selects for update any displayed records that match any filters assigned to this table.
To These Properties	multiple properties	The available properties change depending on the specific table.
Apply these values	text, etc.	Presents the value to modify for each property.

People View Filter window

This window sets up the search criteria used to find people records.

March 25, 2025

51

People view filter criteria

Figure 25. People View filter

Filter

☐ Last Name

%

Must Include

▼

☒ Case Sensitive

☐ First Name

%

Must Include

▼

☒ Case Sensitive

☐ Department

%

Must Include

▼

☒ Case Sensitive

☐ Person Type

%

Must Include

▼

☒ Case Sensitive

☐ Tenant Name

%

Must Include

▼

☒ Case Sensitive

☐ Employee Id

%

Must Include

▼

☒ Case Sensitive

Ok

Cancel

You access the filter by clicking the Filter button (  ) on the People view.

Criterion	Value	Description
Last Name	wildcard	Sets up a search by last name.
First Name	wildcard	Sets up a search by first name.
Department	wildcard	Sets up a search by department.
Person Type	wildcard	Sets up a search by person type.
Tenant Name	wildcard	Sets up a search by tenant name.
Employee ID	wildcard	Sets up a search by employee ID.

Add New (or edit) Person view

This view provides properties for manually creating and configuring new personnel records, one person at a time.



Figure 26. Add Person view

HomeMonitoringPersonnelReportsSystem SetupPhoto

PeopleBadgesAccess RightsTenantsAdditional Personnel Data

SavePeople

SummaryPersonAccess RightsBadges

Last NameManners

First NameMelody

Middle Initial

Employee Id654

DepartmentCustomer Service

Person TypeManager

TenantNone

Supervisortrue


Trace CardTrace Off


PIN

PIN (number only):

Confirm PIN:

Portrait

You access this view by clicking **Personnel > People**, followed by clicking the Add people button (  ). You access the edit version of this view by double-clicking a row in the People view table. You access an existing personnel record for the purpose of editing it by clicking **Personnel > People**, followed by clicking the

Hyperlink button (  ).



The screen capture shows an existing view and a new person view.






Links

Links appear as large buttons just below the name of the view.

- **Save** updates the station database with the current information.
- **People** returns to the People view.

Buttons

-  Save updates the database with the current information.
-  Return to parent People view.

-  Add New Person opens the Add New Person view.
-  Duplicate opens a New window and populates each property with properties from the selected item. Using this button speeds the item creation.
-  Assign New Badge opens a view for assigning a badge to the person.
-  Enroll or Enroll New Badge opens the Enroll New Badge view.
-  Print Badge sends the badge data to the printer.

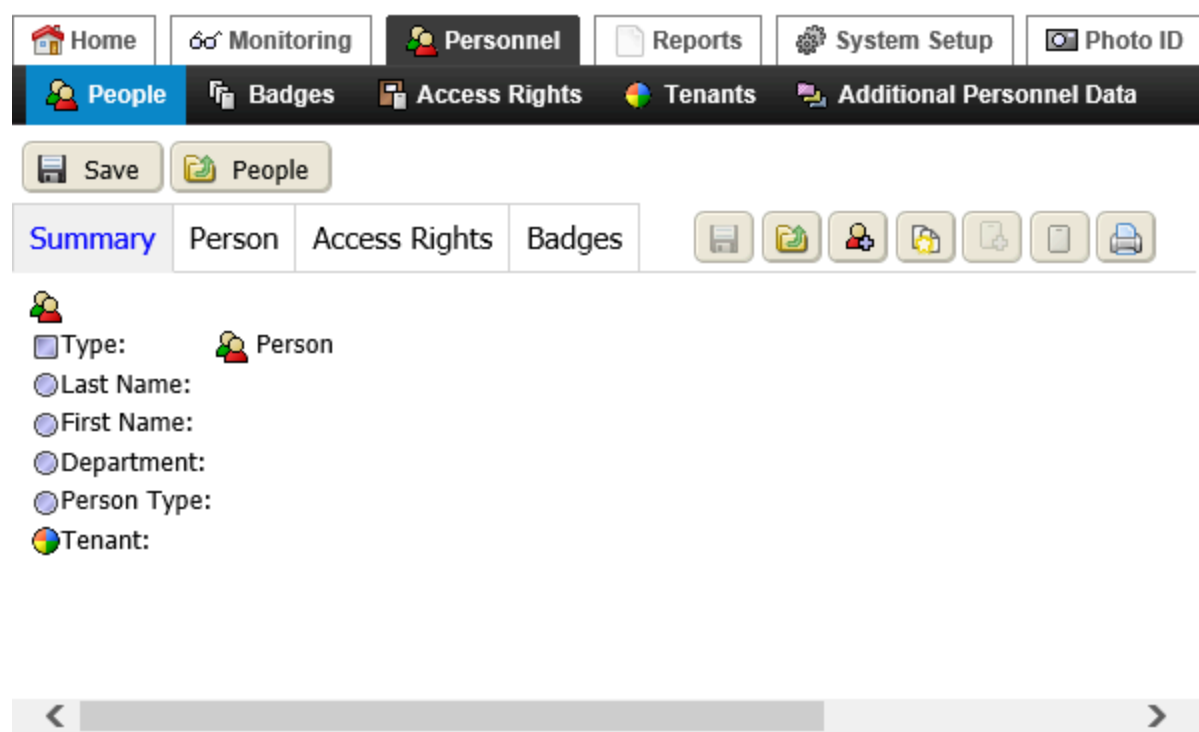
Property	Value	Description
Last Name	text	Defines the person's family name.
First Name	text	Defines the person's given name.
Middle Initial	text	Defines the person's middle initial.
Employee Id	text	Assigns an ID to the person.
Department	text	Defines the department name.
Person Type	Ref Chooser	Defines an attribute that describes the person. Possibilities include: Supervisor, Manager, Operator, Local, Remote, Home Office, Satellite Office, Exempt, Hourly. If this property is empty, the system uses the default Person Type. If the property does not match an existing Person Type, the system creates a new type.
Tenant	Ref chooser	Defines the company name of the associated tenant.
Supervisor	true or false (default)	Indicates if the person is in a managerial role within the organization.
Trace Card	Trace On or Trace Off (default)	Controls an alarm when the system grants access at a specified door to the associated person. This property works together with the Trace Card Alert property associated with the reader that is assigned to the person's access right.
PIN (Personal Information Number)		This personnel code is used for keypad entry.

Property	Value	Description
Portrait	camera hyperlink	Opens a link to Asure ID for capturing a photo.
Additional properties	various	If your company collects more personnel information, additional properties appear at the end of the Person property sheet. The Additional Personnel Data view creates these properties.

New person Summary tab

This tab displays a read-only list of information about a single personnel record. It displays any time you save changes made in another tab. Located at the bottom of the listing are all the badges and access right assignments associated with the record. Each listed badge or access right is a hyperlink to the Edit Existing Badge or Edit Existing Access Right view.

Figure 27. Summary tab



You access this view by clicking **Personnel > People**, followed by double-clicking a person row in the table.

If access rights and a badge are assigned to the person, hyperlinks at the bottom of the Summary tab link to the relative records.

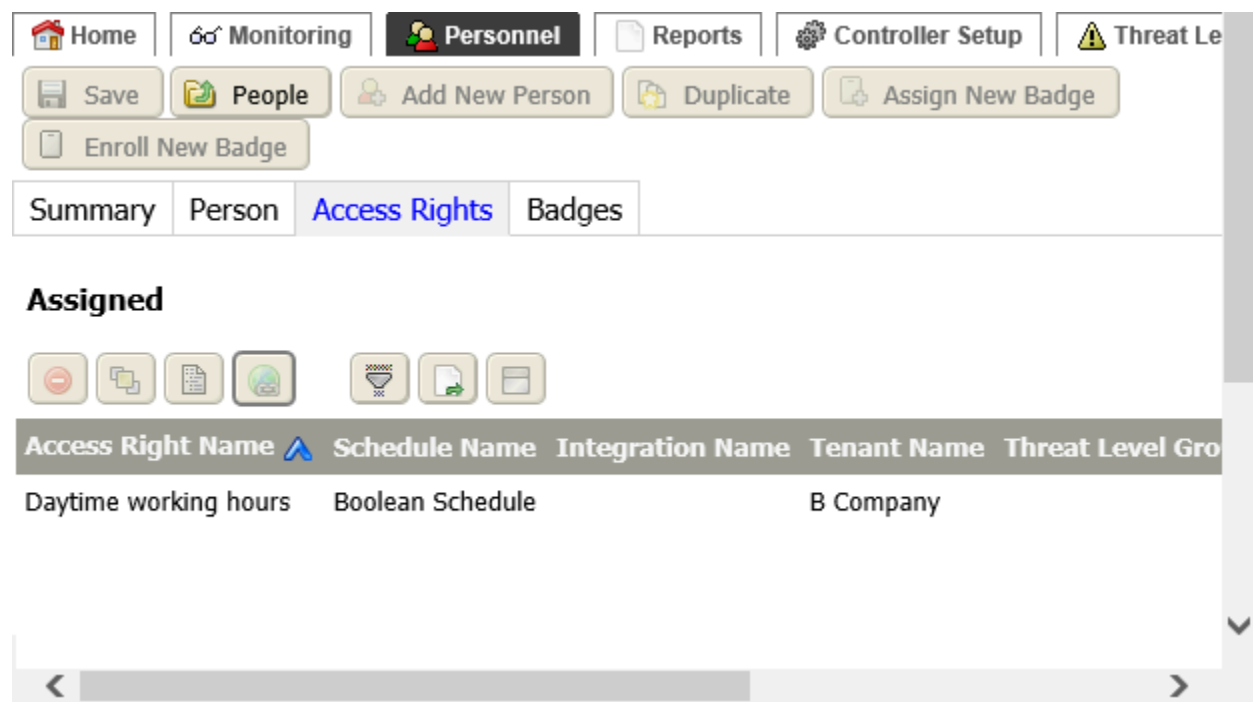
Property	Description
Type	Identifies the summary window as one that provides person details.
Last Name	Reports the family name of the person.
First Name	Reports the given name of the person.

Property	Description
Department	Reports where within the organization’s flow chart the person works.
Person Type	Reports additional information about the person.
Tenant	Reports the name of the associated tenant.
Access Rights	Lists the person’s access rights.

New Person Access Rights tab

This tab consists of two panes with tabular information: The Newly Assigned pane shows the access rights assigned to the individual whose name appears at the top of the view. The Unassigned pane lists available access rights.



Figure 28. Access Rights tab



To open this tab using the main menu, click **Personnel > People**. To add a person, click the **Add** button or to edit an existing person’s record double-click a person row in the table. Finally, click the Access Rights tab.

Control buttons

In addition to the standard control buttons (Summary, Hyperlink, Filter, and Export), the following are the buttons specifically related to the Newly Assigned pane:

-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  Change Assignment Properties opens the Change Assignment Properties window.



- Assign Mode buttons open and close the Unassigned pane.

In addition to the standard control buttons (Summary, Hyperlink, Filter, and Export), the Assign button is specifically related to the Unassigned pane. You use this button to assign a selected access right to the person’s record, which you are adding or editing.

Columns

You can change these properties before or after the assignment right has expired.

Table 5. Access rights columns

Column	Description
Access Right Name	Identifies the title of the access right associated with the entity.
Schedule Name	Reports the name of the associated schedule (if any).
Integration Name	Reports the name of the associated integration ID. The system performs building automation actions, such as turning the lights on, associated with this type of ID.
Tenant Name	Reports the name of the associated tenant.
Threat Level Group Name	Reports the name of the associated threat level group.
Start Date	Reports the beginning date from the schedule.
End Date	Reports the final date from the schedule.
Assigned Threat Level	Reports the threat level assignment.

Change Assignment Properties window

This window updates the access rights assignment for a person. Changing this assignment overrides the link between an access right’s **Default Assigned Threat Level** and the **Default Access Right Threat Level** defined on the threat level group.

Figure 29. Change Assignment Properties window

Change Assignment Properties

Start Date

☒

Always Effective

☐

06

Oct

2011

04

:

12

PM

EDT

End Date

☒

Always Effective

☐

06

Oct

2011

04

:

12

PM

EDT


Assigned Threat Level

--Default--

Ok

Cancel

Access right assignment properties are available in the **Change Assignment Properties** window.

This window opens in the edit user view when you select an access right from a person’s Access Right tab and click the Change Assignment Properties button .

Property	Value	Description
Start Date	date	Determines when an access right

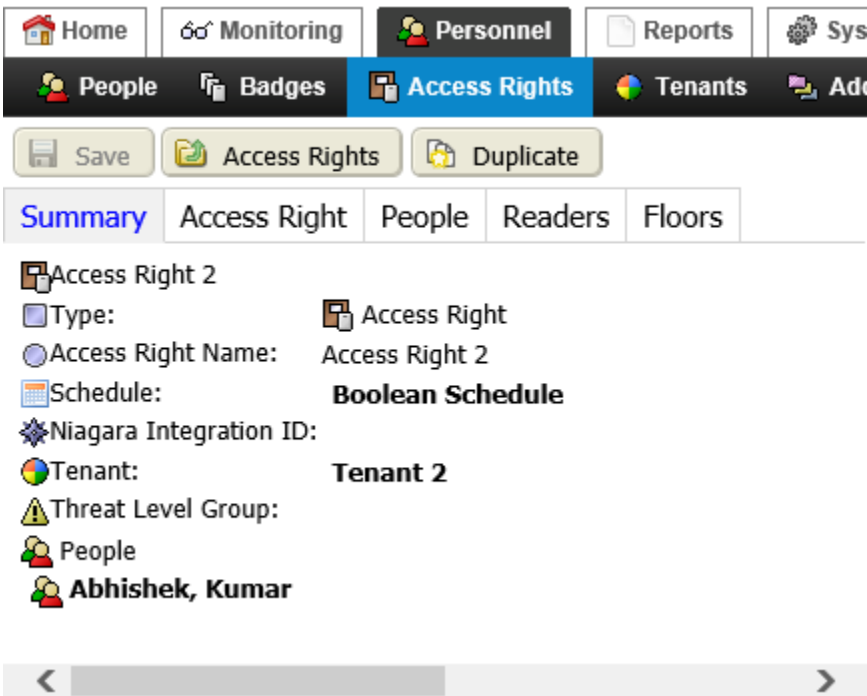
Property	Value	Description
		becomes valid for a specific person.
End Date	date	Determines when an access right is no longer valid for a specific person.
Assigned Threat Level	drop-down list, defaults to Default	Directly assigns a threat level to the person. To break the connection between the access right and threat level group, this property must be configured to something other than Default. When a group of people share the same access right, you use this assignment to configure a different procedure for a single member of the group during a threat level activation.

Access Rights Summary window

This window summarizes the access rights associated with a specific person.

This view summarizes the access rights information.

Figure 30. Access Rights Summary window



Property	Description
Type	Reports the type of database record.
Access Right Name	Identifies the associated access right.
Schedule	Identifies the schedule associated with the access right.

Property	Description
Niagara Integration ID	Identifies the integration ID associated with the access right.
Tenant	Reports the name of the associated tenant.
Threat Level Group	Reports the threat level group assigned to the access right.

Add Access Rights filter window

This window reduces the access rights table rows to only those you are interested in viewing.

Figure 31. Add New Person Access Rights filter window

Filter

☐ Access Right Name

%

Must Include

☒ Case Sensitive

☐ Schedule Name

%

Must Include

☒ Case Sensitive

☐ Integration Name

%

Must Include

☒ Case Sensitive

☐ Tenant Name

%

Must Include

☒ Case Sensitive

☐ Threat Level Group Name

%

Must Include

☒ Case Sensitive

☐ Start Date

Time Range

? to ?

>>

☐ End Date

Time Range



? to ?

>>

☐ Assigned Threat Level

Ok

Cancel

To access this filter, click **Personnel > People**, click the Add button () , click the Access Rights tab and click the Filter button ().

Property	Value	Description
Access Right Name	text	Defines the name of the access right.
Schedule Name	text	Defines the name of the schedule that is associated with the access right.
Integration Name	text	Defines the integration name associated with the right.
Tenant Name	text	Defines the tenant name associated with the right.
Threat Level Group Name	text	Defines the threat level group associated with the right.
Start Date	date	Defines when access rights start for

Property	Value	Description
		the person.
End Date	date	Defines when access rights end for the person.
Assigned Threat Level	text	Defines the threat level for the person.

## Badges tab

This tab consists of two panes with tabular information: The Newly Assigned pane shows the badges assigned to the individual whose name appears at the top of the view. The Unassigned pane lists available access rights.

### Figure 32. Badges tab

Save

People

Add New Person

Duplicate

Assign New Badge

Enroll New Badge

Summary

Person

Access Rights

Badges

### Newly Assigned

Credential	Facility Code	Description	Wiegand Format Name	Status
<div> <div></div> <div></div> <div></div> </div> <div> <div></div> <div></div> <div></div> </div>				



### Unassigned

Credential	Facility Code	Description	Wiegand Format Name	Status
0000000000023450	0		55-Bit Wiegand Format	Issue

You access this view by clicking **Personnel > People**, followed by clicking the **Add** button or double-clicking a person row in the table, then clicking the **Badges** tab.

## Control buttons

The following control buttons are available in the Newly Assigned pane.

-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  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.





- Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.

In addition to the standard control buttons Summary, Hyperlink, Filter, and Export, the Assign button is specifically related to the Unassigned pane. You use this button to assign a selected access right to the person’s record, which you are adding or editing.

Columns

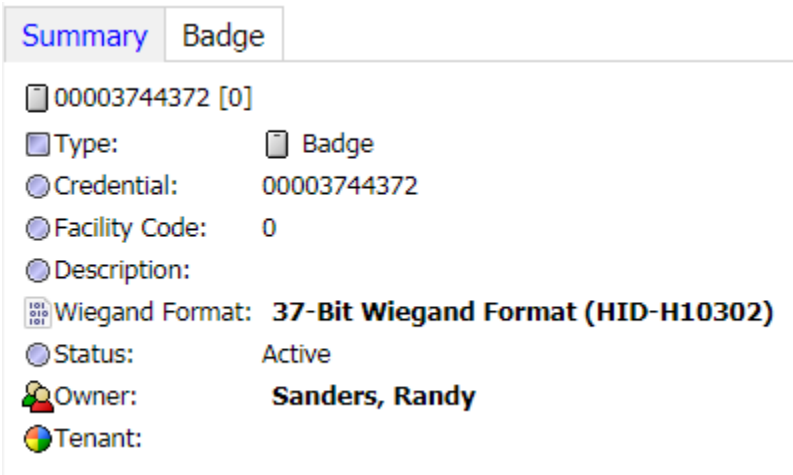
Column	Description
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Last Name	Reports the family name of the person.
First Name	Reports the given name of the person.
Tenant Name	Reports the name of the associated tenant.

Badges Summary tab

This tab, which is part of the Personnel view, summarizes detail information for each badge.

Properties

Figure 33. Badge Summary tab



You access this window from the main menu by clicking **Personnel > People**, followed by clicking the Add



button ( ) and clicking the Summary tab or by double clicking on an existing person and selecting the Summary tab.

















Property	Description
Type	Identifies this summary as containing badge data.
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Owner	Reports the person to whom the badge is assigned.
Tenant	Reports the name of the associated tenant.


Badges view

Every badge that is entered into the system has associated data that is available for display. This view creates and enrolls individual batches as well as groups of badges.

Control buttons





Figure 34. Default Badges view



Credential 	Facility Code	Description	Wiegand Format Name	Status
0000000000000110	0	000110	55-Bit Wiegand Format	Issueable
00000000000075001	0	75001	55-Bit Wiegand Format	Active

You access this view from the main menu by clicking **Personnel > Badges**.

The following are the Badges control buttons:

-  Enroll creates a new badge record by scanning the badge at a reader.
-  Add opens a view or window for creating a new record in the database.
-  Batch Enroll creates and configures new badges by scanning them at a reader.
-  Range Create Badges creates and configures a specific number of new badges by specifying the beginning and ending credential numbers.



- Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.



- 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.



- Show Readers opens the Person Reader Report. The [Reports](#) chapter documents this report.



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



- Show Expirations opens the Person Access Right Report view.



- Delete removes the selected record (row) from the database 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.

## Columns

**Table 6.** Badges columns

Column	Description
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Last Name	Reports the family name of the person.
First Name	Reports the given name of the person.
Tenant Name	Reports the name of the associated tenant.

## Quick Edit window

This window makes available the properties for the selected badge to they can be edited quickly.

Figure 35. Badges Quick Edit window

Quick Edit

Apply to selected items: 1

Apply to all records with the current filter

Description

Employee Badge

Status

Active

Issue Date

TBA

11

Aug

2017

10

:

00

AM

EDT

Expiration Date

Never

11

Aug

2017

12

:

22

PM

EDT


Tenant

FGH Company

>>

Ok

Cancel

You access this view from the main menu by clicking **Personnel > Badges**, followed by selecting a badge record and clicking the Quick Edit button ().

Property	Value	Description
(application)	radio buttons	Apply to selected items: 1 executes the change(s) for only the selected badge. Apply to all records.... executes the change(s) for all badges in the view. If the view is filtered, changes apply to only the filtered badges.
Description	text	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Status	drop-down list	Reports "Issueable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue Date	radio buttons	<div>Defines when each badge is authorized for use. Two options are possible:</div> <div>TBA (to be assigned) allows the issue date to be defined at a later time.</div> <div>Six data options: <code>Month</code>, <code>Day</code>, <code>Year</code>, <code>hour</code>, <code>minutes</code> and <code>AM/PM</code> define the</div>

64

March 25, 2025

Property	Value	Description
issue date.		
Expiration Date	radio buttons	Configures the date and time after which each badge is no longer authorized for use:  never indicates that the badge does not expire.  Six date options: Month, Day, Year, hour, minutes, and AM/PM.
Tenant	Ref chooser	Defines the company name of the associated tenant.

Badges Filter window

This window reduces the badges table rows to only those you are interested in viewing.

Figure 36. Badges filter window

Filter

☐ Credential

%

Must Include

☒ Case Sensitive

☐ Facility Code

%

Must Include

☒ Case Sensitive

☐ Description

%

Must Include

☒ Case Sensitive

☐ Wiegand Format Name

%

Must Include

☒ Case Sensitive☐ Status☐ Last Name

%

Must Include

☒ Case Sensitive☐ First Name

%

Must Include

☒ Case Sensitive☐ Tenant Name

%

Must Include

☒ Case Sensitive

Ok

Cancel

To access this filter, click **Personnel > Badges**, and click the Filter button ().


Criterion	Description
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the purpose or characteristics


Criterion	Description
	of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Last Name	Reports the family name of the person.
First Name	Reports the given name of the person.
Tenant Name	Reports the name of the associated tenant.

Enroll New Badge view

This view creates a new badge record by scanning the badge at a reader. A Save button is located at the top of the view.

Figure 37. Badge tab - Enroll New Badge view

 Save

 Badges

Summary

Badge

Credential

Facility Code

Description

Wiegand Format

Status

Issue Date

Expiration Date

Owner

Tenant

Acceptable Formats

Scanned Badge

Enrollment Reader

None


Issueable ▾

☒ TBA


☐ 08 ▾ - Sep ▾ - 2018 08 ▾ : 48 ▾ AM ▾ IST

☒ Never

☐ 08 ▾ - Sep ▾ - 2018 08 ▾ : 48 ▾ AM ▾ IST

 None

>>

 None

>>

☐ None

>>

You access this view by clicking **Personnel > Badges** followed by clicking the Enroll button (.

Many enroll badge properties are the same as those for creating a new badge. The following table documents

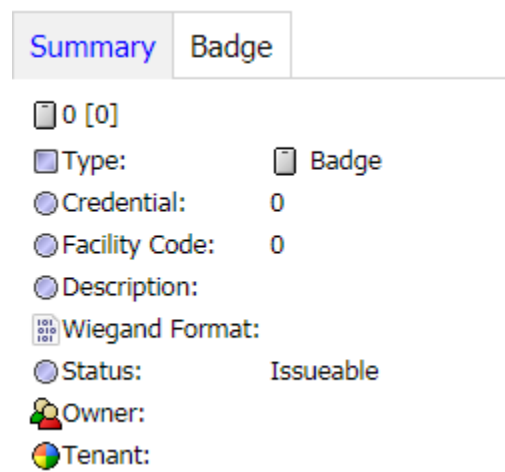
the unique enrollment properties.

Property	Value	Description
Acceptable formats	read-only	Displays the usable card formats for a scanned badge. If more than one format is acceptable, click on the format to use. If only one format is acceptable, or when you select a format from a list of two or more, the system automatically enters the format into the Wiegand Format property.
Scanned Badge	read-only number	Displays the Card ID number detected by the scanner.
Enrollment Reader	Ref Chooser	Defines the reader to use for enrolling new badges.

Enroll New Badge Summary tab

This tab displays badge information as soon as you save new badge data using the properties configured on the Badges tab.

Figure 38. Summary tab for Enroll New Badge



When the data are saved, this tab displays in the appropriate Edit view.

Table 7. Enroll New Badge Summary tab fields

Field	Description
Type	Identifies this summary as containing badge enrollment information.
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the


Field	Description
	purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Owner	Reports the name of the card holder.
Tenant	Reports the name of the associated tenant.


### Add (or edit) New Badge view

This view provides properties to manually create new badges and edit existing badges, one badge at a time. A **Save** button is located at the top of the view.

The Badge tab is the active tab, by default, when you initially open the view. The tab includes the properties to configure a new badge record.

Figure 39. Add New Badge view

 Save

 Badges

Summary

Badge

Credential

0000000000001110

Facility Code

0


Description

Headquarters

Wiegand Format

101  
010  
101

55-Bit Wiegand Format



Status

Active ▾

Issue Date

☐ TBA


☒ 08 ▾ - Sep ▾ - 2018 08 ▾ : 09 ▾ AM ▾ IST

Expiration Date


☒ Never


☐ 08 ▾ - Sep ▾ - 2018 08 ▾ : 58 ▾ AM ▾ IST

Owner


 Bradley, Mandana

>>






Tenant

 None

>>

You access this view by clicking **Personnel > Badges**, followed by clicking the Add badge button (.

Property	Value	Description
Credential No.	number	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.

68

March 25, 2025



Property	Value	Description
Facility Code	text	Identifies the physical building, organization or campus where the badge may be used.
Description	text	Defines a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Ref chooser	Opens the Ref Chooser window used to assign a Wiegand Format from the list of available formats.
Status	drop-down list	Reports "Issueable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue Date	radio buttons	<p>Defines when each badge is authorized for use. Two options are possible:</p> <p>TBA (to be assigned) allows the issue date to be defined at a later time.</p> <p>Six data options: <b>Month, Day, Year, hour, minutes</b> and <b>AM/PM</b> define the issue date.</p>
Expiration Date	radio button and drop-down lists	<p>Configures the date and time after which each badge is no longer authorized for use:</p> <p><b>never</b> indicates that the badge does not expire.</p> <p>Six date options: <b>Month, Day, Year, hour, minutes, and AM/PM</b>.</p>
Owner	Ref chooser	Automatically fills (if you enrolled the person from another view), or defines the owner using the Ref Chooser. The person to whom the badge is assigned is the badge owner.
Tenant	Ref chooser	Defines the company name of the associated tenant.

Add New Badge Summary tab

This tab displays badge information as soon as you configure and save new badge data using the properties on the Badges tab. When the data are saved, this tab displays in the appropriate Edit view.

Figure 40. Add New Badge Summary tab

Summary

Badge

00003744372 [0]

Type:

Badge

Credential:

00003744372

Facility Code:

0

Description:

101  
010  
101

Wiegand Format:

37-Bit Wiegand Format (HID-H10302)

Status:

Active

Owner:

Sanders, Randy

Tenant:

Table 8. Add New Badge Summary tab fields

Field	Description
Type	Identifies this summary as containing badge enrollment information.
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Owner	Reports the name of the card holder.
Tenant	Reports the name of the associated tenant.

Badge tab

This tab appears when you create or edit a new badge.

Properties

Save

Badges

Summary

Badge

Credential

00000000000012345

Facility Code

0

Description

MyBadge

Wiegand Format

55-Bit Wiegand Format

Status

Issueable

Issue Date

TBA

15

Sep

2018

05

00

PM

EDT

Expiration Date

Never

15

Sep

2018

05

00

PM


EDT

Owner

None

Tenant

None


You access this tab from the main menu by clicking **Personnel > Badges** followed by clicking the Add button (  ) or, to edit an existing badge, by double-clicking the badge row in the Badges view.


Property	Value	Description
Credential	read-only	Displays the badge number.
Facility Code	read-only	Displays the building or other number that identifies where the badge can be used..
CredentialDescription	read-only	Displays any additional information about the badge.
Wiegand Format	read-only (Ref Chooser)	Identifies the wiring standard for the card reader.
Status	read-only	Reports "Issueable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue Date	read-only	Displays when the badge was issued.
Expiration Date	read-only	Indicates when the badge is no longer valid.
Owner	read-only	Identifies the person to whom the badge is assigned.
Tenant	read-only	Identifies the tenant to whom this badge belongs.

Batch Enroll Badges view, Badge tab

This view configures and creates new badges by scanning them in at any connected reader.

Figure 41. Batch Enroll Badges, Badge tab

 Save


 Badges

Summary

Badge

Description

Wiegand Format

 None

>>

Status

Issueable ▾

Issue Date

☒ TBA

08 ▾

Sep ▾

2018

09 ▾

: 03 ▾

AM ▾

IST

Expiration Date

☒ Never

08 ▾

Sep ▾

2018


09 ▾

: 03 ▾

AM ▾


IST

Owner

 None

>>

Tenant


 None

>>

New Badges

Scanned Badge

Enrollment Reader

 None

>>

You access this view by expanding **Personnel > Badges** and clicking the Batch Enroll button ().

The Badge tab contains the batch enroll properties. A **Save** button is located at the top of the view.

Property	Value	Description
Description (badge)	text	Defines a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format (badge)	Ref chooser	Opens the Ref Chooser window used to assign a Wiegand Format from the list of available formats.
Status (badge)	drop-down list	Reports "Issueable" until the

Property	Value	Description
		badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue Date (badge)	radio buttons	<p>Defines when each badge is authorized for use. Two options are possible:</p> <p>TBA (to be assigned) allows the issue date to be defined at a later time.</p> <p>Six data options: <code>Month</code>, <code>Day</code>, <code>Year</code>, <code>hour</code>, <code>minutes</code> and <code>AM/PM</code> define the issue date.</p>
Expiration, Expiration Date (badge)	radio button and drop-down lists	<p>Configures the date and time after which each badge is no longer authorized for use:</p> <p><code>never</code> indicates that the badge does not expire.</p> <p>Six date options: <code>Month</code>, <code>Day</code>, <code>Year</code>, <code>hour</code>, <code>minutes</code>, and <code>AM/PM</code>.</p>
Owner (badge)	Ref chooser	Automatically fills (if you enrolled the person from another view), or defines the owner using the Ref Chooser. The person to whom the badge is assigned is the badge owner.
Tenant	Ref chooser	Defines the company name of the associated tenant.
Scanned Badge	read-only number	Displays the badge ID of the most recently-scanned badge.
Enrollment Reader	Ref chooser (required)	Identifies the reader to use.

### Batch Enroll Summary tab

This tab displays badge information as soon as you save new badge data using the properties configured on the Badges tab. When the data are saved, this tab displays in the appropriate edit: view.

**Figure 42.** Batch Enroll Badges Summary tab

Summary

Badge

0 [0]

Type:

Badge

Credential:

0

Facility Code:

0

Description:

101  
010  
101

Wiegand Format:

Status:

Issueable

Owner:

Tenant:


**Table 9.** Enroll New Badge Summary tab properties


Field	Description
Type	Identifies this summary as containing badge enrollment information.
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Owner	Reports the name of the card holder.
Tenant	Reports the name of the associated tenant.

Range Create Badges view, Badge tab

This view configures and creates a specific number of new badges by specifying beginning and ending credential numbers.

**Figure 43.** Range Create Badges view, Badge tab

 Save

 Badges


Summary

Badge

Facility Code

Description

Wiegand Format

 None

>>

Status

Issueable

▼

Issue Date

☒ TBA

☐

08

▼

Sep

▼

2018

09

▼

:

19

▼

AM

▼

IST

Expiration Date

☒ Never

☐

08

▼

Sep

▼

2018

09

▼

:

19


▼

AM

▼


IST

Owner

 None

>>


Tenant

 None

>>

Credential Start

Credential Finish

You access this view by clicking **Personnel > Badges**, followed by clicking the Range Create Badges button (  ).

You access this tab from the main menu by clicking

The Badge tab contains the range-create badges properties. A **Save** button is located at the top of the view.

Property	Value	Description
Facility Code	text	Identifies the physical building, organization or campus where the badge may be used.
Description	text	Defines a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Ref chooser	Opens the Ref Chooser window used to assign a Wiegand Format from the list of available formats.
Status	drop-down list	Reports "Issueable" until the

Property	Value	Description
		badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue Date	radio buttons	<p>Defines when each badge is authorized for use. Two options are possible:</p> <p>TBA (to be assigned) allows the issue date to be defined at a later time.</p> <p>Six data options: <code>Month</code>, <code>Day</code>, <code>Year</code>, <code>hour</code>, <code>minutes</code> and <code>AM/PM</code> define the issue date.</p>
Expiration Date	radio button and drop-down lists	<p>Configures the date and time after which each badge is no longer authorized for use:</p> <p><code>never</code> indicates that the badge does not expire.</p> <p>Six date options: <code>Month</code>, <code>Day</code>, <code>Year</code>, <code>hour</code>, <code>minutes</code>, and <code>AM/PM</code>.</p>
Owner	Ref chooser	Automatically fills (if you enrolled the person from another view), or defines the owner using the Ref Chooser. The person to whom the badge is assigned is the badge owner.
Tenant	Ref chooser	Defines the company name of the associated tenant.
Credential Start	number	Identifies the number to use for the first badge in the range.
Credential Finish	number	Identifies the number to use for the last badge in the range

### Range Create Badges Summary tab

This tab displays badge information as soon as you save new badge data using the properties configured on the Badge tab. When the data are saved, this tab displays in the appropriate edit view.



**Figure 44.** Range Create Badges Summary tab

Summary

Badge

00003744372 [0]

Type:

Badge

Credential:

00003744372

Facility Code:

0

Description:

101  
010  
101

Wiegand Format:

**37-Bit Wiegand Format (HID-H10302)**

Status:

Active

Owner:

**Sanders, Randy**

Tenant:

**Table 10.** Range Create Badges Summary tab properties

Property	Description
Type	Identifies this summary as reporting badge enrollment information.
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Owner	Reports the name of the card holder.
Tenant	Reports the name of the associated tenant.

Access Rights view

An access right is database record that identifies which facilities a person may enter. A schedule associated with an access right identifies the door(s) and reader(s) a person may use to enter. An access right provides information about where a person typically resides in a building. Multiple tenants may share the same access rights. This table view lists all the access rights that exist in the system.

To open this view, expand **Personnel** and click **Access Rights**.

Figure 45. Access Rights view

Access Right Name	Schedule Name	Integration Name	Tenant Name
Employees	MorningHours		
Operator	Evening		
Tridium	Always		

You access the **Access Rights** views by clicking **Personnel > Access Rights**.

Control buttons

In addition to the standard control buttons (Filter, Column Chooser, Refresh, Manage Reports, and Export), the following are Access Rights control buttons:

- Add opens a view or window for creating a new record in the database.
- Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
- 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.
- Delete removes the selected record (row) from the database table. This button is available when you select an item.
- Match with discovery initiates an action to update a single item that is already in the system database. It is available 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.
- 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.
- Duplicate opens a New window and populates each property with properties from the selected item. Using this button speeds the item creation.
- Show Expirations opens the Person Access Right Report view.

-  Show Readers opens the Person Reader Report. The *Reports* chapter documents this report.

Columns

Table 11. Access Rights columns

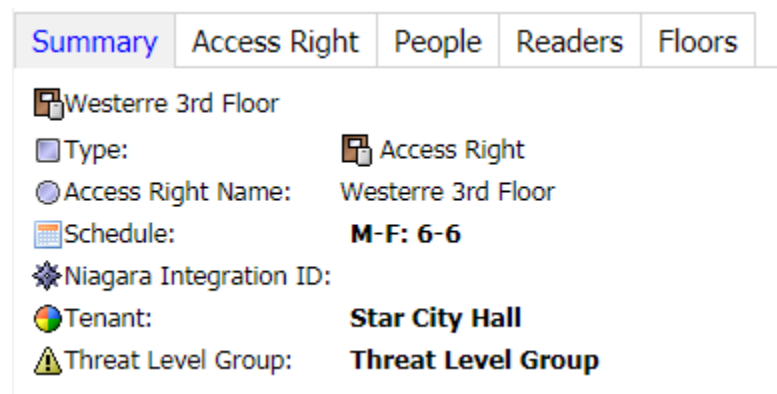
Column	Description
Access Right Name	Identifies the title of the access right associated with the entity.
Schedule	Reports the name of the associated schedule (if any).
Niagara Integration ID	Reports the name of the associated integration ID. The system performs building automation actions, such as turning the lights on, associated with this type of ID.
Tenant	Reports the name of the associated tenant.
Threat Level Group	Reports the name of the associated threat level group.

Access Rights Summary tab

The summary tab provides the details for the currently-selected access right.

The Summary tab on the New **Access Right** view displays the following information. The system updates it after you enter and save an access right. The Summary tab may also include context-appropriate lists of floors, people and card readers that are associated with the displayed access right.

Figure 46. Access rights Summary window



You access the Summary tab from the **Access Rights** view by clicking the Summary tab in an existing Access Right or by clicking the Summary tab from the Add New Access Right view.

You access the new access right Summary tab by clicking the Summary tab.

Table 12. Summary of access right properties

Property	Description
Type	Identifies this summary as a collection of access right data.
Access Right Name	Identifies the title of the access right associated with the entity.
Schedule	Reports the name of the associated schedule (if any).
Niagara Integration ID	Reports the name of the associated integration ID. The system performs building automation actions, such as turning the lights on, associated with this type of ID.

Property	Description
Tenant	Reports the name of the associated tenant.
Threat Level Group	Reports the name of the associated threat level group.
People	Reports the names of the people authorized to enter the building.

Quick Edit window

This window edits the important properties associated with a person’s access rights.

Figure 47. Access Rights Quick Edit view

Quick Edit

☒ Apply to selected items: 1

☐ Apply to all records with the current filter

☐ Schedule

Building unlocked

>>

☐ Niagara Integration ID

None

>>

☐ Tenant

FGH Company

>>

☐ Threat Level Group

None

>>

☐ Threat Level Operation

Normal

☐ Default Assigned Threat Level

--Default--

☐ Add People

None

>>

☐ Remove People

None

>>

☐ Add Readers

None

>>


☐ Remove Readers

None

>>

Ok

Cancel

This window opens when you click the Quick Edit button () at the top of the Access Rights view.

Apply to selected items: <number selected> changes only the selected access rights.

Apply to all records with the current filter changes all records identified by the filter.

Property	Value	Description
Schedule	text	Identifies the name of the schedule (if any) that is assigned to the access right.
Niagara Integration ID	text	Describes the physical space where a tenant card holder typically resides in a facility. This information may be passed to a building automation system by BACnet, for example, so that

Property	Value	Description
		when a person exercises this access right by entering the facility, the appropriate lighting, HVAC, and other controls adjust automatically.
Tenant	Ref chooser	Defines the company name of the associated tenant.
Threat Level Group	Ref chooser	Lists the Threat Level Group (if any) that is assigned to the access right.
Threat Level Operation (appears only when a <b>Threat Level Group</b> is assigned)	drop-down list (defaults to Normal)	<p>Defines how the access right responds to a threat level.</p> <p><b>Normal</b> allows normal access (as if no threat level is assigned) when the currently-active threat level is equal to or less than the threat level assigned to the person's access right.</p> <p><b>Specific Level</b> allows normal access (as if no threat level is assigned) as long as the currently-active threat level is equal to the threat level assigned to the person's access right.</p> <p><b>Reverse</b> allows normal access (as if no threat level is assigned) as long as the currently-active threat level is equal to or greater than the threat level assigned to the person's access right.</p> <p><b>Reverse</b> allows some types of people (emergency responders) into a facility when the active threat level is elevated.</p>
Default Assigned Threat Level	defaults to -Default-	<p>Defines a specific threat level to associate with an access right.</p> <p>If you leave this property set to -Default-, the access right inherits the threat level from the <b>Default Access Right Threat Level</b> property as defined for the selected threat level group.</p>
Add People	Ref Chooser	Associates people to this access

Property	Value	Description
		right.
Remove People	Ref Chooser	Disassociates people from this access right.
Add Readers	Ref Chooser	Associates one or more readers with this access right.
Remove Readers	Ref Chooser	Disassociates one or more readers with this access right.

Filter window

This window selects which records to view in the table.

Figure 48. Filter window for access rights

Filter

☒ Access Right Name

%

Must Include

☒ Case Sensitive

☐ Schedule Name

%

Must Include

☒ Case Sensitive

☐ Integration Name

%

Must Include

☒ Case Sensitive

☐ Tenant Name

%

Must Include

☒ Case Sensitive☐ Threat Level Group Name

%

Must Include

☒ Case Sensitive

Ok

Cancel

To access this filter from the main menu, click **Personnel > Access Rights**, followed by clicking the Filter button



Type	Value	Description
Access Right Name	wild card (%)	Sets up one or more access rights as search criteria.
Schedule Name	wild card (%)	Sets up one or more schedule names as search criteria.
Integration Name	wild card (%)	Sets up one or more integration names as search criteria.
Tenant Name	wild card (%)	Sets up one or more tenant names as search criteria.
Threat Level Group Name	wild card (%)	Sets up one or more threat level group names as search criteria.

## Add New (and edit) Access Rights view, Access Right tab

This view provides properties to configure and create new access rights.

**Figure 49.** Add New Access Right view

Save

Access Rights

Duplicate

Summary

Access Right

People

Readers

Floors

Access Right Name

Employees

Schedule

MorningHours

»

Niagara Integration ID

None

»

Tenant

None

»

Threat Level Group

None

»

Description

You access this view by clicking **Personnel > Access Rights**, followed by clicking the Add access right button (  ).

To edit an existing access right you double-click a row in the Access Rights table. A **Save** button is located at the top of the view.

Property	Value	Description
Access Right Name	text	Provides a descriptive title for the access right.
Schedule Name	Ref chooser (required value)	Identifies the name of an existing schedule that provides a boolean (true or false) output to indicate when the access right is in effect over a 24-hour day, 7-day week. For example, an access right called "Weekdays: 8 to 5," which is associated with a schedule set up for Monday through Friday, 8 am to 5 pm would not allow access before 8 am or after 5 pm Monday through Friday.
Niagara Integration ID	text	Describes the physical space where a tenant card holder typically resides in a facility. This

Property	Value	Description
		information may be passed to a building automation system by BACnet, for example, so that when a person exercises this access right by entering the facility, the appropriate lighting, HVAC, and other controls adjust automatically.
Tenant	Ref chooser	Defines the company name of the associated tenant.
Threat Level Group	Ref chooser	Associates the access right with a threat level group. If you assign the group, the system expands the tab adding two additional properties: <b>Threat Level Operation</b> and <b>Default Assigned Threat Level</b> .
Threat Level Operation (appears only when a <b>Threat Level Group</b> is assigned)	drop-down list (defaults to Normal)	<p>Defines how the access right responds to a threat level.</p> <p><b>Normal</b> allows normal access (as if no threat level is assigned) when the currently-active threat level is equal to or less than the threat level assigned to the person's access right.</p> <p><b>Specific Level</b> allows normal access (as if no threat level is assigned) as long as the currently-active threat level is equal to the threat level assigned to the person's access right.</p> <p><b>Reverse</b> allows normal access (as if no threat level is assigned) as long as the currently-active threat level is equal to or greater than the threat level assigned to the person's access right.</p> <p><b>Reverse</b> allows some types of people (emergency responders) into a facility when the active threat level is elevated.</p>
Default Assigned Threat Level	defaults to -Default-	<p>Defines a specific threat level to associate with an access right.</p> <p>If you leave this property set to</p>

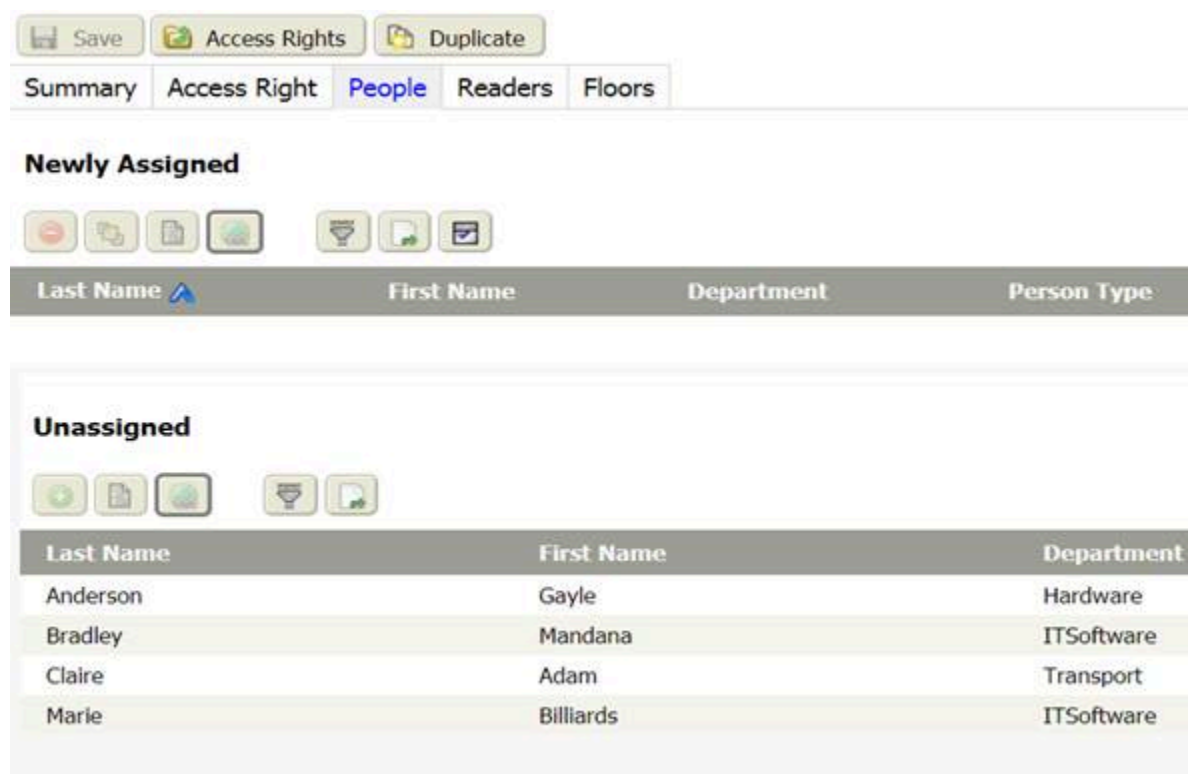



Property	Value	Description
		-Default-, the access right inherits the threat level from the Default Access Right Threat Level property as defined for the selected threat level group.
Description	text	Provides a longer description of the access right and its purpose.

People tab

This tab provides a set of standard control buttons for using the learn mode to assign people to the access right. It displays a table of available people, as well as lists the currently assigned or newly assigned people.





Figure 50. Add New Access Rights People tab



To view access right assignments by employee name, click **Personnel > Access Rights**. Then click the Add access right button (  ) followed by clicking the People tab.

Control buttons

The following control buttons provide the functions on this tab.

-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  Change Assignment Properties opens the Change Assignment Properties window.
-  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.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.

Columns

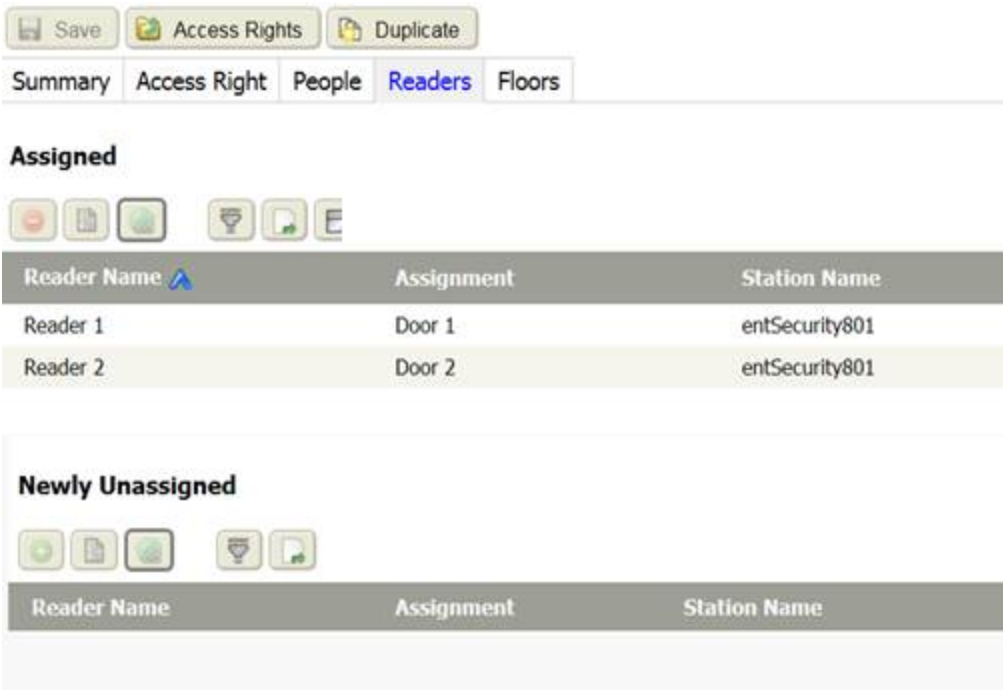
**Table 13.** Access Rights, People tab columns

Column	Description
Last Name	Reports the family name of the person.
First Name	Reports the given name of the person.
Department	Reports where within the organization’s flow chart the person works.
Person Type	Reports additional information about the person.
Tenant Name	Reports the name of the associated tenant.
Start Date	Reports the beginning date from the schedule.
End Date	Reports the final date from the schedule.
Assigned Threat Level	Reports the threat level assignment.

Readers tab

This tab provides a set of standard control buttons for using the learn mode to assign readers to the access right. It displays a table of available readers, as well as lists the currently assigned or newly assigned readers.




Figure 51. Access Rights, Readers tab



To view reader assignments, click **Personnel > Access Rights**. Then click the Add access right button (  ) followed by clicking the Readers tab.

Control buttons

These buttons provide the features on this view.

-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  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.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.

Columns

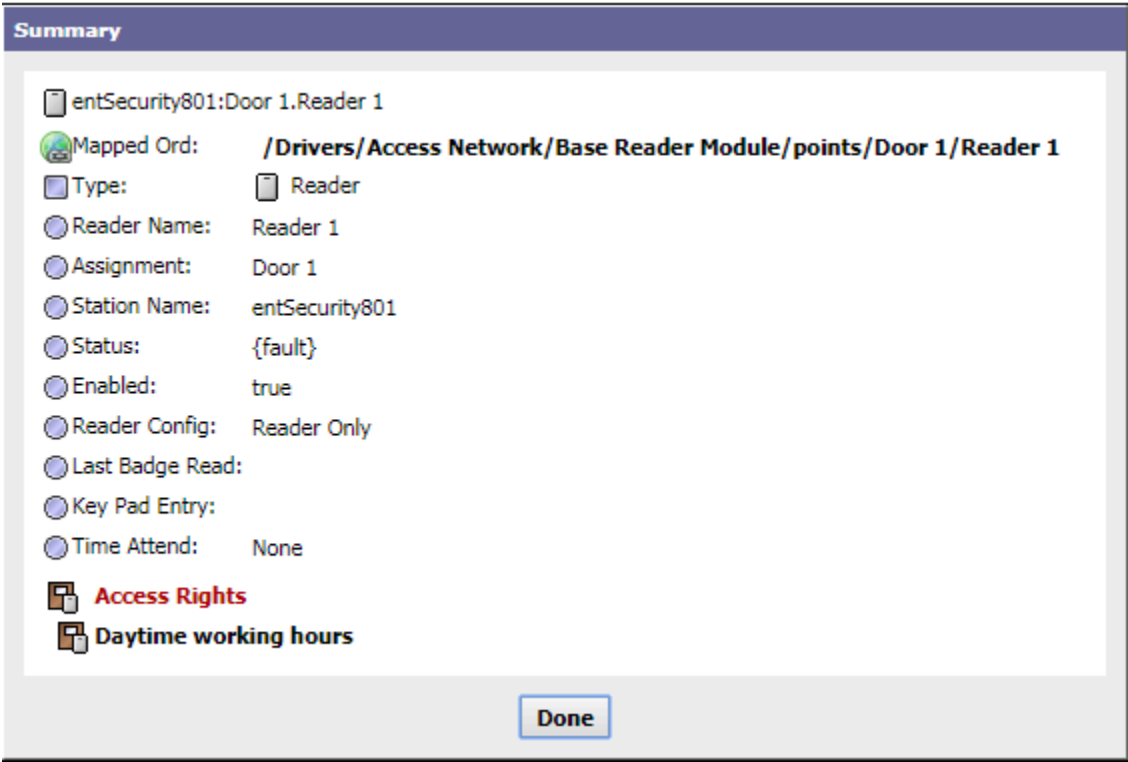
Table 14. Access Rights, People tab columns

Column	Description
Reader Name	The name associated with the reader.
Assignment	Indicates the door with which the reader is associated.
Station Name	Reports the name of the station managing the access rights.

Readers tab, Summary window

This window summarizes reader properties.

**Figure 52.** Readers tab Summary window



This window opens when you click the Summary button () with an Access Right selected. The follow table lists typical Summary properties displayed in this window.

**Table 15.** Summary properties

Property	Description
Mapped Ord	Locates the device in the station.
Type	Indicates the type of device.
Reader Name	Indicates the name of the reader.
Assignment	Indicates the door to which the reader is assigned.
Station Name	Identifies the name of the controlling station.
Status	Indicates the current status of the device.
Enabled	Indicates if the device is enabled (true) or disabled (false)
Reader Config	Indicates how the reader is configured: as "Reader Only," or "Reader and Keypad," or other options that depend on the reader model. When configured to "Reader Only," only a badge swipe is required to gain access. If "Reader and Keypad," the person must swipe a badge and enter a PIN.
Last Badge Read	Identifies the last badge the reader processed.
Key Pad Entry	Displays the most recent PIN entered at the reader key pad. For security reasons, this property is hidden.
Time Attend	Indicates when the last badge swipe at the reader occurred.

Readers tab, Filter window

This window defines search criteria.

**Figure 53.** Readers tab Filter window

Filter

☐ Reader Name

Must Include

▼

☒ Case Sensitive

☐ Assignment

Must Include

▼

☒ Case Sensitive

☐ Station Name

Must Include

▼

☒ Case Sensitive

Ok

Cancel

You open this window by clicking the Filter button ().

Property	Value	Description
Reader Name	wild card (%)	Sets up one or more reader names as search criteria.
Assignment	wild card (%)	Sets up one or more floor assignments as search criteria.
Station Name	wild card (%)	Sets up one or more station names as search criteria.

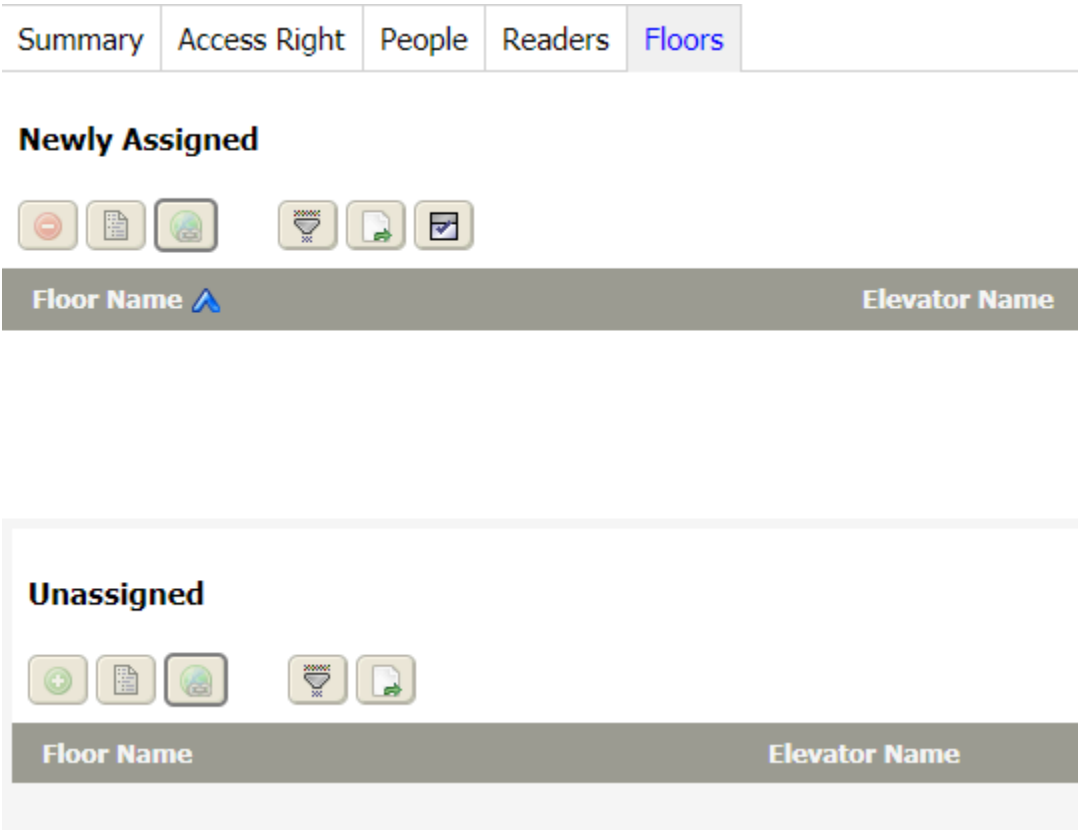
Floors tab

This tab provides a set of standard control buttons for using the learn mode to assign floors to the access right. It displays a table of available floors, as well as lists the currently assigned or newly assigned floors.

**NOTE:**

Floors are only available when elevators are configured.




**Figure 54.** Access Rights, Floors tab



To view floor assignments, click **Personnel > Access Rights**. Then click the Add access right button () followed by clicking the Floors tab.

**Control buttons**

These buttons provide view features:

-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  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.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.

Columns

**Table 16.** Access Rights, People tab columns

Column	Description
Floor Name	Reports the name associated with the reader.
Elevator Name	Reports the name of the elevator.
Station Name	Reports the station name.

Floors tab, Filter window

This window sets up search criteria related to elevators and floors.

**Figure 55.** New Access Right, Floors tab Filter window

Filter

☐ Floor Name

Must Include

▼

☒ Case Sensitive

☐ Elevator Name

Must Include

▼

☒ Case Sensitive

☐ Station Name

Must Include

▼

☒ Case Sensitive

Ok

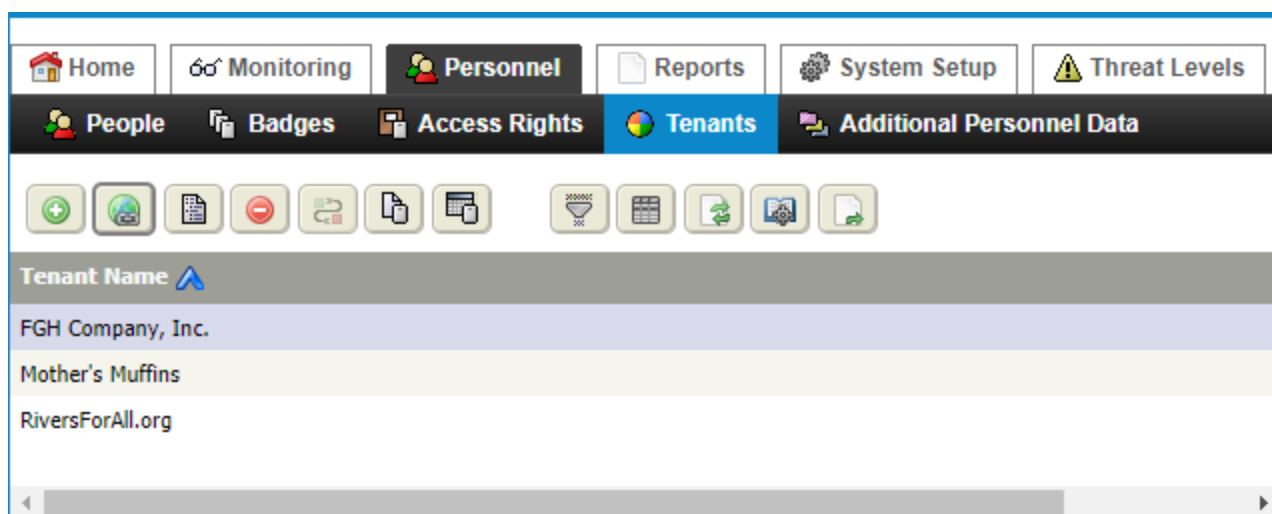
Cancel

You open this window by clicking the Filter button ().

Property	Value	Description
Floor Name	wild card (%)	Sets up the name of one or more floors as search criteria.
Elevator Name	wild card (%)	Sets up the name of one or more elevators as search criteria.
Station Name	wild card (%)	Sets up the name of one or more stations as search criteria.







Tenants view

These views, window and tabs manage tenant information.

**Figure 56.** Tenants view

To open this view, expand **Personnel** and click **Tenants**.

In addition to the standard control buttons (Column Chooser, Refresh, Manage Reports, and Export, these control buttons apply specifically to Tenants:

- 
 Add opens a view or window for creating a new record in the database.
- 
 Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
- 
 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.
- 
 Delete removes the selected record (row) from the database table. This button is available when you select an item.
- 
 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.)
- 
 Show Readers opens the Person Reader Report. The [Reports](#) chapter documents this report.





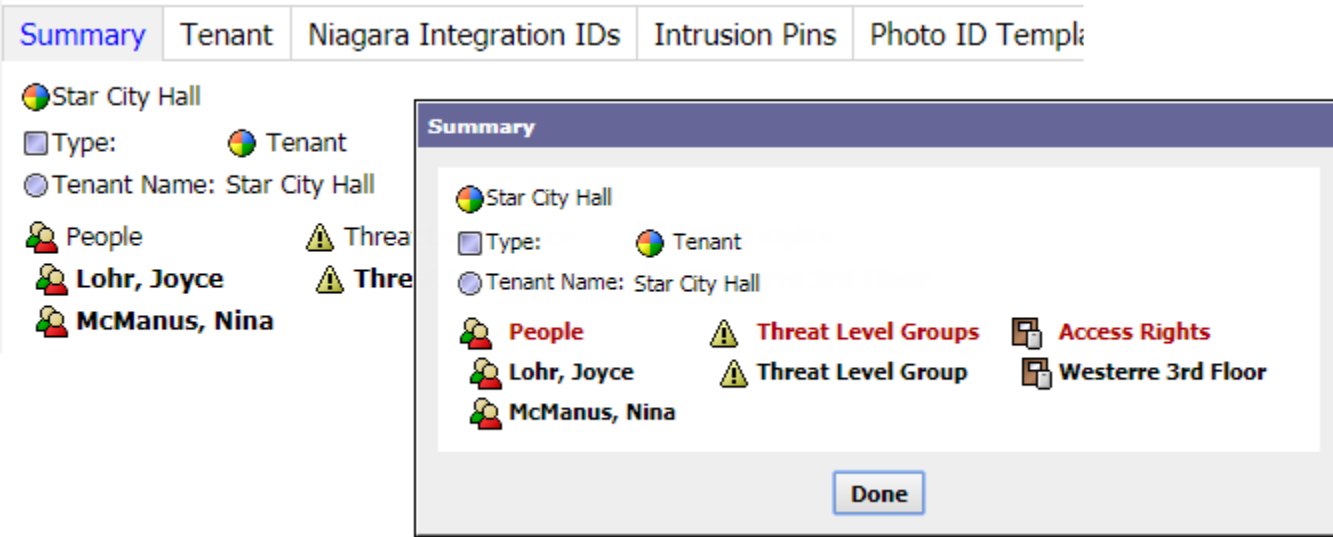
- Show Expirations opens the Person Access Right Report view.


Tenants Summary window/tab

This window and tab display information about a single tenant.

The Summary tab is present but does not display updated information until you enter data and save the Add New Tenant or edit tenant tabs. When a new tenant is saved, this tab displays in the appropriate edit view. This tab may also include context-appropriate lists of integration ID, people, badges, and access rights that are associated with the displayed tenant.

Figure 57. Tenants Summary window and tab



You access the Summary window from the Tenants view by clicking the Summary button (  ).

You access the Summary tab from the Add New Tenant view (after entering and saving a tenant) by clicking the Summary tab.

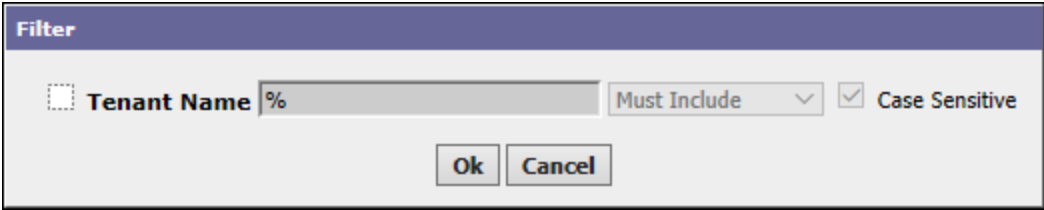
Table 17. Tenant properties

Property	Description
Type	Reports the type of database record.
Tenant Name	Reports the name of the tenant.
People	People assigned to the tenant group
Threat Level Groups	Threat level groups assigned to the tenant
Access Rights	Access rights assigned to the Tenant
Other	Additional assigned properties can include: Niagara Integrations IDs, Intrusion Pins, Photo ID Templates, andBadges.

Filter window

This window sets the search criterion for tenant records.

**Figure 58.** Tenants Filter window



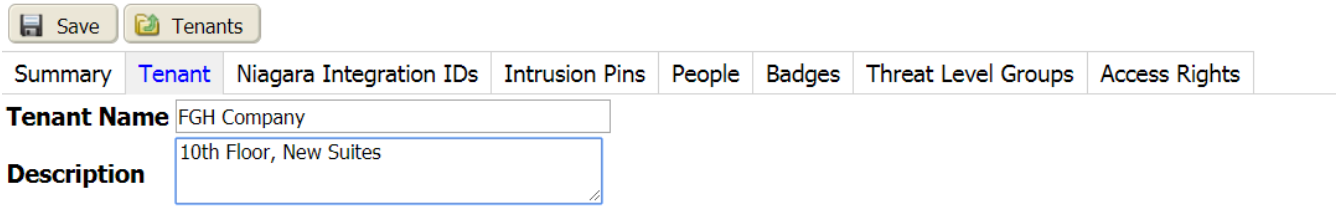
The tenant name serves as the sole criterion for searching.


Add (or edit) a New Tenant view


This view adds or edits a tenant record in the database.

This tab is the active tab, by default.

**Figure 59.** Tenant tab



You access this view by clicking **Personnel > Tenants**, followed by clicking the Add button (). To edit an

existing tenant, double-click on a table row or, with the row selected, click on the Hyperlink button (.

The Tenant tab is the active tab, by default. A **Save** button is located at the top of the view and the following tabs and property fields are available for specifying a new tenant.




Property	Value	Description
Tenant Name	text	Defines the name of the tenant.
Description	text	Provides any general information about the nature of the tenant.

Tenants Niagara Integration IDs tab

This tab assigns integration IDs to the tenant. An integration ID associates BAS (Building Automation System), such as room temperature and lighting with a tenant.

You access this view by clicking **Personnel > Tenants**, followed by clicking the Niagara Integration IDs tab.

In addition to the standard control buttons (Export and Assign Mode), the Newly Assigned pane of this report provides these report-specific tabs:


-  Unassign disassociates the integration ID from the tenant.
-  Summary opens a window that summarizes the selected integration ID's properties.
-  Hyperlink opens the integration ID view for the selected ID. This view is documented in the [Controller Setup—Remote Devices](#) chapter.


The Unassigned pane includes the Assign button (  ), which assigns a discovered integration ID to the tenant.

### Tenants Intrusion Pins tab

This tab assigns intrusion PINs to the tenant.

Figure 60. Intrusion Pins tab

 Save

 Tenants

Summary

Tenant

Niagara Integration IDs




Intrusion Pins




People

Badges

T




Assigned







Intrusion Pin Name	Schedule Name	Tenant Name
DoorPin	Evening	FGH Company

Newly Unassigned









Intrusion Pin Name	Schedule Name	Tenant Name
--------------------	---------------	-------------

You access this view by clicking **Personnel > Tenants**, followed by clicking the Intrusion Pins tab.

Control buttons

In addition to the standard control buttons (Export and Assign Mode), the Newly Assigned pane of this report provides these report-specific tabs:


-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  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.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.


The Unassigned pane includes the Assign button () , which assigns a discovered intrusion PIN to the tenant.

Tenants People tab

This tab assigns people to the tenant.

Figure 61. Tenant tab

 Save

 Tenants

Summary

Tenant

Niagara Integration IDs




Intrusion Pins




People

Badges

Three




Newly Assigned







Last Name	First Name	Department	Person Type
-----------	------------	------------	-------------

Unassigned








Last Name	First Name	Department	Person Type
Anderson	Gayle	Hardware	
Bradley	Mandana	ITSoftware	
Claire	Adam	Transport	
Marie	Billiards	ITSoftware	

You access this view by clicking **Personnel > Tenants**, followed by clicking the People tab.

Control buttons

In addition to the standard control buttons (Export and Assign Mode), the Newly Assigned pane of this report provides these report-specific tabs:

-  Remove Assignment (Unassign) disassociates an assignment that was previously made.


-  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.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.


The Unassigned pane includes the Assign button () , which assigns a discovered person to the tenant.

Tenants Badges tab

This tab assigns badges to the tenant.







Figure 62. Badges tab







 Save

 Tenants

Summary	Tenant	Niagara Integration IDs	Intrusion Pins	People	Badges	Threat Level Groups
---------	--------	-------------------------	----------------	--------	--------	---------------------


Newly Assigned





Credential	Facility Code	Description	Wiegand Format Name	Status	Last Name
Unassigned					
<div><div></div></div>					
Credential	Facility Code	Description	Wiegand Format Name	Status	Last Name
0000000000001110	0	Headquarters	55-Bit Wiegand Format	Active	Bradley
00000000000023450	0	Main Building	55-Bit Wiegand Format	Issueable	

You access this view by clicking **Personnel > Tenants**, followed by clicking the Badges tab.

In addition to the standard control buttons (Export and Assign Mode), the Newly Assigned pane of this report provides these report-specific tabs:

-  Unassign disassociates the badge from the tenant.

-  Summary opens a window that summarizes the selected badge's properties.
-  Hyperlink opens the badges view for the selected badge. This view is documented in the *Badges, views, tabs, and windows* topics.

The Unassigned pane includes the Assign button () , which assigns a discovered badge to the tenant.

### Tenants Threat Level Groups tab

This tab assigns a threat level group to a tenant.

**Figure 63.** Threat Level Group tab

Save

Tenants

Summary

Tenant

Niagara Integration IDs

Intrusion Pins




People




Badges







Threat Level Groups

Access

Newly Assigned







Threat Level Group Name	Path 	Active Level	Default Access Right Threat Level
Unassigned			
<div><div></div><div></div></div>			
Threat Level Group Name	Path	Active Level	Default Access Right Threat Level
Threat Level Group	/Threat Level Group/	Low [0]	Low [0]

You access this view by clicking **Personnel > Tenants**, followed by clicking the Threat Level Groups tab.

#### Control buttons

In addition to the standard control buttons (Export and Assign Mode), the Newly Assigned pane of this report provides these report-specific tabs:

-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  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.




- Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.


The Unassigned pane includes the Assign button () , which assigns a discovered threat level group to the tenant.

Tenants Access Rights tab

This tab assigns access rights to the tenant.







Figure 64. Access Rights tab

 Save

 Tenants






Summary	Tenant	Niagara Integration IDs	Intrusion Pins	People	Badges	Threat Level
---------	--------	-------------------------	----------------	--------	--------	--------------

Newly Assigned



Access Right Name	Schedule Name	Integration Name	Tenant Name
-------------------	---------------	------------------	-------------

Unassigned



Access Right Name	Schedule Name	Integration Name	Tenant Name
honeywell	Schedule123		

You access this view by clicking **Personnel > Tenants**, followed by clicking the Access Rights tab.

Control buttons

In addition to the standard control buttons (Export and Assign Mode), the Newly Assigned pane of this report provides these report-specific tabs:

- Remove Assignment (Unassign) disassociates an assignment that was previously made.

- 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

100

March 25, 2025



same information as the Summary window.



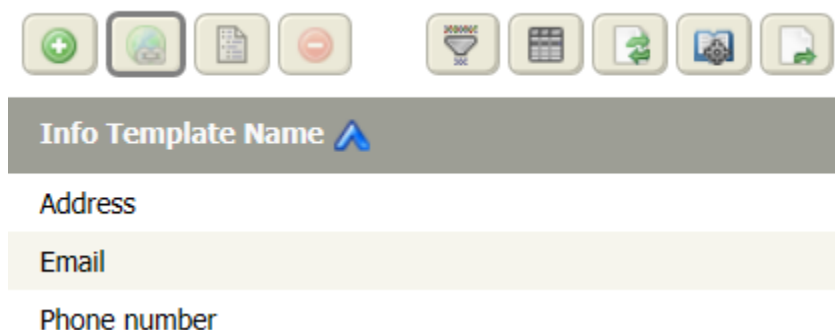
- Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.

The Unassigned pane includes the Assign button () , which assigns a discovered access right to the tenant.

## Additional Personnel Data view

This view lists all the existing Person Info Templates. These templates create custom properties that are added to personnel (people) records.

**Figure 65.** Additional Personnel Data view



**NOTE:** You can use the column chooser mode to add up to 10 additional data rows for a person.

### Control buttons

The following are the control buttons for this view:



- Add opens a view or window for creating a new record in the database.



- Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.



- 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.



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

Columns

Table 18. Additional Personnel Data columns

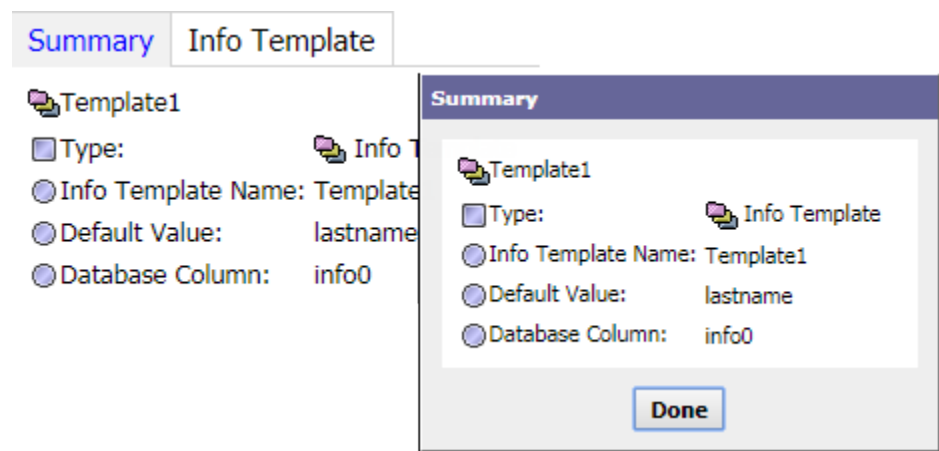
Column	Description
Info Template Name	Provides a descriptive title (display name) for the template.
Default Value	Reports the text that by default displays for the property in the Add New Person and edit person views.

Additional Personnel Data Summary window/tab

This window and tab display information about a additional personnel template.

The Summary tab is present but does not display updated information until you enter data and save the Add New Info Template or edit the Info Template tab. When a new template is saved, this tab displays in the appropriate edit view. This tab may also include context-appropriate lists of additional information.

Figure 66. Additional Personnel Data Summary window and tab



You access the **Summary** window from the Additional Personnel Data view by clicking the Summary button.

You access the Summary tab from the Add New Info Template view (after entering and saving a template) by clicking the Summary tab.

Table 19. Summary properties

Property	Description
Type	Identifies these summary data as additional personnel data.
Info Template	Reports the name of the template that contains the additional data.
Default value	Displays the value that defaults when no other value is provided.
Database column	Identifies the column in the table to which the property is mapped.

Additional Personnel Data Filter window

This window defines the search criteria for searching the database.

**Figure 67.** Filter (Additional Personnel Data

Filter

☐ Info Template Name

%

Must Include

▼

☒ Case Sensitive

☐ Default Value

%

Must Include

▼

☒ Case Sensitive

Ok

Cancel

You open this filter by clicking **Personnel > Additional Personnel Data** followed by clicking the Filter button (



).

Criterion	Value	Description
Info Template Name	wildcard (%)	Sets up a search by the name of the template.
Default Value	wildcard (%)	Sets up a search by the default value.

### Add (or edit) an Info Template view

This view provides properties for adding a new or editing an existing person. The templates you create here appear at the end of the Person tab in the Add New (or edit) Person view.

The Info Template tab is the active tab, by default.

**Figure 68.** Add New Info Template view

Summary

Info Template

Info Template Name

Info Extra

Default Value

A Value

Smart Sense


true ▼

Multi Line

true ▼

To create or edit a Person Info Template you click **Personnel > Additional Personnel Data**, and click the add

button (  ).

To edit an existing Info Template you double-click a row in the table or click the hyperlink button (  ).

## Properties

Property	Value	Description
Info Template Name	text	Provides a descriptive title for the property. This is the label that appears at the end of the Person tab in the Add New Person or edit person views.
Default Value	text	Sets a string value that appears by default when the property displays in the Add New Person or edit person views.
Smart Sense	true or false	When set to true, the system allows you to include a link (the >> icon) to the <b>String Chooser</b> window. The link appears next to the information value property in the Add New Person or edit person views.
Multi Line	true or false	When set to true, this option configures the value text box for more than a single line of text.

# Chapter 4. Reports views

The system provides three groups of pre-configured reports: history reports, hardware reports, and miscellaneous reports. In addition, you can save your own custom-filtered and configured reports.

**Figure 69.** Reports menu


























		Reports
		Access History
		Alarm History
		Intrusion History
		Attendance History
		Audit History
		Log History
		Hardware Reports
		Doors
		Readers
		Inputs
		Outputs
		Elevators
		Remote Modules
		Intrusion Displays
		BACnet Points
		LDAP Audit History
		Miscellaneous Reports
		Person Access Right Report
		Person Reader Report
		Access Right Reader Report
		Personnel Changes

Table controls also apply to reports.

Types of reports

- History reports are logs that have similar display characteristics and are listed directly under the **Reports** menu item.

Reducing report size

There are two ways to reduce the size of a report:

- You may filter reports to include only the records you are interested in. If you do not filter report data, the system alerts you that only the top 5,000 lines are available. You can individually edit history report record capacities.
- For reports that query an SQL database (the Orion space), you may configure the **Report Type** property,



which is available when you click the Column Chooser or Table control button ( ) on the report. This property uses native SQL pagination and Sub-SQL join statements to combine information from the database.

**NOTE:** The data displayed on any report are based on the last filter settings. If, when you access a report, you do not see the information you expect, check the report filter (click the Filter button).

Advanced Time Range Options window

This window provides options to further filter report records based on time. The options you configure using this window restrict the data retrieved by the initial filter.

Properties

Figure 70. Advanced Time Range Options window

Advanced Time Range Options

Start Time

12:00 AM

End Time

12:00 AM

Days Of Week

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Schedule

None >>

Ok

Cancel

To access these options from any report, click the chevron to the right of the **Time** property. For example, when viewing alarm history, the time properties are **Alarm Time** and **Normal Time**.

**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*.

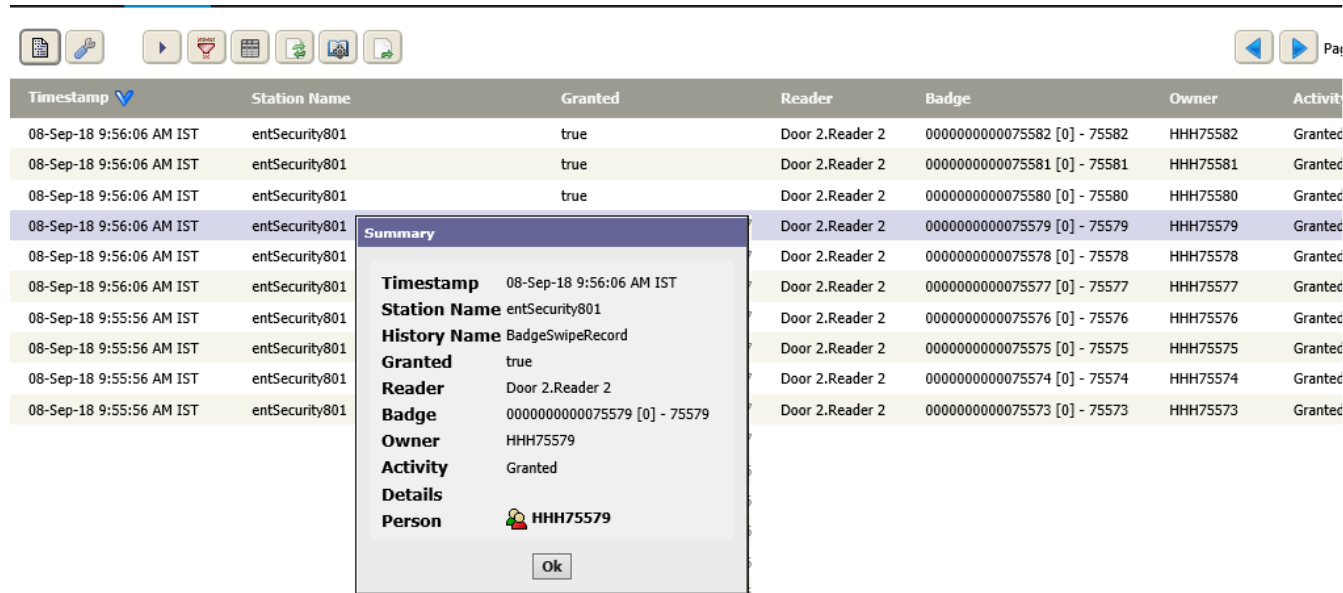
Property	Value	Description
Start Time	hour: minute	Defines a time of day to begin

Property	Value	Description
		reporting alarms.
End Time	hour: minute	Defines the time of day to stop reporting alarms.
Days of Week	check boxes	Defines the days of the week for which to apply the start and end times.
Schedule	Ref Chooser	Instead of using start and end times during days of the week, defines the alarms to include based on an existing schedule.

Access History Report and Summary window

This report lists each person who accessed the building.

Figure 71. Access History report and Summary window



You view this report by clicking **Reports > Access History**. You access the Summary window by selecting a row

in the table and clicking the Summary button ( ).

Control buttons

In addition to the standard control buttons (Auto Refresh, Column Chooser, Filter, Refresh, Manage Reports and Export), this report includes these control buttons:

- 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.

-  Purge Config opens the **Purge Config** window for setting up when and how to remove history records from the database.

Columns

**Table 20.** Access History report columns and Summary window properties

Column/Property	Description
Timestamp	Reports when the record was written to the database.
Granted	Reports if access was granted (true) or denied (false).
Reader	Reports the name of the reader associated with the access right.
Badge	If the alarm was triggered by an access control violation, identifies the responsible badge.
Owner	Identifies the person who accessed the building.
Activity	Reports what the person was doing: entering or exiting.
Details	Provides additional information.
Person Id	Identifies the <b>Employee Id</b> of the person who accessed the building.

Purge Config window (simple)

This window provides properties for setting the maximum number and means for handling history records (capacity). You must be logged in as a user with the appropriate write permissions for the Purge Config button

 (  ) to display in the toolbar.

**NOTE:** Once history records have been purged, they cannot be retrieved unless they were previously backed up.

**Figure 72.** Purge Config window in a remote controller station



This window opens in a remote controller station when you click **Reports**, click one of the history reports, and


click the Purge Config button (  ).

**NOTE:** The exact properties differ, depending on the type of history view associated with the **Purge Config** window.

Property	Value	Description
Capacity	number	Defines the maximum number of history records allowed in the





the Purge Config button ().

This purge window presents in a Supervisor station for the following reports: Access History, Alarm History, Intrusion History, Audit History, and Log History.

Property	Value	Description
Data Expiration	date and time (default: 1 year, that is: 08760 hours)	Specifies when data may be deleted from the database. This means that data that are older than 365 days are eligible for purging from the database using the Auto Purge or Manual purge settings.
Auto Purge	Additional options	Schedule record purge jobs according to a daily or interval schedule.
Manual	date and time	Provides an alternative to <b>Auto Purge</b> , that allows you to set a specific day and time to purge expired data.

Access History Filter window

This window defines the search criteria for limiting the records that appear in the Access History view.

**Figure 74.** Access History Filter window

Filter

☒ **Timestamp**

Today ▾ >>

☐ **Granted**

false ▾

☐ **Reader**

%

Must Include ▾

☒ Case Sensitive

☐ **Badge**

%

Must Include ▾

☒ Case Sensitive

☐ **Owner**

%

Must Include ▾

☒ Case Sensitive

☐ **Activity**

☐ **Details**

%

Must Include ▾

☒ Case Sensitive

Ok

Cancel

This window opens when you click **Reports > Access History**, followed by clicking the Filter button ().

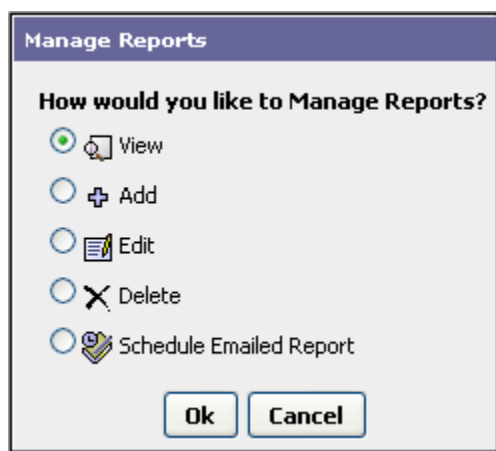
Criterion	Value	Description
Timestamp	drop-down list	Selects a period of time for displaying access history. To further

Criterion	Value	Description
		filter report records based on this timestamp, refer to a topic titled "Advanced Time Range Options window."
Granted	read-only	Selects for display only access records generated by granted requests (true) or rejected requests (false).
Reader	wild card (%)	Selects access records processed by a specific reader.
Badge	wild card (%)	Selects access records generated by a specific badge.
Owner	wild card (%)	Selects access records generated when a specific person entered.
Activity	Enum chooser	Selects access records generated by a specific event. The list of events is long, including activities, such as Invalid PIN, Occupancy Violation, Manual Override, etc.
Details	wild card (%)	Selects access records based on alarm details.

## Manage Reports window

This window works with pre-configured reports and any custom reports that you may create. You can view, add, edit, delete and email reports.

**Figure 75.** Manage Reports window (custom reports)



This window opens when you click the Manage Reports button (  ) at the top of a view. This button

appears as a standard button on may views where it provides options to view, add, edit, delete and email reports.

This window is context sensitive. It only provides options that apply to the type of data currently displaying. For example, if you are viewing the Audit History report, only Audit History records are available for viewing, adding, editing, or emailing.

The only options available for managing pre-configured reports are: `Add` (create a custom report) and `Schedule Emailed Report` (set up the pre-configured report to be emailed).

Selecting the `View`, `Edit`, and `Delete` options open a window that lists the custom reports. You choose the report to view, edit, or delete from this list.

**NOTE:** You cannot delete the pre-configured reports.

Add (or edit) Report window

This window sets up custom reports.

Figure 76. Add/Edit Report window

Add Report

Name

Navigation Path

None

Icon

Index

0

Ok

Cancel

This window opens when you click the Manage Reports button (  ) followed by clicking the `Add` option.

Property	Value	Description
Name	text	Defines a unique name for the report.
Navigation Path	hierarchy (defaults to None)	Selects where in the station hierarchy to store the new report. The default allows access to the report from the <code>Manage Reports</code> window even though the report does not appear in the menu hierarchy.
Icon	URL	Defines an icon to associate with the report.
Index	integer	Determines where the report appears (left to right) in the navigation path.

Schedule Emailed Report window

This window configures visual and email properties.

**Figure 77.** Schedule Emailed Report window

Schedule Emailed Report: LogHistory

Title

logHistory

File Type

PDF

Include Headers

true

Include BOM

true

Use CRLF Line Endings

LF (\n)

Delimiter

,

Username

admin

Export Schedule

None

Email Account

None

From:

To:

Cc:

Bcc:

Subject:

Email

Ok

Cancel

This window opens when you click the Manage Reports button (  ) followed by clicking the Schedule Emailed Report option.

Property	Value	Description
Title	text	Creates a title for the email.
File Type	drop-down list (defaults to PDF)	PDF creates a PDF file.CSV creates a comma delimited file.
Include Headers	true (default) or false	Configures the inclusion of report headings.
Include BOM	true (default) or false	
Use CRLF Line Endings	drop-down list	Configures how to terminate each line of the report: LF = line feed, CRLF = carriage return, line feed.
Deliminitor	character (defaults to comma (,))	Defines the character used to

Property	Value	Description
		separate individual fields of information.
Username	read-only	Identifies the current user.
Export Schedule	Ref Chooser	Opens a list of schedules from which to choose an email schedule.
Email Account	Additional properties	Defines the From, To, cc, Bcc and Subject for the email.
Email	text	Provides the body of the email. This might include instructions or other information.

## Alarm History report

This report contains a table of time-stamped alarm records that include a listing of activities, such as alarm acknowledgments, alarm descriptions, as well as associated sources, credential numbers, and owner names.

**Figure 78.** Alarm History report





Alarm Time	Normal Time	Source Name	Alarm Class	Source State	Ack State	Priority	Message
08-Sep-18 10:00 AM IST	08-Sep-18 10:01 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex
08-Sep-18 9:59 AM IST	08-Sep-18 10:00 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex
08-Sep-18 9:58 AM IST	08-Sep-18 9:59 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex
08-Sep-18 9:57 AM IST	08-Sep-18 9:58 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex
08-Sep-18 9:56 AM IST	08-Sep-18 9:57 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex
08-Sep-18 9:55 AM IST	08-Sep-18 9:56 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex
08-Sep-18 9:54 AM IST	08-Sep-18 9:55 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex
08-Sep-18 9:53 AM IST	08-Sep-18 9:54 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex
08-Sep-18 9:52 AM IST	08-Sep-18 9:53 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Tex


This report opens when you click **Reports > Alarm History**.

### Control buttons

In addition to the standard control buttons (Auto Refresh, Column Chooser, Filter, Manage Reports and Export), this report includes these control buttons:

-  Show Alarm Details opens the Alarm Details window, which provides additional information about the selected alarm.  
This button is available on the Alarm History view.
-  Purge Config opens the Purge Config window for setting up when and how to remove history records from the database.



- Review Video plays back a video associated with an alarm. The alarm video icon (  ) next to the alarm identifies alarms with associated videos.

## Columns

**Table 21.** Alarm History Report columns

Column	Description
Alarm Time	Reports when the alarm condition occurred.
Normal Time	When displayed, shows a null value until the point returns to a normal state, then it displays the time that the point status returned to normal.
Source Name	Reports the component that transitioned from normal to offnormal, fault, or alert. If defining search criteria, you can use wild cards here.
Alarm Class	Reports the <code>Display Name</code> of the alarm class associated with the point, recipient or other component.
Source State	Reports the component state transition: <ul style="list-style-type: none"> <li>Offnormal (normal to offnormal)</li> <li>Alert (normal to alert)</li> <li>Fault (normal to fault)</li> <li>Normal (offnormal, alert, or fault to normal)</li> </ul>
Ack State	Reports the state of the alarm (unacknowledged, acknowledged).
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to <code>Offnormal</code> , from normal to <code>Fault</code> , from offnormal, fault or alert to <code>Normal</code> , and from normal to <code>Alert</code> ). The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1. The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Message	Describes how to handle an alarm.
Badge	If the alarm was triggered by an access control violation, identifies the responsible badge.
User	If the alarm was triggered by an access control violation, identifies the person associated with the badge. If the alarm was generated by malfunctioning equipment, identifies the system user, if known.

## Alarm history Summary window

This window displays detailed information for a single alarm history row.

Figure 79. Alarm History Summary window

Alarm Details

Timestamp

16-Aug-17 8:22:58 AM EDT

Uuid

11e7827d-a360-f2de-0000-00000000901d

Source State

Alert

Ack State

Unacked

Ack Required

false

Source

local:|station:|slot:/Drivers/AccessNetwork/R2R\$20Module09\$20\$2d\$20Dr\$2e\$20\$234\$20\$26\$205/points/Door\$204\$20\$2d\$20ICE\$20South\$20Shop\$20Entry\$20Door\$20Haulers/Reader4\$20\$2d\$20South\$20ICE\$20Shop\$20Entry\$20Haulers\$20PIN\$2fReader/grantedButNotUsedAlert;slot:/Drivers/NiagaraNetwork/WebsEntSec601/alarms

Alarm Class

defaultAlarmClass

Priority

150

Normal Time

null

Ack Time

null

User

Hiquet, Kent

TimeZone

America/Indianapolis (-5/-4)

badge

32156 [30] - 2017 ICE Keyfob


escalated

Alarm Data

msgText

Granted But Not Used

person

 Hiquet, Kent

sourceName

WebsEntSec601:R2R Module09 - Dr. #4 & 5.Reader4 - South ICE Shop Entry Haulers PIN/Reader

Alarm Transition

Alert

Last Update

16-Aug-17 8:22 AM EDT

Ok


You access this window from the main menu by clicking **Reports > Alarm History**, followed by selecting an alarm history record and clicking the Summary button ().

Table 22. Alarm Details properties

Property	Description
Timestamp	Reports when the record was written to the database.
Uuid	Reports the Universally Unique Identifier.
Source State	Reports the component state transition: <ul style="list-style-type: none"><li>• Offnormal (normal to offnormal)</li><li>• Alert (normal to alert)</li><li>• Fault (normal to fault)</li><li>• Normal (offnormal, alert, or fault to normal)</li></ul>
Ack State	Reports the state of the alarm (unacknowledged, acknowledged).
Ack Required	Indicates if the alarm must be acknowledged ( <code>true</code> ) or not ( <code>false</code> ).
Source	Reports the ORD that created the alarm.



Property	Description
Alarm Class	Reports the routing information for the alarm.
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to <code>Offnormal</code> , from normal to <code>Fault</code> , from <code>offnormal</code> , <code>fault</code> or <code>alert</code> to <code>Normal</code> , and from normal to <code>Alert</code> ). The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1. The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Normal Time	When displayed, shows a null value until the point returns to a normal state, then it displays the time that the point status returned to normal.
Ack Time	Displays the time that the alarm was acknowledged (if applicable).
User	Reports several pieces of information about the system user who was logged in when the system generated the alarm, including: name, timezone, badge number and if the alarm has been referred up the management hierarchy (escalated).
Alarm Data	Reports additional information about the alarm, including any message text configured for the alarm, the user, and abbreviated information about the component that generated the alarm.
Alarm Transition	Shows the initial source state that caused the alarm to be generated. The Alarm Transition may not be the current state of the alarm source. Once an Alarm Transition is created, it does not change for a single alarm record. For example, if the source state returned to "Normal" after an "Offnormal" status, this value remains at "Offnormal".
Last Update	Displays the time the system most recently updated the alarm.

## Review Video view

This view plays back the video associated with an alarm.

This opens from the main menu when you click **Reports > Alarm History**, followed by selecting an alarm history

record and clicking the Review Video button ()

## Alarm history Filter window

This filter provides a variety of ways to limit the number of alarms shown in the alarm history view.

**Figure 80.** Alarm History Filter window

Filter

☒ Alarm Time

Today

>>

☐ Normal Time

Time Range

? to ?

>>

☐ Source Name

%

Must Include

☒ Case Sensitive

☐ Alarm Class

%

Must Include

☒ Case Sensitive

☐ Source State

☐ Ack State

☐ Priority

☐ min

0

☐ max

0

☐ Message

%

Must Include

☒ Case Sensitive

☐ Badge

%

Must Include

☒ Case Sensitive

☐ User

%

Must Include

☒ Case Sensitive

Ok

Cancel

This window opens from the main menu when you click **Reports > Alarm History**, followed by selecting an alarm history record and clicking the Filter button ()

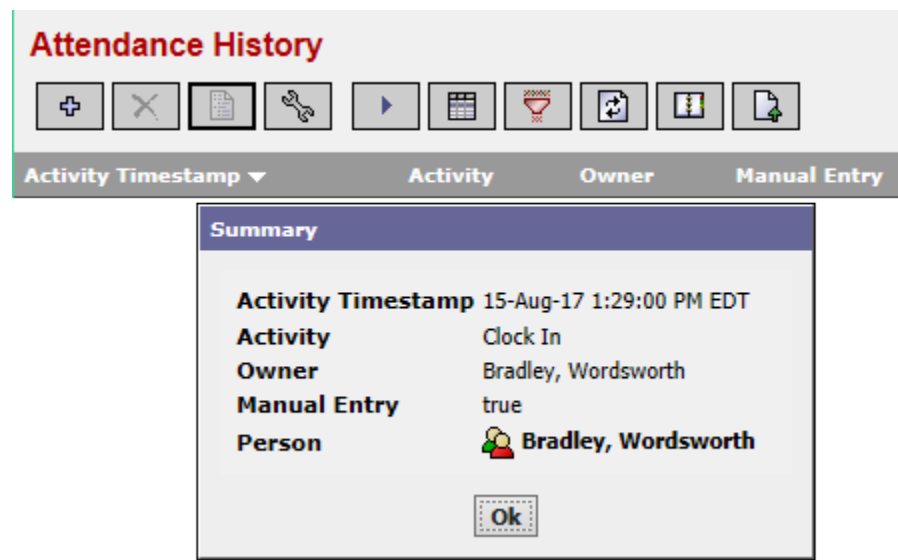
Criterion	Value	Description
Alarm Time	drop-down list	Selects the period of time to include in the report. To further filter report records based on alarm time, refer to a topic titled "Advanced Time Range Options window."
Normal Time	drop-down list and Ref Chooser	Selects a time range for reporting alarms that returned to normal. To further filter report records based on normal time, refer to a topic titled "Advanced Time Range Options window."
Source Name	wild card (%)	Selects alarms to include based on the component ORD.
Alarm Class	wild card (%)	Selects alarms based on alarm class. Alarm class defines alarm routing.
Source State	Enum chooser	Selects an alarm state: Normal, Offnormal, Fault and Alert.
Ack State	Enum chooser	Selects the state of the acknowledgment: Acked


Criterion	Value	Description
		(acknowledged), Unacked (unacknowledged) and Act Pending (about to be acknowledged).
Priority	number	Selects alarms to display based their priority from 1 to 150, where 1 is the highest priority.
Message	wild card (%)	Selects alarms to display based on the message associated with the alarm.
Badge	wild card (%)	Selects alarms to display based on the badge number of a person.
User	wild card (%)	Selects alarms to display based on the user who was logged in when the system generated the alarm.

Attendance History Report and Summary window

This report lists badge transactions marked with the date and times that badge holders arrived and left. These data are used to calculate time worked.





Figure 81. Attendance History report and Summary window



You access this report by clicking **Reports > Attendance History**. You access the Summary window by selecting an attendance history record and clicking the Summary button (  )

Control buttons

In addition to the standard control buttons (Auto Refresh, Column Chooser, Filter, Manage Reports and Export), this report includes these control buttons:

-  Manual Add opens the Manual Add window with which to create an attendance record. You would need to do this if the person failed to scan their badge in and out.
-  Manual Hide opens the Manual Hide confirmation window for permanently hiding (not deleting) an attendance record. The Window warns that hiding the selected record is not reversible and only affects entries that have been created using the Manual Add window.
-  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.
-  Purge Config opens the Purge Config window for setting up when and how to remove history records from the database.

Columns and properties

Table 23. Attendance History columns and Summary window properties

Column/Property	Description
Activity Timestamp	Reports when the record was written to the database.
Activity	Reports the nature of the attendance event: None, Clock In or Clock Out.
Owner	Reports the person’s name.
Manual Entry	Reports true if a manual entry was used to clock in or out, or false if the person clocked in and out with a badge.

Manual Add (attendance record) window

The Manual Entry function allows you to enter attendance data into the Attendance History report if, for example a badge was not used on entry. Clicking the **Insert** button opens the **Manual Add** window.

Figure 82. Manual Add window

Manual Add


Activity Timestamp


18 Feb 2009 05:13 PM EST

Activity

Clock In

Owner

 Fick, Don

>> 

Ok

Cancel

To open this window click **Reports > Attendance History** followed by clicking the Add button ().

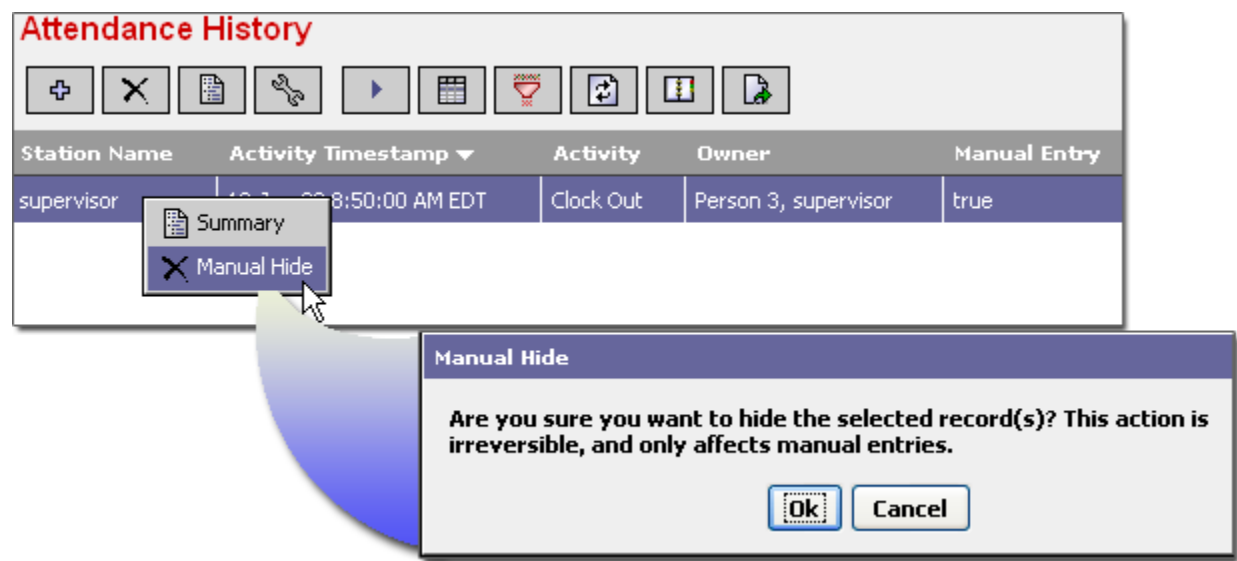
Property	Value	Description
Activity Timestamp	date and time (defaults to the	Defines the time the person entered

Property	Value	Description
	current time)	or left the building.
Activity	drop-down list	Clock In identifies an entry time. Clock Out identifies an exit time. None defines an activity other than clocking in or clocking out.
Owner	Ref Chooser	Identifies the person for whom you are adding the attendance record.

Manual Hide (confirmation) window

This window warns that hiding the selected record is not reversible and only affects records created using the Manual Add window.

Figure 83. Manual Hide confirmation window (opened using the right-click menu



Attendance History Filter window

This window defines search criteria for limiting the number of attendance history records that appear in the view.

**Figure 84.** Attendance History Filter window

Filter

☒ Activity Timestamp

Today ▾ >>

☐ Activity

☐ Owner

% ▾ Must Include ▾ ☒ Case Sensitive

☐ Manual Entry

false ▾

Ok

Cancel

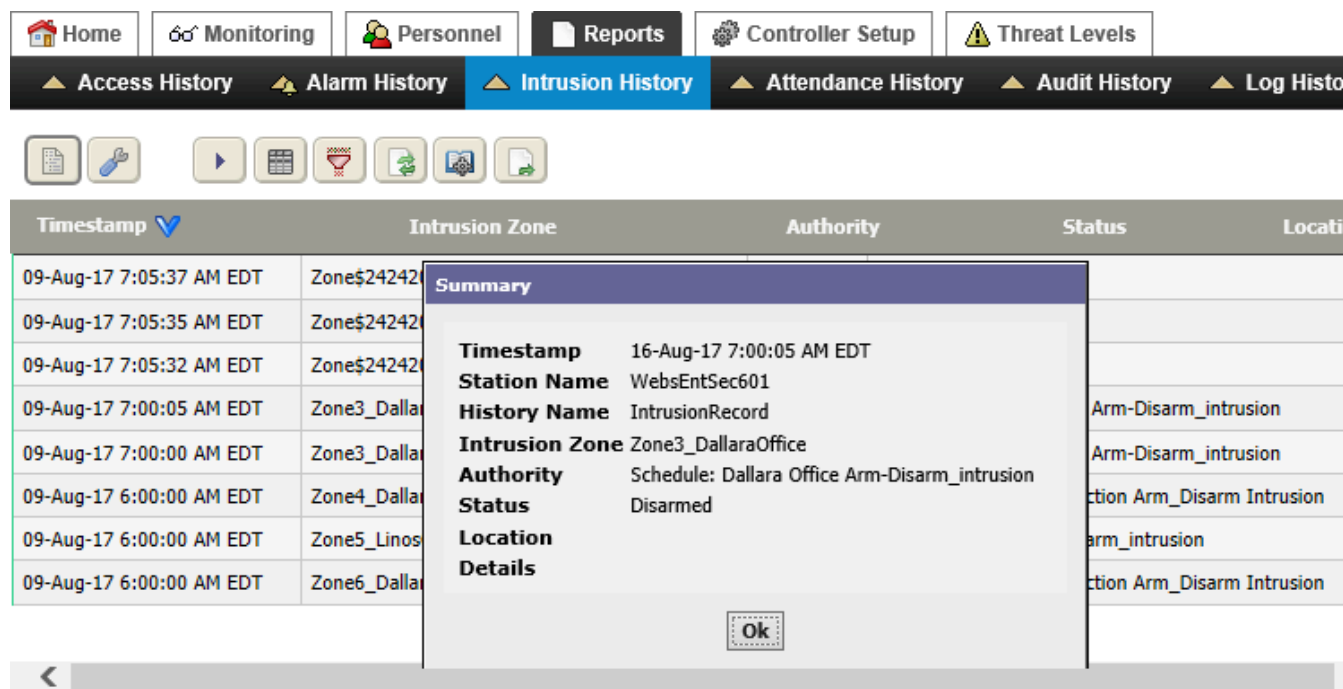
You access this window from the main menu by clicking **Reports > Attendance History**, followed by selecting an alarm history record and clicking the Filter button ()

Criterion	Value	Description
Activity Timestamp	drop-down list and Advanced Time Range Options window	Selects a time range for reporting an attendance event. To further filter report records based on this activity ytimestamp, refer to a topic titled "Advanced Time Range Options window."
Activity	Enum selector	Selects the nature of the event: None, Clock In, or Clock Out.
Owner	wild card (%)	Selects attendance history data for a specific person.
Manual Entry	true or false (default)	Selects attendance history data that was created by the system (false) or manually entered (true).

### Intrusion History report and Summary window

This history report contains timestamped data specifically related to the arming and disarming of intrusion zones. Each time an intrusion zone is armed or disarmed, several properties are recorded, including time, authorization (PIN, Person), and changed status.



Figure 85. Intrusion History report and Summary window



This report opens when you click **Reports > Intrusion History**. The **Summary** window opens when you select a row in the table and click the Summary button (  ).

Control buttons

In addition to the standard control buttons (Auto Refresh, Column Chooser, Filter, Manage Reports and Export), this report includes these control buttons:

-  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.
-  Purge Config opens the **Purge Config** window for setting up when and how to remove history records from the database.

Columns

Table 24. Intrusion Zone Report columns and Summary window properties

Column	Description
Timestamp	Reports when the record was written to the database.
Station Name	Reports the name of the station under the control of which the event occurred.
Intrusion Zone	Reports the name of the intrusion zone.
Authority	Reports which schedule is mapped to the intrusion zone.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.

Column	Description
Location	Reports where the event occurred.
Details	Reports additional information.

Intrusion History Filter window

This window defines search criteria for limiting the number of records that appear in the history report.

Figure 86. Intrusion History Filter window

Filter

☒ Timestamp

Today

>>

☐ Intrusion Zone

%

Must Include

☒ Case Sensitive

☐ Authority

%

Must Include

☒ Case Sensitive

☐ Status

☐ Location

%

Must Include

☒ Case Sensitive

☐ Details

%

Must Include

☒ Case Sensitive

Ok

Cancel

This window opens from the main menu when you click **Reports > Intrusion History**, followed by selecting an

alarm history record and clicking the Filter button (  )

Criterion	Value	Description
Timestamp	drop-down list	Selects a time range for reporting an intrusion event. To further filter report records based on this timestamp, refer to a topic titled "Advanced Time Range Options window."
Intrusion Zone	wild card (%)	Selects records based on the intrusion zone name.
Authority	wild card (%)	Reports which schedule is mapped to the intrusion zone.
Status	Enums chooser	Selects records based on the status of the zone:  <div>Arming selects event records that occurred when the zone was in the process of arming.</div> <div>Armed selects event records</div>



Criterion	Value	Description
	<div><div>Enums</div><div><div>Arming</div><div>Armed</div><div>Disarmed</div><div>Allowing Time For Disarm</div><div>Unable To Arm</div></div><div><div>Ok</div><div>Cancel</div></div></div>	<p>that occurred when the zone was armed.</p> <p>Disarmed selects event records that occurred when the zone was not armed.</p> <p>Allowing Time For Disarm selects event records that occurred when the zone was waiting to receive the code to disarm.</p> <p>Unable to Arm selects event records that occurred when the door was open or some other condition was preventing the zone from arming.</p>
Location	wild card (%)	Selects based on location.
Details	wild card (%)	Selects records based on an intrusion-related message.

### Audit History Report and Summary window

This report contains a record for each operation that occurs in the system. Available on the Supervisor station, this report provides a log of all system operator actions.

**Figure 87.** Audit History report and Summary window

Page 1 of 1

Timestamp	Station Name	Operation	Target	Slot Name	Old Value	Value
08-Sep-18 9:51:05 AM IST	entSecurity801	Invoked	/Services/AlarmService/Intrusion\$20Zone1	changeUuid		6682b1f1-9dfe-4be3-bed1-feb5beb3c901
08-Sep-18 9:50:31 AM IST	entSecurity801	Added	/Services/AlarmService	Intrusion\$20Zone1		Intrusion Zone1
08-Sep-18 9:49:30 AM IST	entSecurity801	Added	/Drivers/SmartKey\$20Network	SmartKey\$20Device		SmartKey Device
08-Sep-18 9:48:08 AM IST	entSecurity	Logout (Timeout)	/Services/WebService	172.21.139.79		
08-Sep-18 9:47:31 AM IST	entSecurity801	Changed	/Drivers/SmartKey\$20Network/communicator	portName	COM3	COM1
08-Sep-18 9:46:19 AM IST	entSecurity801	Added	/Drivers	SmartKey\$20Network		SmartKey Network
08-Sep-18 9:43:20 AM IST	entSecurity801	Changed	/Drivers/AccessNetwork/Remote\$20Reader\$20Module2/points/Door\$202/Reader\$202/grantedButNotUsedAlert			
08-Sep-18 9:43:20 AM IST	entSecurity801	Changed	/Drivers/AccessNetwork/Remote\$20Reader\$20Module2/points/Door\$202/Reader\$202/grantedButNotUsedAlert			
08-Sep-18 9:43:10 AM IST	entSecurity801	Changed	/Drivers/AccessNetwork/Remote\$20Reader\$20Module2/points/Door\$202/Reader\$202/grantedButNotUsedAlert			
08-Sep-18 9:43:10 AM IST	entSecurity801	Changed	/Drivers/AccessNetwork/Remote\$20Reader\$20Module2/points/Door\$202/Reader\$202/grantedButNotUsedAlert			
08-Sep-18 9:42:47 AM IST	entSecurity801	Changed	/Drivers/AccessNetwork/Remote\$20Reader\$20Module2/points/Door\$202/Reader\$202/grantedButNotUsedAlert			

Summary

Timestamp

08-Sep-18 9:43:20 AM IST

Station Name

entSecurity801

History Name

AuditHistory

Operation

Changed

Target

/Drivers/AccessNetwork/Remote\$20Reader\$20Module2/points/Door\$202/Reader\$202/grantedButNotUsedAlert

Slot Name

enableLogging

Old Value

true


Value

false

User Name



admin

Ok

This report opens when you click **Reports > Audit History**. You access the Summary window by selecting an audit history record and clicking the Summary button (  )

Buttons

In addition to the standard control buttons (Auto Refresh, Column Chooser, Filter, Manage Reports and Export), this report includes these control buttons:

-  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.
-  Purge Config opens the **Purge Config** window for setting up when and how to remove history records from the database.

Columns

**Table 25.** Audit History report columns and Summary window properties

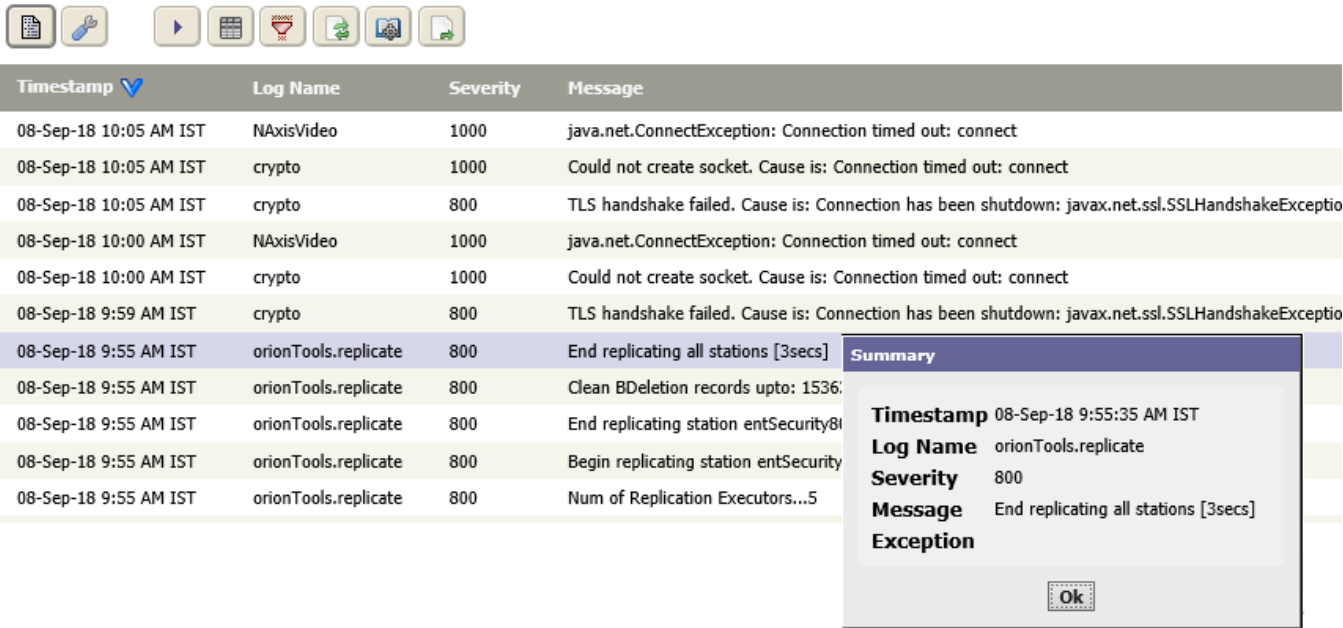
Column/Property	Description
Timestamp	Reports when the record was written to the database.
Station Name	Reports the name of the station under the control of which the event occurred.
Operation	Reports a single word to explain the activity: Changed, Invoked, Login, Logout, Removed.
Target	Reports the service to which the history belongs.
Slot Name	Reports the slot path of the component in the station.
Old Value	Reports the previous configuration before this history record was created.
Value	Reports the current configuration value of the component.
User Name	Reports the user name of the logged-in user.

## Log History Report and Summary window


This report maintains a buffered history (LogHistory) of some of the messages that are generated by the system’s standard output. These messages can be very helpful for troubleshooting problems at the system level. You can select the Log History report to check the log history for recent messages.

**NOTE:** The Log History report you view from a Supervisor station are local to the Supervisor. The Log History report does not show the records of the subordinate stations. You have to go to each individual subordinate station to view its log records.

**Figure 88.** Log History report and Summary window





This view opens when you click **Reports > Log History**. You access this window from the main menu by clicking

**Reports > Log History**, followed by selecting an alarm history record and clicking the Summary button (  ).

### Buttons

In addition to the standard control buttons (Auto Refresh, Column Chooser, Filter, Manage Reports and Export), this report includes these control buttons:

-  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.
-  Purge Config opens the **Purge Config** window for setting up when and how to remove history records from the database.

Columns

**Table 26.** Log History columns and Summary window properties

Column/Property	Description
Timestamp	Reports when the record was written to the database.
Log Name	Name of the log file.
Severity	Reports the significance of the event. A value of 1000 is severe. A value of 800 is a warning. A value of 600 provides information.
Message	Describes how to handle an alarm.
Exception	Reports the exception stack trace if Severity equals 1000.

Log history Filter window

This window specifies search criteria for limiting the number of records that display in the table.

**Figure 89.** Log History Filter window

Filter

☒ **Timestamp**

Today

 >>

☐ **Log Name**

%

Must Include

☒ Case Sensitive

☐ **Severity**

☐ min 

0

☐ max 

0

☐ **Message**

%

Must Include

☒ Case Sensitive

☐ **Exception**


%

Must Include

☒ Case Sensitive

Ok

Cancel

This window opens from the main menu when you click **Reports > Log History**, followed by selecting an alarm history record and clicking the Filter button (  ).




Criterion	Value	Description
Timestamp	Drop-down list and Advanced Time Range Options window	Selects a time range for reporting a log event. To further filter report records based on this timestamp, refer to a topic titled "Advanced Time Range Options window."
Log Name	wild card (%)	Selects the log name that contains the records to display.
Severity	min and max numbers	Reports the significance of the event. A value of 1000 is severe. A value of 800 is a warning. A value of 600 provides information.
Message	wild card (%)	Selects records to display based on an associated message.

Criterion	Value	Description
Exception	wild card (%)	Selects based on the exception stack trace, which is available if <b>Severity</b> equals 1000.

Hardware reports

Hardware reports provide information about devices, such as modules, doors, readers, and elevators. They also may also include input and output points on system modules and building automation system points (BACnet points). Each hardware report contains a list of these types of items.







Each hardware report provides the same set of control buttons. In addition to the standard control buttons (Auto Refresh, Column Chooser, Manage Reports and Export), these control buttons provide varying results:

-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.  
These views are documented in the chapter titled "Controller Setup - Remote Devices."
-   Filter buttons open the Filters window, which defines a query action for limiting the output visible in tables and reports. The gray version indicates unfiltered data. The red version indicates filtered data.

Doors Report and Filter window

This report lists the doors in the system, provides information about them, and reports their status.

Figure 90. Doors report and Filter window



Station Name	Description	Module	Door Status
entSecurity801	Door 1	Remote Reader Module	{fault,alarm,unackedAlarm} Locked Closed
entSecurity801	Door 2	Remote Reader Module	{fault,alarm,unackedAlarm} Locked Closed
entSecurity801	Door 1		
entSecurity801	Door 2		
entSecurity801	Door 1		
entSecurity801	Door 2		

Filter

☐ Station Name

%

Must Include

☒ Case Sensitive

☐ Description

%

Must Include

☒ Case Sensitive

☐ Module

%

Must Include

☒ Case Sensitive

☐ Door Status

%

Must Include

☒ Case Sensitive

Ok

Cancel

This report opens when you click **Reports > Hardware > Doors**. The Filter window opens when you click the

Filter button ().








Table 27. Doors report columns and search criteria

Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the door.
Module	Displays data, and selects data to view based on the controller module that controls the door.
Door Status	Displays data, and selects data to view based on door status: Locked Closed, Unlocked Closed, etc.

Readers Report and Filter window

This report lists the readers in the system, provides information about them, and reports their status.

Figure 91. Readers report and Filter window



Station Name	Description	Assignment	Module
entSecurity801	Reader 1	Door 1	Remote Reader Module
entSecurity801	Reader 2	Door 2	Remote Reader Module
entSecurity801	Reader 1	Door 1	Remote Reader Module1
entSecurity801			Remote Reader Module1
entSecurity801			Remote Reader Module2
entSecurity801			Remote Reader Module2

Filter

☐ Station Name

%

Must Include

☒ Case Sensitive

☐ Description

%

Must Include

☒ Case Sensitive

☐ Assignment

%

Must Include

☒ Case Sensitive

☐ Module

%

Must Include

☒ Case Sensitive

☐ Function

Must Include

☒ Case Sensitive

Ok

Cancel


This report opens when you click **Reports > Hardware > Readers**. The **Filter** window opens when you click the Filter button ().

Table 28. Readers report columns and search criteria







Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the reader.
Assignment	Displays data, and selects data to view based on the door to which the reader is assigned.
Module	Displays data, and selects data to view based on the controller module associated with the reader.
Function	Displays data, and selects data to view based on the job that this reader performs. The filter, opens an Enum chooser with these self-explanatory functions:  Reader Only  Reader Plus Keypad  Reader Or Keypad

Column/criterion	Description
	Reader Or Intrusion Keypad
	Intrusion Keypad

Inputs Report and Filter window

This report lists the inputs identified when the system discovers each parent device or module and adds it to the network. Inputs include door sensors, exit requests, ADA control, glass break sensors, and motion sensors.

Figure 92. Inputs report and Filter window



Station Name	Description	Termination	Module	Status
entSecurity801	Di1	1	Remote Reader Module	inactive {ok}
entSecurity801	Di2	2	Remote Reader Module	inactive {ok}
entSecurity801	Exit Request	2	Remote Reader Module	Inactive {fault,alarm,unackedAlarm} CUT
entSecurity801	Sensor	1	Remote Reader Module	Closed {fault,alarm,unackedAlarm} CUT
entSecurity801	Exit Request	4	Remote Reader Module	Inactive {fault,alarm,unackedAlarm} CUT
entSecurity801	Sensor	3		Inactive {fault,alarm,unackedAlarm} CUT
entSecurity801	Di1	1		
entSecurity801	Di2	2		
entSecurity801	Exit Request	2		
entSecurity801	Sensor	1		

Filter

☐ Station Name

%

Must Include

☒ Case Sensitive

☐ Description

%

Must Include

☒ Case Sensitive

☐ Termination

min 0

max 0

☐ Module

%

Must Include

☒ Case Sensitive

☐ Status

%

Must Include

☒ Case Sensitive

☐ Proxy Ext


%

Must Include

☒ Case Sensitive

☐ Facets

No facets



Ok

Cancel

This report opens when you click **Reports > Hardware > Inputs**. The **Filter** window opens when you click the

Filter button ().

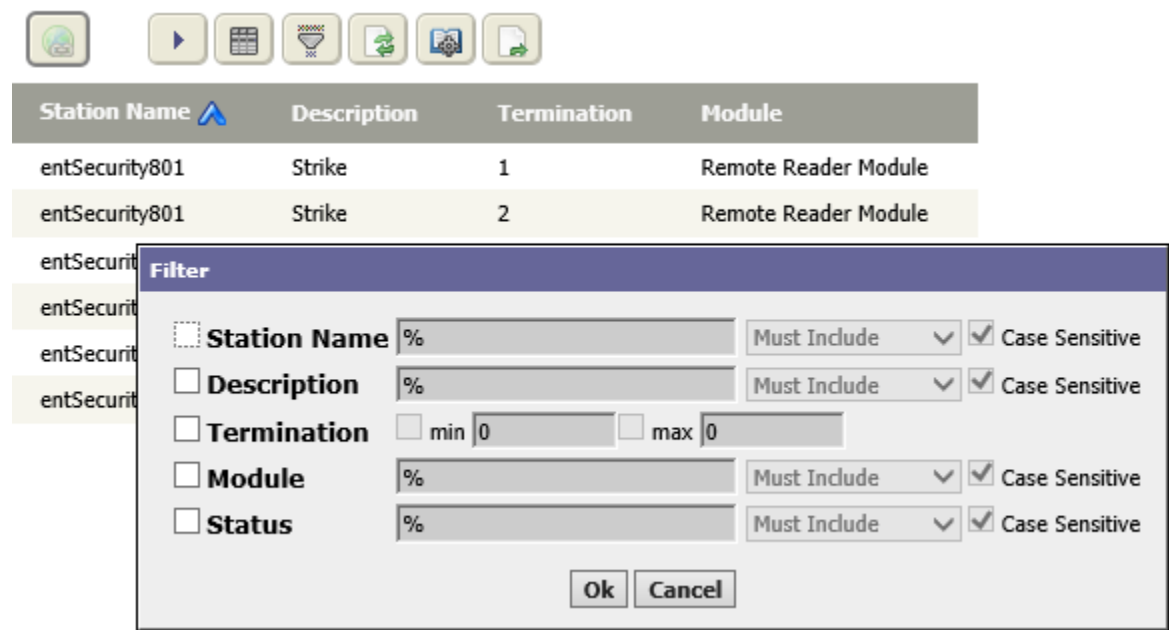
Table 29. Inputs report columns and search criteria

Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the input.
Termination	Displays data and selects data to view based on the numbered terminal point that the input is assigned to. This may be especially helpful when the display name (shown in the Description column) is renamed.
Module	Displays data, and selects data to view based on the controller module associated with the input.
Status	Displays data and selects data to view based on the input status: inactive/Inactive, Closed, Opened, Locked, Off, etc.

### Outputs report and Filter window

This report lists the outputs identified when the system discovers each parent device or module and adds it to the system network. Outputs include strikes, relays, alarms, lights on/off, heater on/off, and air conditioner on/off.

**Figure 93.** Outputs report



This report opens when you click **Reports > Hardware > Outputs**.

**Table 30.** Outputs report columns

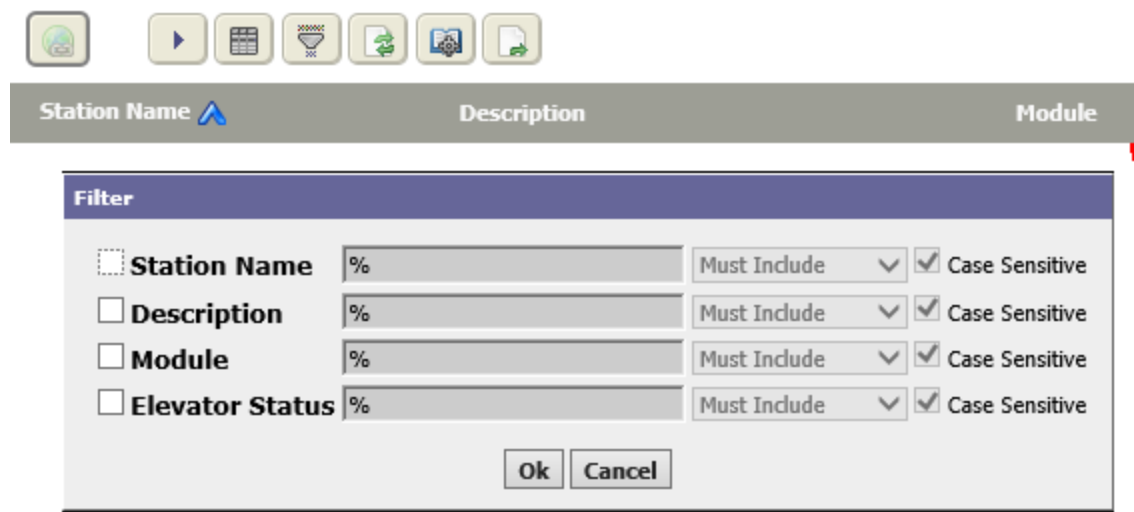
Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the output.
Termination	Displays data and selects data to view based on the numbered terminal point that the output is assigned to. This may be especially helpful when the display name (shown in the Description column) is renamed.
Module	Displays data, and selects data to view based on the controller module associated with the output.
Status	Displays data and selects data to view based on output status: : inactive/Inactive, Closed, Opened, Locked, Off, etc.


### Elevators Report and Filter window

Elevators are devices that are assigned to modules. The Elevator report lists all elevators that are assigned under a station.



**Figure 94.** Elevators report and Filter window



This report opens when you click **Reports > Hardware > Elevators**. The **Filter** window opens when you click the Filter button ().

**Table 31.** Elevators report columns and search criteria

Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the elevator.
Module	Displays data, and selects data to view based on the controller module associated with the elevator.
Elevator Status	Displays data, and selects data to view based on the elevator status.

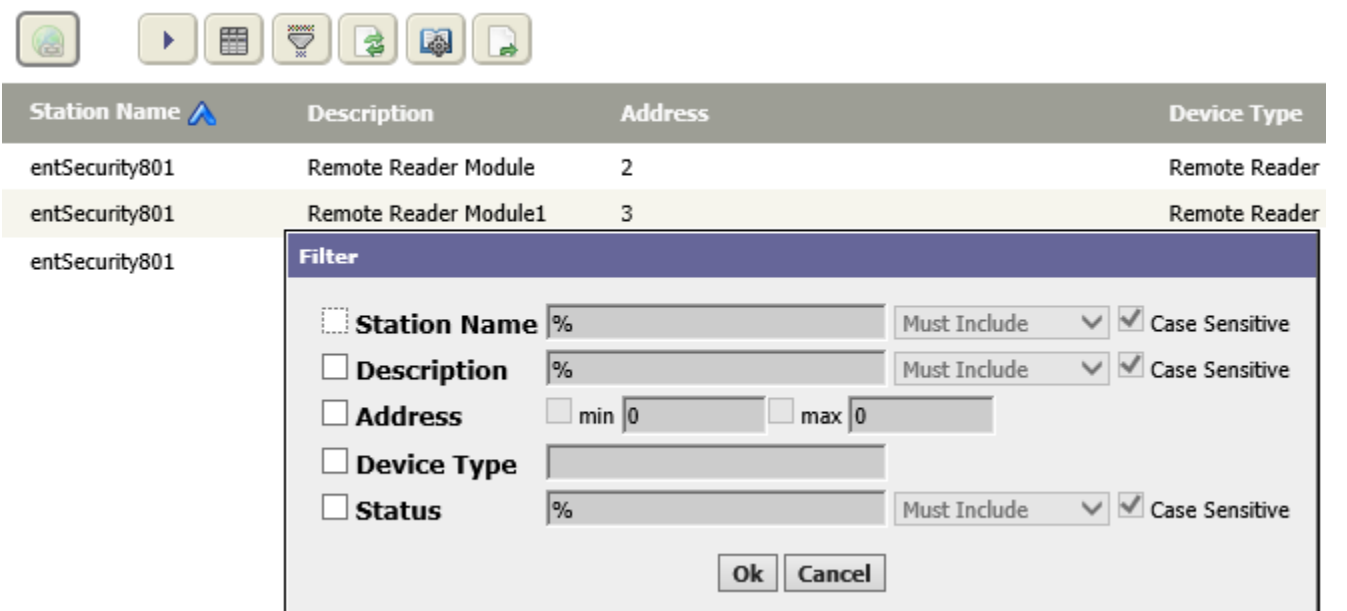
### Remote Modules Report and Filter window

Modules are the core hardware components that attach to the controller unit. The Modules report lists all modules that are in a station Access Device Manager Database.

NOTE:

A Modules report from a Supervisor station shows the modules that are under all subordinate stations.

Figure 95. Modules report and Filter window




This report opens when you click **Reports > Hardware > Remote Modules**. The **Filter** window opens when you click the **Filter** button (  ).

Table 32. Remote Modules report columns and search criteria







Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the module.
Address	Displays data, and selects data to view based on the random integer value assigned to the reader. Each reader has a different integer, which may start from one (1).
Device Type	Displays data, and selects data to view based on the type of module. The Filter window opens an Enum chooser with these self-explanatory device types:  None  Base Board Reader  Remote Reader  Remote Input Output  Io16  Io16V1



Column/criterion	Description
	lo34
	lo34sec
Status	Displays data, and selects data to view based on the condition of the remote module: {ok}, {unackedAlarm}, {fault}, etc.

BACnet Points and Filter window

This report lists all BACnet points in the system database.

Figure 96. BACnet Points report and Filter window



Page  of 4Page Size

Station Name	Description	BACnet Object Id	Status
entSecurity801	Remote Reader Module.Di1	binaryValue:0	{ok}
entSecurity801	Remote Reader Module.Di2	binaryValue:1	{ok}
entSecurity801	Remote Reader Module.Sdi1	binaryValue:2	{ok}
entSecurity801	Remote Reader Module.Sdi2	binaryValue:3	{ok}
entSecurity801	Remote Reader Module.Sdi3	binaryValue:4	{ok}
entSecurity801	Remote Reader Module.Sdi4	binaryValue:5	{ok}
entSecurity801			
entSecurity801			
entSecurity801			
entSecurity801			
entSecurity801			
entSecurity801			

Filter

☐ Station Name

Must Include

☒ Case Sensitive

☐ Description

Must Include

☒ Case Sensitive

☐ BACnet Object Id

Must Include

☒ Case Sensitive


☐ Status

Must Include

☒ Case Sensitive

Ok

Cancel

This report opens when you click **Reports > Hardware > BACnet Points**. The **Filter** window opens when you click the **Filter** button ().

In addition to the common report columns controls, the Bacnet Points report includes a BACnet Object Id column and a Value column that identify the Bacnet point type (analog, binary, or other) and value, respectively.

Table 33. BACnet Points report columns and search criteria

Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the BACnet points.
BACnet Object Id	Displays data, and selects data to view based on the type of BACnet point: analog, binary, or other.
Value	Displays data, and selects data to view based on the current value of the point.
Status	Displays data, and selects data to view based on the condition of the point: {ok}, etc.

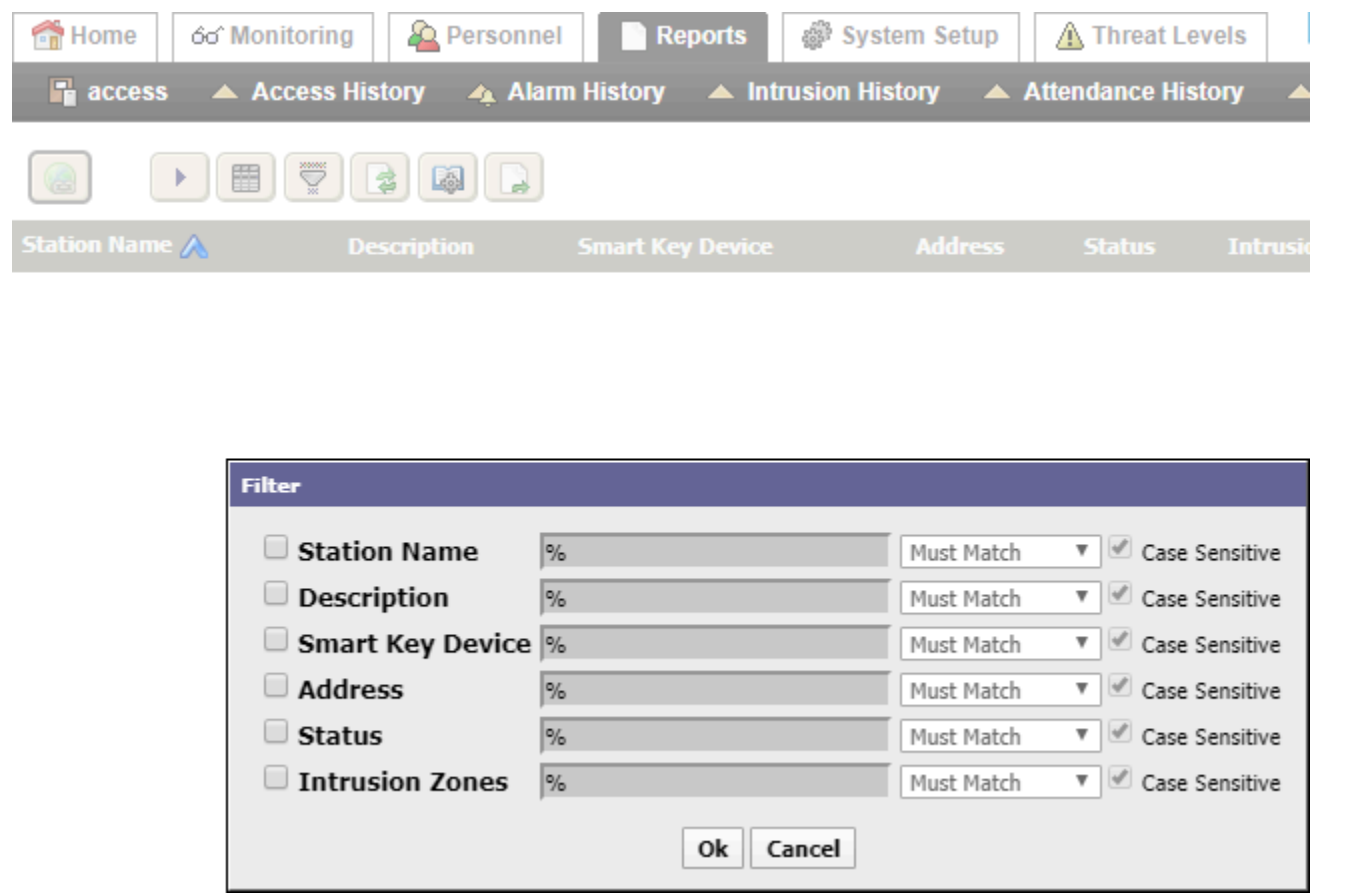
### Intrusion Displays Report and Filter


This report lists the intrusion displays in the database.

Intrusion displays present information about the status of an intrusion zone and let users interact with the zone using a keypad, touchpad, or other means of data input. The Intrusion Displays report lists the intrusion displays in a station. This may include intrusion displays from multiple intrusions zones.

Double-click on the intrusion display entry or click the **Intrusion Displays** menu item under the **Intrusion Setup** menu to view and edit details about a particular display.

**Figure 97.** Intrusion Displays report and Filter window



This report opens when you click **Reports > Hardware > Intrusion Displays**. The **Filter** window opens when you click the **Filter** button (  ).

The Intrusion Displays report includes default columns that show what intrusion zone the display is assigned to, the name and address of any SmartKey device assigned to the intrusion display, the display status, and the stations name. Other columns may be added.

**Table 34.** Intrusion Displays report columns and search criteria

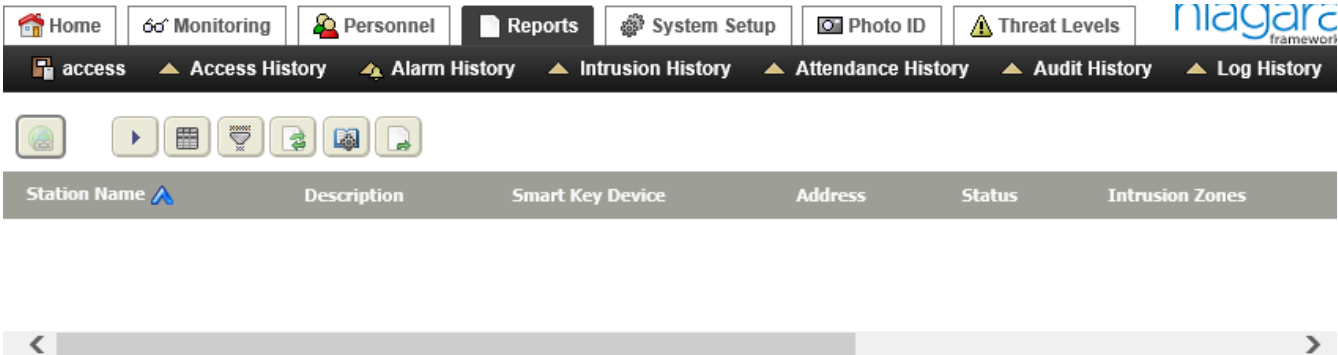
Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.

Column/criterion	Description
Description	Displays data, and selects data to view based on any description associated with the intrusion display.
Smart Key Device	Displays data, and selects data to view based on the name and address of any SmartKey device assigned to the intrusion display.
Address	Displays data, and selects data to display based on the integer value assigned to the intrusion SmartKey device.
Status	Displays data, and selects data to display based on the last recorded condition of the display device.
Intrusion Zones	Displays data, and selects data to display based on the associated intrusion zone the display is assigned to.

## Consolidated Intrusion Displays report

This report appears only in a Supervisor station. It lists all intrusion displays throughout the system.

**Figure 98.** Consolidated Intrusion Displays report



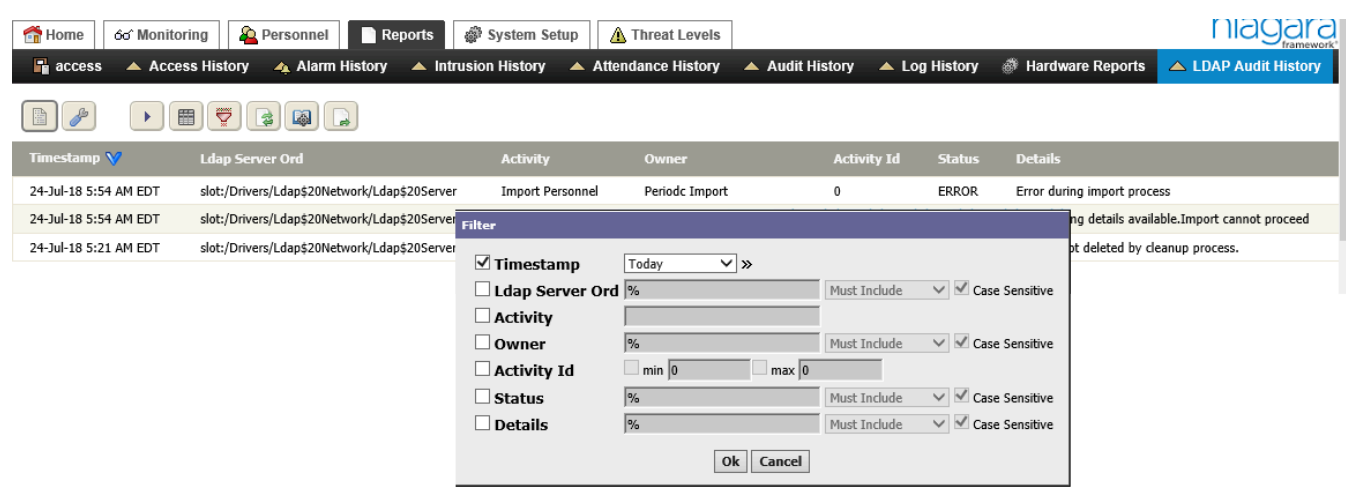
The Consolidated Intrusion Displays report view is available on a Supervisor when you click the **Intrusion Displays** menu item under the **Intrusion Setup** menu or when you select **Reports > Hardware Reports > Intrusion Displays**.

Report columns are the same as those displayed on an Intrusion Displays report created for a single, local station.

## LDAP Audit History report

This report summarizes the activity recorded with the LDAP server.

Figure 99. LDAP Audit History report and Filter window



This report opens when you click **Reports > LDAP Audit History**. The Filter window opens when you click the Filter button (  ).

This report provides these columns of information and filter options.

Table 35. LDAP Audit History columns and search criteria

Column/criterion	Description
Timestamp	Reports when the record was written to the database.
Ldap Server Ord	Reports the address of the LDAP server.
Activity	Identifies the type of LDAP request.
Owner	Reports the LDAP Display Name.
Activity ID	Reports the type of activity.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Details	Provides additional information.

## Miscellaneous reports

Miscellaneous reports include: Person Access Right Report, Person Reader Report, Access Right Reader Report, and Personnel Changes report.



The miscellaneous reports include:






- Person Access Right Report
- Person Reader Report
- Access Right Reader Report
- Personnel Changes



### Person Access Right Report

For a given person, this report identifies information related to access rights.

Figure 100. Person Access Right Report and Filter








Page  of Many

Person	Access Right Name	Start Date	End Date	Tenant
HHH75118	honeywell	null	null	
HHH75160	honeywell	null	null	
HHH75633	honeywell	null	null	
HHH75651	honeywell	null	null	
HHH75716	honeywell	null	null	
HHH75746	honeywell			
HHH75994	honeywell			
HHH76070	honeywell			
HHH76191	honeywell			
HHH76293	honeywell			

Filter

☐ Person

 None

☐ Access Right Name

%

Must Include

☒ Case Sensitive

☐ Start Date

Time Range


>>

☐ End Date

Time Range

>>

☐ Tenant

 None



Ok

Cancel

To access this report, expand **Personnel** select a person and click the Show Expirations button () or by clicking **Reports > Miscellaneous > Person Access Right Reader Report**.

Control buttons

In addition to the standard control buttons (Filter, Column Chooser, Refresh, manage Reports, and Export), these control buttons apply to the Person Access Right Report.

-  Hyperlink to Person opens the Edit Person view for the person associated with the selected record.
-  Hyperlink to Access Right opens the Edit Access Right view for the access right associated with the selected record.

Columns

Table 36. Person Access Right Report columns

Column	Description
Person	Reports the name of the employee.
Access Right Name	Identifies the title of the access right associated with the entity.
Start Date	Reports the beginning date from the schedule.
End Date	Reports the final date from the schedule.
Tenant	Reports the name of the associated tenant.

Person Reader Report

This report shows the reader(s) associated with one or more specific people.

**Figure 101.** Person Reader Report and Filter

Page  of Many

Page Size

Person	Access Right Name	Reader	Tenant
HHH75091	honeywell	entSecurity801:Door 1.Reader 1	
HHH75091	honeywell	entSecurity801:Door 2.Reader 2	
HHH75582	honeywell	entSecurity801:Door 1.Reader 1	
HHH75582	honeywell	entSecurity801:Door 2.Reader 2	
HHH75650	honeywell	entSecurity801:Door 2.Reader 2	
HHH75650	honeywell		
HHH75795	honeywell		
HHH75795	honeywell		
HHH75901	honeywell		
HHH75901	honeywell		

Filter

☐ Person

☐ Access Right Name

☐ Reader

☐ Tenant

None

Must Include ☐ Case Sensitive

None

None

None

Ok

Cancel

To access this report, expand **Personnel** select one or more people and click the Show Readers button ( ) or by clicking **Reports > Miscellaneous > Person Reader Report**.

Control buttons

In addition to the standard control buttons (Filter, Column chooser, Refresh, Manage Reports, and Export) this report provides these control buttons:

- Hyperlink to Person opens the Edit Person view for the person associated with the selected record.
- Hyperlink to Access Right opens the Edit Access Right view for the access right associated with the selected record.
- Hyperlink to Reader opens the reader view, which is documented in the remote devices chapter of the *Niagara Enterprise Security Reference*.

Columns

**Table 37.** Person Reader Report columns

Column	Description
Person	Reports the name of the employee.
Access Right Name	Identifies the title of the access right associated with the entity.
Reader	Reports the name of the reader associated with the access right.
Tenant	Reports the name of the associated tenant.



Access Right Reader Report and Filter window

This report lists access rights with their assigned reader so that you can easily see where readers are assigned.

Figure 102. Access Right Reader Report and Filter

Access Right Name	Reader	Tenant
honeywell	entSecurity801:Door 2.Reader 2	
honeywell	entSecurity801:Door 2.Reader 2	
honeywell	entSecurity801:Door 1.Reader 1	
honeywell	entSecurity801:Door 1.Reader 1	
honeywell		
honeywell		

Filter

☐ Access Right Name

Must Include


☒ Case Sensitive

☐ Reader

☐ Tenant



Ok

Cancel

You may access this report by clicking **Personnel > Access Rights** followed by selecting an access right and clicking the Show Readers button () or by clicking **Reports > Miscellaneous > Access Right Reader Report**.

Control buttons

In addition to the standard control buttons (Filter, Column Chooser, Refresh, Manage Reports, and Export), these control buttons apply to access rights and readers:

-  Hyperlink to Access Right opens the Edit Access Right view for the access right associated with the selected record.
-  Hyperlink to Reader opens the reader view, which is documented in the remote devices chapter of the *Niagara Enterprise Security Reference*.

Columns

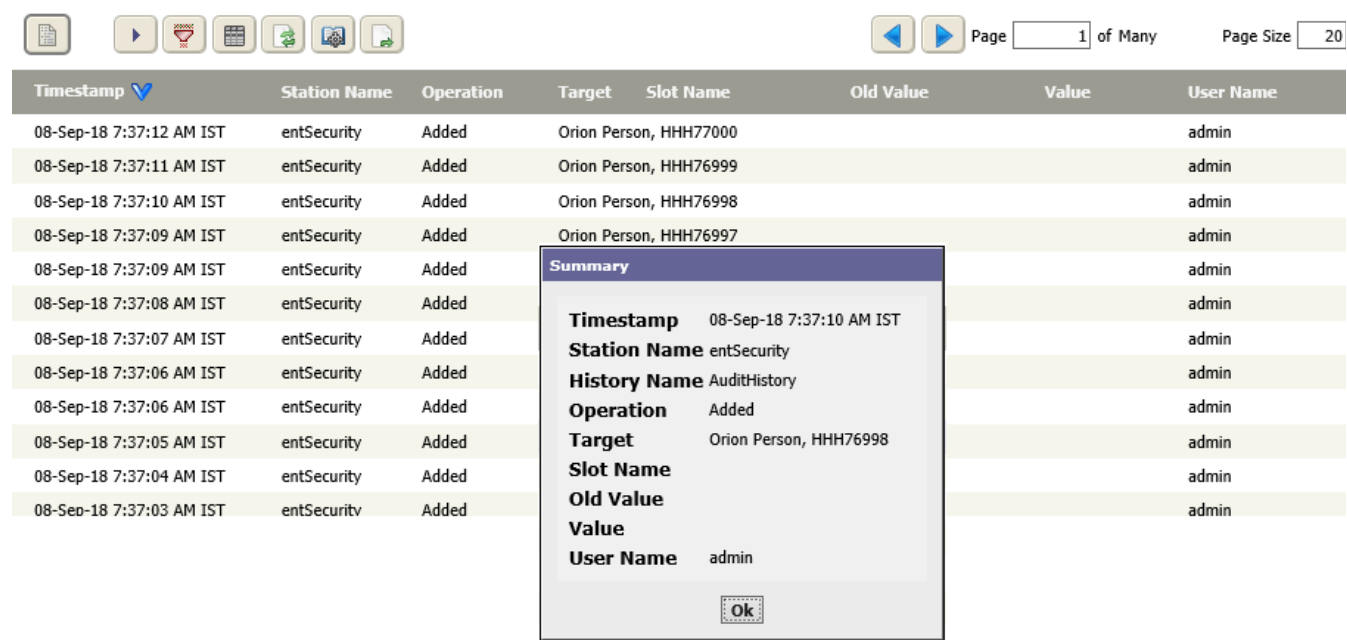
Table 38. Access Right Reader Report columns


Column	Description
Access Right Name	Identifies the title of the access right associated with the entity.
Reader	Reports the name of the reader associated with the access right.
Tenant	Reports the name of the associated tenant.

Personnel Changes report and Summary window


This report lists audit records of person-related changes. These changes include when, where, and what actions were taken. The **Summary** window shows the same information for a specific change row.

**Figure 103.** Personnel Changes report and Filter



You access this report by clicking **Reports > Miscellaneous > Personnel Changes**. You access the Summary window from the Personnel Changes view by clicking the Summary button (  ).

Control buttons

In addition to the standard control buttons (Auto Refresh, Column Chooser, Filter, Manage Reports and Export), this report includes a Summary button (  ). Selecting a row and clicking this button opens a summary of the information contained in the row.

Columns

**Table 39.** Personnel Changes columns and Summary window properties

Column/Property	Description
Timestamp	Reports when the record was written to the database.
Operation	Indicates what happened to the record: Added, Changed or Removed.
Target	Identifies the database and person’s name.
Slot Name	Identifies what changed.
Old Value	Reports the property value before the change occurred.
Value	Reports the current property value.
User Name	Reports the name of the user associated with this person.

Personnel Changes Filter window

This window defines search criteria for limiting the number of records in the Personnel Changes view.

Figure 104. Personnel changes Filter window

Filter

☒ Timestamp

Today

»

☐ Operation

☒ Target

Person

%

☒ filter.include

☐ filter.exact

☒ 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

This window opens from the Personnel Changes view when you click the Filter button ().

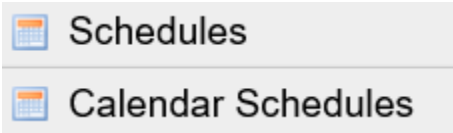
Criterion	Value	Description
Timestamp	drop-down list	Selects a period of time for displaying personnel change history.
Operation	Enums chooser	Selects the what happened to the record: Added, Changed, Removed.
Target (required criterion)	drop-down list and wild card (%)	<div>Defines the records to view:</div> <div>Person selects changes made to specific people.</div> <div>Badge selects changes made to selected badges.</div> <div>Access Right selects changes made to specific access rights.</div> <div>Tenant selects changes made to tenant records.</div> <div>Person Acc Join selects changes made to a person's access right. The access right is associated with a person or badge.</div>
Slot Name	wild card (%)	Defines what changed.
Old Value	wild card (%)	Defines the value before the change.

Criterion	Value	Description
Value	wild card (%)	Defines the value after the change.
User Name	wild card (%)	Defines the type of user, such as admin, operator etc.

# Chapter 5. Controller (System) Setup–Schedules

These views and windows add schedules and special events, which the system uses to manage automatic processes and trigger events.

**Figure 105.** Schedules menu



## Schedules view





This view manages weekly schedules. These manage normal daily events.




**Figure 106.** Schedules view



To open this view from the home page, expand **Controller Setup > Schedules**, and click **Schedules**.

In addition to the standard control buttons (Filter, Column Chooser, Refresh, Manage Reports and Export), the following relate specifically to schedules:

-  Add opens a view or window for creating a new record in the database.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  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.
-  Delete removes the selected record (row) from the database table. This button is available when you select an item.

-  Rename opens the Rename window with which to change the name of the selected item.
-  Duplicate opens a New window and populates each property with properties from the selected item. Using this button speeds the item creation.
-  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.

Below the buttons, the table shows all current schedules that are available according to the privilege-level of the user that is currently logged on.

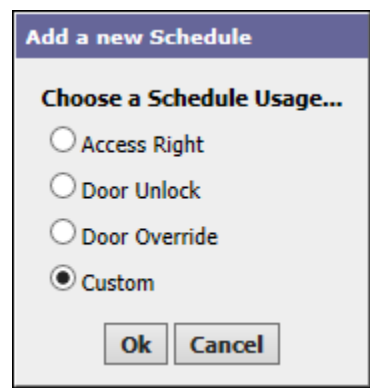
**Table 40.** Schedules view table default columns

Column	Description
Schedule Name	Reports the name of the associated schedule (if any).
Usage	Helps to identify the schedule and provide filtering options when choosing a schedule from a list.
Access Right Name	Identifies the title of the access right associated with the entity.
Intrusion Pin Name	Identifies the name of the intrusion pin.


Add a new Schedule window

This window identifies the type of schedule to create. When you click **Ok**, the system opens the Add New Schedule view.

**Figure 107.** Add a New Schedule window



To access this window from the main menu, click **Controller (System) Setup > Schedules**, followed by clicking

the Add control button ().

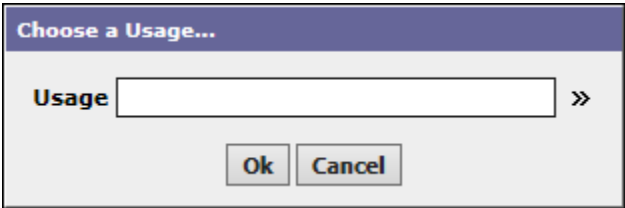
The radio buttons identify the type of component with which to associate the schedule.

- Access Right
- Door Unlock

- Door Override
- Custom (defines another components)

Selecting Custom, opens the **Choose A Usage...** window.

**Figure 108.** Choose a Usage... window

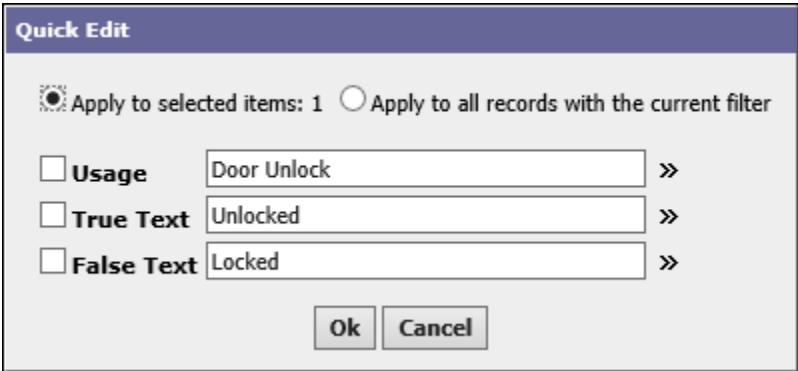



This window opens a string chooser.

Schedules Quick Edit window

This window edits schedule properties.

**Figure 109.** Schedule Quick Edit window



You access this window from the main menu by clicking **Controller (System) Setup > Schedules**, followed by selecting a schedule clicking the Quick Edit button (  ).

Property	Value	Description
Apply	radio buttons	Identify which schedule(s) to update.
Usage	String chooser	Updates the purpose of the schedule.
True Text	String chooser	Updates the text associated with a configured day and time on the schedule.

Property	Value	Description
False Text	String chooser	Updates the text associated with days and times that are outside the schedule.

Schedules Filter window

This window the search criteria used to search for schedules in the database.

Figure 110. Schedule Filter window

Filter

☐ Schedule Name

%

Must Include

☒ Case Sensitive

☐ Usage

%

Must Include

☒ Case Sensitive

☐ Access Right Name

%

Must Include

☒ Case Sensitive

☐ Intrusion Pin Name

%

Must Include

☒ Case Sensitive

Ok

Cancel

You access this window from the main menu by clicking **Controller (System) Setup > Schedules**, followed by clicking the Filter button ().

Criterion	Value	Description
Schedule Name	wild card (%)	Searches based on the name of the schedule.
Usage	wild card (%)	Searches based on the purpose of the schedule.
Access Right Name	wild card (%)	Searches based on the name of the access right associated with the schedule.
Intrusion Pin Name	wild card (%)	Searches based on the name of the intrusion PIN associated with the schedule.

Add New (edit or duplicate) Schedule view

This view adds a schedule to the database. Once added, the same set of tabs edit the schedule. Duplicating an existing schedule saves time because all you have to do is change the properties that differ from the source schedule.



SummarySchedulerSchedule SetupSpecial EventsAccess RightsIntrusion Pins

	Sun	Mon	Tue	Wed	Thu	Fri	Sat	
12:00 AM								12:00 AM
3:00 AM								3:00 AM
6:00 AM								6:00 AM
9:00 AM	Denied						Denied	9:00 AM
12:00 PM								12:00 PM
3:00 PM								3:00 PM
6:00 PM								6:00 PM
9:00 PM								9:00 PM
12:00 AM								12:00 AM

Start:

0900AMEDT




Finish:

0500PMEDT

Output:

☐ null ☒ Denied






The Default Output for this Schedule is currently set to "Denied {ok}".

This view opens when you click the Add (  ) or Duplicate (  ) control buttons at the top of the Schedules view. The edit view opens when you select a schedule in the Schedules view and click the Hyperlink button (  ).

**Display Name** provides a unique name for the schedule.

Buttons

In addition to the standard control buttons (Delete, Rename, Column Chooser, Refresh, Manage Reports and Export, these control buttons perform schedule functions:

-  Add opens a view or window for creating a new record in the database.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  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.
-  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.



- Filter buttons open the Filters window, which defines a query action for limiting the output visible in tables and reports. The gray version indicates unfiltered data. The red version indicates filtered data.

Schedule, Summary tab

For any selected day, this tab displays a read-only summary of all schedule events with source.

Summary

Scheduler

Schedule Setup

Special Events

Access Rights

Intrusion Pins

Always

Mapped Ord: **/Services/EnterpriseSecurityService/schedules/Always**

Type: Schedule

Schedule Name: Always

Usage:

Status: {ok}

Out Source: Default Output

Out: Access {ok}

In: - {null}

Next Time: 25-Sep-18 12:00 AM IST

Next Value: Access {ok}

Intrusion Pins

**Test**

This tab opens when you double-click a schedule in the Schedules view and any time you save changes made in another tab.

Table 41. Schedule properties

Property	Description
Mapped Ord	Shows the location of the schedule.
Type	Identifies this Summary tab as a schedule summary.
Schedule Name, Schedule	Reports the name of the associated schedule (if any).
Usage	Helps to identify the schedule and provide filtering options when choosing a schedule from a list.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Out Source	Displays the current day, for example: Week: Thursday.
Out	Reports the output value of the schedule component. This value is true during any configured calendar day(s), otherwise it is false.
In	Describes the current input, such as a linked schedule. If this property is linked and it has a value (non-null), this value overrides the scheduled output.
Next Time	Reports the next date and time this event will occur. This could be a beginning or ending of a scheduled event. If the next event is more than a year into the future, this column reports null.

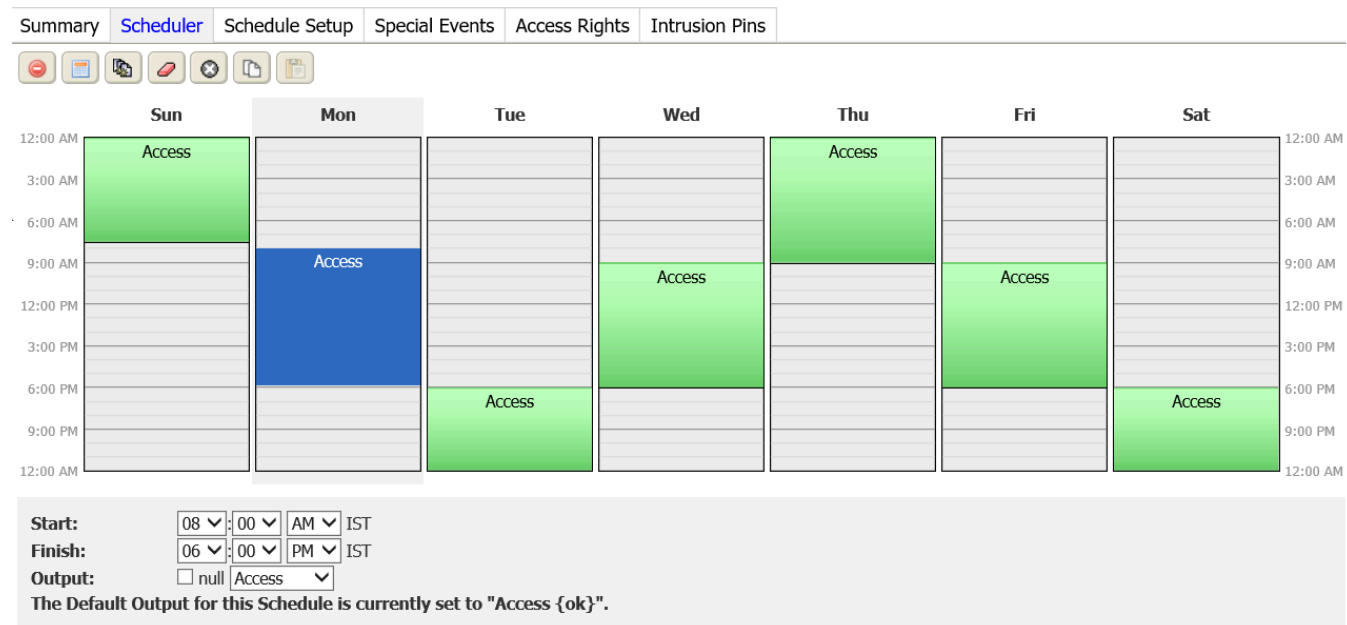
Property	Description
Next Value	Reports the next scheduled out value (true or false) to occur at Next Time. This value is meaningless if Next Time is null.
Intrusion Pins and Access Rights	Identifies the intrusion pins and access rights assigned to the schedule.

Located at the bottom of the tab is a list of all the access rights and intrusion PIN assignments associated with the schedule.


Schedler tab

This tab specifies Sunday-through-Saturday (weekly) normally-scheduled event times and output value that repeat from week to week, based on the day of the week and the time of day.

Figure 111. Scheduler tab




To access this tab from the main menu click **Controller (System) Setup > Schedules**. If you are creating a new







schedule, click the Add button (  ). If you are editing an existing schedule, select the schedule row in the table and click the Hyperlink button, or double-click the existing schedule row, then click the Scheduler tab.

The weekly Scheduler right-click menu opens when you right-click a selected event. The options it provides are the same as those provided by the control buttons.

Buttons

The Scheduler control buttons are:

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

-  All Day Event sets up an event that starts at 12 am and ends at 12 am the next day.
-  Apply M-F configures Monday through Friday using the current day.
-  Clear Day removes all events on the selected day.
-  Clear Week removes all events scheduled for the entire selected week.
-  Copy Day copies all events for the selected day to use with the paste button.
-  Paste Day places all events copied from another day into the selected day. This button is active only if you used the copy day button first.

Property	Value	Description
Start	hour:minute, AM, PM	Fine tunes the start time. For any event, this time is inclusive. The event extends to, but does not include the end time. In other words, there is no output “blip” between adjacent events, even across days. For example, if a Monday event ends at midnight, a Tuesday event starts at midnight. Schedule output continues, provided both events have the same Output value.
Finish	hour:minute, AM, PM	Fine tunes the end time.
Output	true or false	Defines a value that the system routes to the access device at the scheduled times.

Schedule Setup (weekly schedules) tab

This tab includes a set of properties that affect the way the schedule works, and provides information about current and projected schedule values. It defines a default output (output during non-event times), schedule effective times, special event cleanup operation, and schedule facets (display text for outputs).

Summary	Scheduler	Schedule Setup	Special Events	Access Rights	Intrusion Pins
<b>Default Output</b>	Access {ok} »				
<b>Cleanup Expired Events</b>	true ▼				
<b>Scan Limit</b>	090 d 00 h 00 m [1day - +inf]				
<b>Last Modified</b>	21-Jun-18 5:01 PM IST				
<b>Out Source</b>	Default Output				
<b>Out</b>	Access {ok}				
<b>In</b>	- {null} »				
<b>Next Time</b>	19-Sep-18 6:00 PM IST				
<b>Next Value</b>	Access {ok}				
<b>Usage</b>	<input type="text"/> »				
<b>True Text</b>	<input type="text" value="Access"/> »				
<b>False Text</b>	<input type="text" value="No Access"/> »				

To access this tab from the main menu, click **Controller (System) Setup > Schedules**, then double-click the a schedule row in the table, and click the Schedule Setup tab.

Property	Value	Description
Default Output	read only	When a schedule event (special or weekly) is not defined from another source, the schedule component's output serves as the default value. Use the <code>null</code> output option when you do not want to specify either a <code>true</code> or <code>false</code> value by default.
Cleanup Expired Events	true (default) or false	Deletes events.  true configures the system to delete one-time special events that will not occur again. When a special event is deleted, a message is sent to the schedule log, and that special event no longer appears on the Special Events tab.
Scan Limit	day, hours, minutes	Defines how far into the future the system looks when calculating the <code>Next Time</code> or <code>Next Value</code> property. Make sure that this value is always positive and always greater than 24 hours.
Last Modified	read-only	Indicates the last time that the

Property	Value	Description
		schedule was modified.
Out Source	read-only	Indicates what is currently generating the out value. For example, the Out Source might be coming from the Default Output value if there is no event scheduled. Or it may be coming from the Input value, if the In property is set to a value other than null.
Out (general)	read-only	<p>Displays the current value of the proxy point including facets and status.</p> <p>The value depends on the type of control point.</p> <p>Facets define how the value displays, including the value's number of decimal places, engineering units, or text descriptors for Boolean/enum states. You can edit point facets to poll for additional properties, such as the native statusFlags and/or priorityArray level.</p> <p>Status reports the current health and validity of the value. Status is specified by a combination of status flags, such as <code>fault</code>, <code>overridden</code>, <code>alarm</code>, and so on. If no status flag is set, status is considered normal and reports <code>{ok}</code>.</p>
In	read-only	Reports the current input value.
Next Time	Baja AbsTime format, for example: 03-Feb-05 5:00 PM	<p>Reports the time of the next scheduled output change for the component. If the time is more than a year away, this value is null.</p> <p>A typical application is for informational display. If needed, you can link slots into control logic. For example the TimeDifference and CurrentTime objects (kitControl, Timer) also provide AbsTime slots.</p>

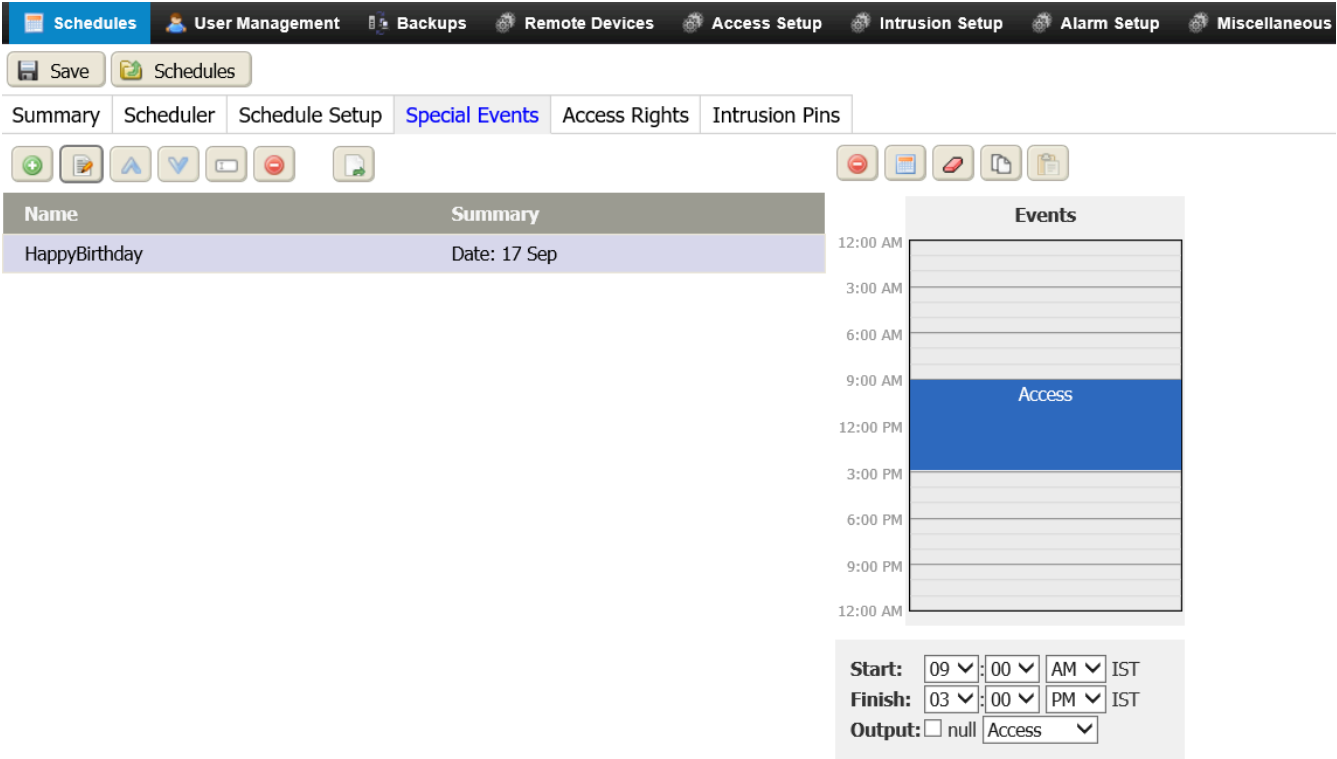
Property	Value	Description
Next Value	(defaults to {ok})	<p>Reports the next scheduled output value. Values are <code>false</code> or <code>{ok}</code>.</p> <p>This value is meaningless if <code>Next Time</code> is <code>null</code>.</p>
Usage	String Chooser	<p>Adds information regarding how to use the schedule. This property can help to identify the schedule and improve filtering options for choosing a schedule from a list. For example, when assigning a schedule to an access right, you might use the <code>Filter</code> window's <code>Usage</code> property to show only access right schedules.</p>
True Text	String Chooser	<p>Defines the text to display when the current time is within the range defined by the schedule. For example, "Unlocked"</p>
False Text	String Chooser	<p>Defines the text to display when the current time is outside of the range defined by the schedule. For example, "Locked"</p>

Special Events tab

This tab defines any one-off exceptions to the standard weekly schedule, as special events. These are not the same events the system manages using a calendar schedule. Rather, these are extra ordinary events that occur only once or rarely, such as time off to view an eclipse of the sun.

Buttons above the table





Figure 112. Special Events editor





You access this tab by clicking **Controller Setup > Schedules > Schedules**, double-clicking a schedule, and clicking the Special Events tab.

The Special Events editor is comprised of two primary areas: the Special Events table and a 24-hour time pane.

In addition to the standard control buttons (Rename, Delete, and Export), these control buttons, located above the Special Events table, manage special events:

-  Add opens a view or window for creating a new record in the database.
-  Edit opens the Edit window.
-  Move Up and Move Down change the sequence of rows in the direction indicated one selected row at a time.
-  Rename opens the Rename window with which to change the name of the selected item



-  Delete removes the selected record (row) from the database table. This button is available when you select an item.
-  Export opens the Export window for creating a PDF or CSV formatted report of the current table.

Buttons above the events day

These control buttons, located above the Events day, apply to the day view on the right.





-  All Day Event sets up an event that starts at 12 am and ends at 12 am the next day.
-  Clear Day removes all events on the selected day.
-  Copy Day copies all events for the selected day to use with the paste button.
-  Paste Day places all events copied from another day into the selected day. This button is active only if you used the copy day button first.

Table 42. Special Events table columns

Property	Description
Name	Reports the name that describes the event or function.
Summary	Summarizes the event configuration, for example: Week and Day: Sun Every Week Every Month

Special Events properties

Property	Value	Description
Start	hour:minute, AM, PM	Fine tunes the start time. For any event, this time is inclusive. The event extends to, but does not include the end time. In other words, there is no output “blip” between adjacent events, even across days. For example, if a Monday event ends at midnight, a Tuesday event starts at midnight. Schedule output continues, provided both events have the same Output value.
Finish	hour:minute, AM, PM	Fine tunes the end time.
Output	true or false	Defines a value that the system routes to the access device at the scheduled times.

Add event window

Creates a special one-off event or references a calendar schedule, which defines a recurring special event.

Add

Display Name


Memorial Day

Type

Date

Ok

Cancel

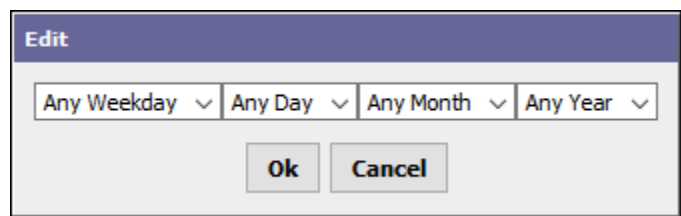
This window opens when you click the Add button () to create a new special event.

Property	Value	Description
Display Name	text	Creates an object name for display purposes, which may differ from the actual object name.
Type	drop-down list	<p>Determines the selection criteria for day or days, with the following choices: <code>Date:(default)</code> defines type by various combinations of weekday, numerical date, month or month combinations, and year.</p> <p>Refer to .</p> <p>Refer to <a href="#">Add (or edit) date range window</a></p> <p><code>Week And Day</code> defines the type by By combination of day of week, week in month, month.</p> <p>Refer to <a href="#">Add (or edit) week and day window</a>.</p> <p><code>Date Range</code> defines the type by start and end range, using for each a combination of day, month, year.</p> <p><code>Custom</code> defines type by various combinations of day, month, weekdays, and year.</p> <p>Refer to <a href="#">Add (or edit) custom window</a>.</p> <p><code>Reference</code> adds a pre-defined Calendar Schedule to your calendar if you have one already setup.</p>

Property	Value	Description
		Selecting <b>Reference</b> opens a second Add window that lists all calendar schedules (Calendars) available in the station, by path. Select any one for the day(s) portion of this special event.  Refer to <a href="#">Add (or edit) reference window</a>

Add (or edit) date window  
This window serves both the weekly and calendar schedules. Its four drop-down lists configure a one-off or recurring special event.

Figure 113. Add/Edit date window



This window opens when you select **Date** for the **Type** property on the Add event window.

You can make only one selection for each property. This includes an *Any...* option, in addition to the specific options.

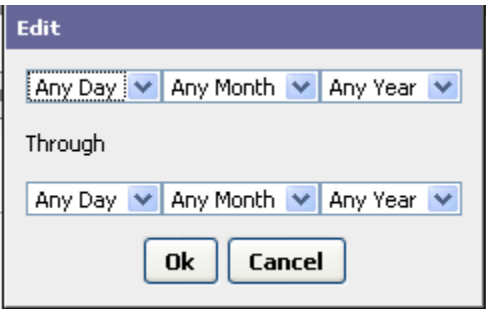
Property	Value	Description
Day of the week	drop-down list, default: Any Weekday	Identifies the day of the week: Sunday, Monday, etc.
Day in the month	drop-down list, default: Any Day	Identifies the day of the month: 1, 2, ... 31.
Month of the year	drop-down list, default: Any Month	Identifies the month of the year: Jan, Feb, etc.
Year	drop-down list, default: Any Year	Identifies the year up to and including 2025.

You can make only one selection for each property. The default of an *Any...* is also valid for each. The system adds all properties together.

For example, if you select a weekday of Tuesday, a day of the month of 5, and leave the remaining properties configured as *Any...* the system specifies the event to occur on the fifth of any month in any year that happens to fall on a Tuesday. If a month has no Tuesday the fifth, then no event occurs that month.

Add (or edit) date range window

This Edit window defines an event, such as a conference or trade show, that has a one-off or recurring start and end date.



This window opens when you select a `Date Range` option for the **Type** property in the **Add** window.

The starting date for the range is at the top of the window.

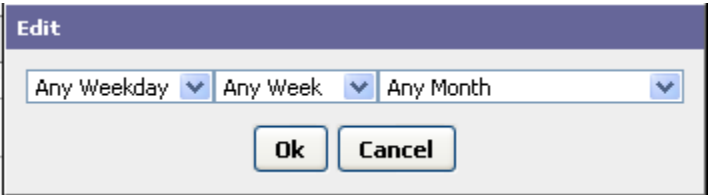
Property	Value	Description
Day of the month	drop-down list, default: Any Day	Identifies the day of the month: 1, 2, ... 31.
Month of the year	drop-down list, default: Any Month	Identifies the month of the year: Jan, Feb, etc.
Year	drop-down list, default: Any Year	Identifies the year up to and including 2025.

Each property offers an `Any . . .` option, in addition to a specific selection (day-of-month, month-of-year, year). You make only one selection in each. The system calculates the from and through dates in the range based on this input.

The start day can be after the end day. For example, the start day can be in December and the end day in March. Such an event begins in December and continues through January and February.

Add (or edit) week and day window

This window configures a regular event that is independent of the year and specific day of the month. Two of the monthly options available in this window allow you to define an event that occurs every-other month through the year, for example: `Week and Day: Sun Every Week Every Month`



This option opens when you select `Week and Day` for the **Type** property in the **Add** window.

Property	Value	Description
Day of the week	drop-down list, default: Any Weekday	Identifies the day of the week: Sunday, Monday, etc.
Week in the month	drop-down list, default: Any Week	Identifies the week number in the month: Week 1, Week 2, etc. and Last 7 Days.
Month of the year	drop-down list, default: Any Month	Identifies the month of the year: Jan, Feb, etc. It includes options to specify every other month beginning with January (Jan) and every other month beginning with February (Feb).

Add (or edit) custom window

If the other combinations do not work, this Edit window offers another way to define date information.

Edit

Any Day

Any Month

Any Weekday

Any Week

Any Year

Ok

Cancel

This window opens when you select Custom for the **Type** property in the Add window.

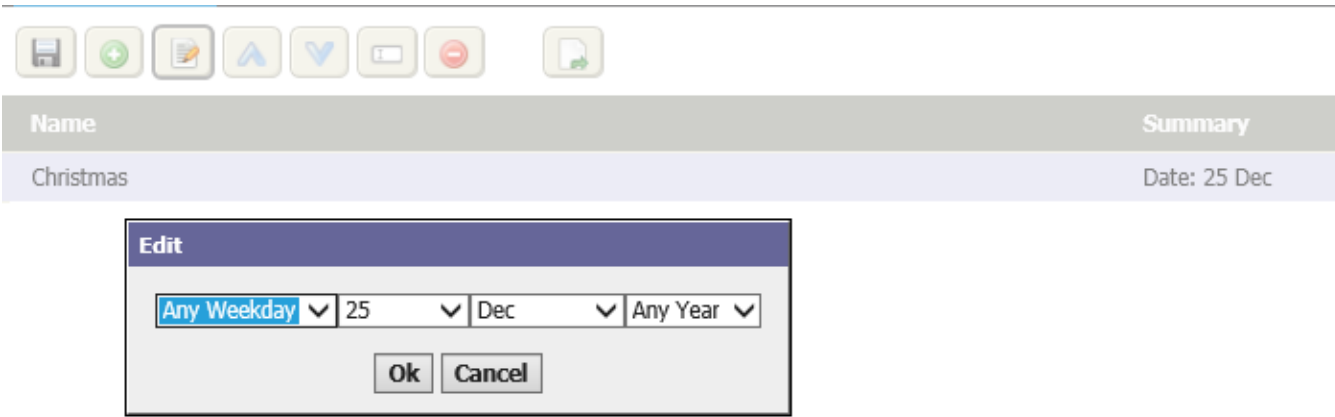
Property	Value	Description
Day of the month	drop-down list, default: Any Day	Identifies the day of the month: 1, 2, ... 31.
Month of the year	drop-down list, default: Any Month	Identifies the month of the year: Jan, Feb, etc.
Day of the week	drop-down list, default: Any Weekday	Identifies the day of the week: Sunday, Monday, etc.
Week in the month	drop-down list, default: Any Week	Identifies the week number in the month: Week 1, Week 2, etc. and Last 7 Days.
Year	drop-down list, default: Any Year	Identifies the year up to and including 2025.

Add (or edit) reference window

This window defines the calendar schedule to associate with this weekly schedule.

Calendar Schedule usage by special event reference allows global changing of day definitions, where multiple weekly schedules can reference one or more calendar schedules. Any edit of a calendar schedule affects all weekly schedules containing the special event that references it.

**Figure 114.** Example of a referenced calendar schedule

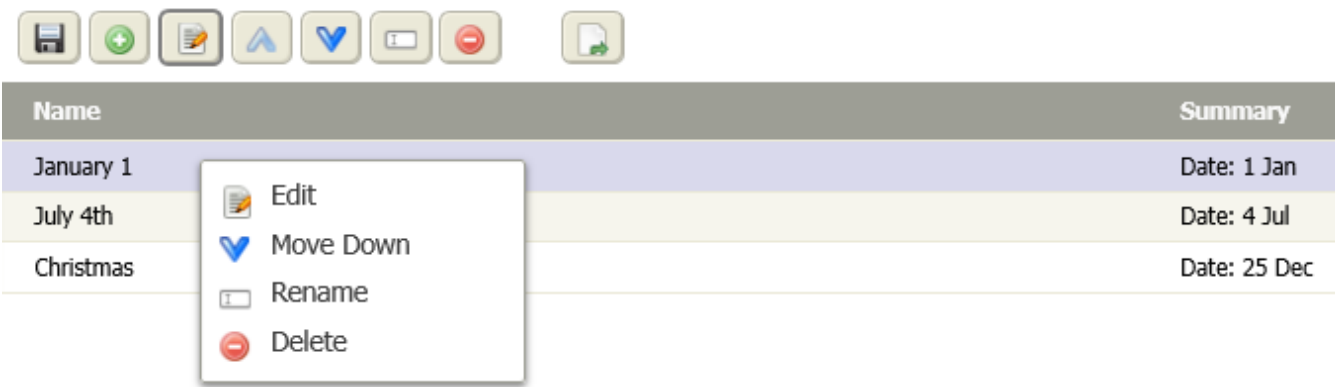


The figure above shows a portion of its Special Events tab, listing a single special event that references a calendar schedule. This indicates that the special event (a holiday calendar day) is defined remotely in the configuration of the referenced calendar schedule.


The unlabeled property in the **Edit** window contains the slot ORD for the calendar schedule. You select it from a drop-down list.

**Special Events right-click menu and other controls**  
Selecting an event on the Special Events tab and right-clicking opens the right-click menu.

**Figure 115.** Right-click menu



Special event menu options may include the following:

- **Edit**—Edit day(s) selection criteria (without changing the special event type). This is the same selecting the event and clicking the Edit button (  ).
- **Rename**—Rename selected special event. This is the same as selecting the event and clicking the Rename



button ( ).

- Move Up—Move special event to a higher priority. This is the same as selecting the event and clicking the



Move Up button ( ).

- Move Down—Move special event to a lower priority. This is the same as selecting the event and clicking the



Move Down button ( ).

- Delete—Removes the selected special event from the schedule component. This is the same as selecting

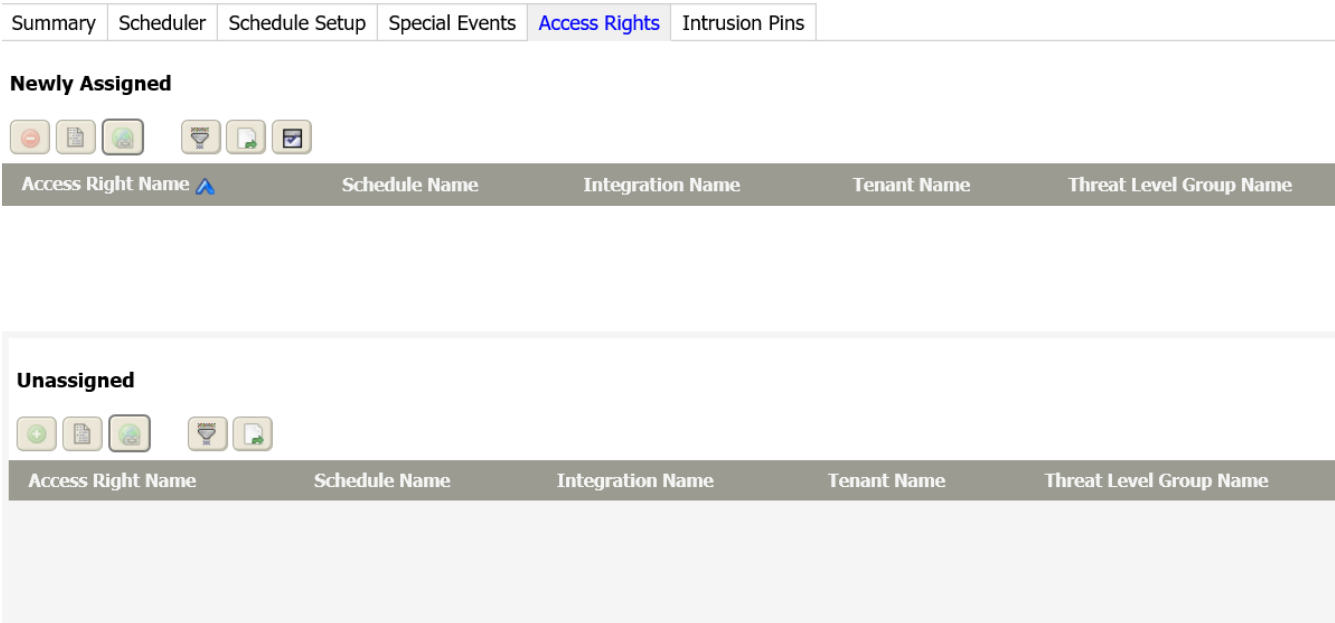


the event and clicking the Delete button ( ).

Access Rights tab

This tab lists assigned access rights and the learn mode to assign access rights to the displayed schedule.

Figure 116. Access Rights tab






You access this view from the main menu by clicking **Controller (System) Setup > Schedules**, followed by clicking the Add button to create a new schedule, and clicking the **Access Rights** tab.

Buttons

In addition to the standard control buttons (Export and Assign Mode) this view provides these control buttons:



- Remove Assignment (Unassign) disassociates an assignment that was previously made.

-  Summary opens the Access Rights Summary window.
-  Hyperlink opens the Access Rights view.
-  Filter opens the Access Rights Filter window.

### Columns

Column	Description
Access Right Name	Identifies the title of the access right associated with the entity.
Schedule Name	Reports the name of the associated schedule (if any).
Integration Name	Reports the name of the associated integration ID. The system performs building automation actions, such as turning the lights on, associated with this type of ID.
Tenant Name	Reports the name of the associated tenant.
Threat Level Group Name	Reports the name of the associated threat level group.

### Intrusion Pins tab

The Intrusion PINs (Personal Identification Numbers) tab lists assigned intrusion PINs and allows you to use the learn mode to assign any intrusion PINs to the displayed schedule.



Figure 117. Intrusion Pins tab

SummarySchedulerSchedule SetupSpecial EventsAccess RightsIntrusion Pins

Assigned

Intrusion Pin Name	Schedule Name	Tenant Name
Test	Always	





Newly Unassigned

Intrusion Pin Name	Schedule Name	Tenant Name
--------------------	---------------	-------------

You access this view from the main menu by clicking **Controller (System) Setup > Schedules**, followed by clicking the Add button to create a new schedule, and clicking the **Intrusion Pins** tab.

Buttons

In addition to the standard control buttons (Export and Assign Mode) this view provides these control buttons:

-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  Summary opens the Intrusion Pins Summary window.
-  Hyperlink opens the Intrusion Pins view.
-  Filter opens the Intrusion Pins Filter window.

March 25, 2025

165

Columns

**Table 43.** Intrusion Pins tab columns

Column	Description
Intrusion Pin Name	Reports the name of the intrusion pin.
Schedule Name	Reports the schedule name.
Tenant Name	Reports the tenant name.


Calendar Schedules view


This view specifies regular exceptions to the weekly schedule. On a calendar schedule, you define entire days, using four types of day event selections: Date, Date Range, Week and Day, or Reference. You can add as many day events as needed in the same calendar schedule.

The system links calendar schedules by referencing them from the special events tab of one or more weekly schedules. Each referenced calendar schedule defines the day portion of a special event. Then, you configure time-of-day events in each special event as needed.

Calendar schedules allow you to define the events for a day, which can be applied to multiple weekly schedules. If events change, all you have to do to change all your weekly schedules is to change the one calendar schedule because all weekly schedules reference it.

**Figure 118.** Calendar Schedules view






Display Name 	Status	Out	Next Time	Next Value	To Display Path String
Calendar Schedule	{ok}	false {ok}	14-Oct-18 12:00 AM IST	false {ok}	/Services/EnterpriseSecurityService/calendarSchedules/Calendar Schedule
Holidays	{ok}	false {ok}	25-Oct-18 12:00 AM IST	false {ok}	/Services/EnterpriseSecurityService/calendarSchedules/Holidays

To open the view from the home page you expand **Controller Setup > Schedules** and click **Calendar Schedules**.

The table in this view shows all current schedules that are available according to the privilege-level of the user that is currently logged on.

Buttons

The following control buttons serve this view:

-  Add opens a view or window for creating a new record in the database.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  Delete removes the selected record (row) from the database table. This button is available when you select an item.



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

Columns

**Table 44.** Calendar Schedules columns

Column	Description
Display Name, Name	Reports the name that describes the event or function.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Out	true indicates that an event is scheduled for the day. All other days (on which nothing is scheduled) are false.
Next Time	Reports the next date and time this event will occur. This could be a beginning or ending of a scheduled event. If the next event is more than a year into the future, this column reports null.
Next Value	Reports the next scheduled out value (true or false) to occur at Next Time. This value is meaningless if Next Time is null.
To Display Path String	Defines the station path for this zone.

Calendar Schedules Filter window

This window defines search criteria with which to limit the number of records displayed in the Calendar Schedules table.

**Figure 119.** Calendar Schedules Filter window

Filter

☐ Display Name

%

Must Include

☒ Case Sensitive

☐ Status

%

Must Include

☒ Case Sensitive

☐ Out

%

Must Include

☒ Case Sensitive

☐ Next Time

Time Range

? to ?

>>

☐ Next Value

%

Must Include

☒ Case Sensitive

☐ To Display Path String


%

Must Include

☒ Case Sensitive

Ok

Cancel

This window opens when you click the Filter button () on the Calendar Schedules view.

Property	Value	Description
Display Name	wild card (%)	Searches for calendar schedule records by name.
Status	wild card (%)	Searches for calendar schedule

Property	Value	Description
		records by status: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Out	wild card (%)	Searches for calendar schedule records based on the value of the schedule's out slot (true or false).
Next Time	drop-down list and Advanced Time Range Options window	Searches based on the next time this event is scheduled to occur.
Next Value	wild card (%)	Searches based on the out value (true or false) for the next time this event is scheduled to occur.
To Display Path String	wild chard (%)	Searches based on the slot path of the schedule in the station.

## Add New (or edit) Calendar Schedule view

This view creates or edits a global calendar schedule that a weekly schedule can reference from its Special Events tab.

**Figure 120.** Calendar Schedules view

Save Calendar Schedules

Display Name

Events Schedule Setup

Save Add Edit Up Down Home -

Name	Summary
Parade	Date: 15 Aug

To access this view from the home page expand **Controller Setup > Schedules > Calendar Schedules**, and click the new button or double-click an existing calendar schedule row in the table.

The buttons at the top of the view perform these functions:

- **Save** stores the schedule in the database.
- **Calendar Schedules** returns to the menu page.

**Display Name** provides a unique name for the calendar schedule. This property is not available in an add view.

Events tab

This view adds and edits events. You typically reference calendar schedules from the Special Events tab of one or more weekly schedules. Each referenced calendar schedule defines the daytime portion of a special event.








Figure 121. Events tab



To access this view from the home page menu, expand **Controller Setup > Schedules > Calendar Schedules**, then click the add button or double-click the calendar row in the table.

Buttons

The following are the Events tab control buttons:

-  Save updates the database with the current information.
-  Add opens a view or window for creating a new record in the database.
-  Edit opens the Edit window.
-  Move Up and Move Down change the sequence of rows in the direction indicated one selected row at a time.
-  Rename opens the Rename window with which to change the name of the selected item.
-  Delete removes the selected record (row) from the database table. This button is available when you select an item.
-  Export opens the Export window for creating a PDF or CSV formatted report of the current table.

Below the buttons, the table shows all current calendar schedules that are available according to the privilege-level of the user that is currently logged on.

Columns

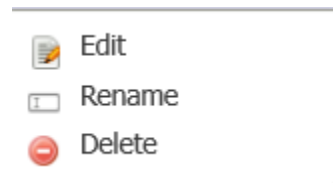
Table 45. Events tab table

Column	Description
Name	Reports the name that describes the event or function.
Summary	Reports the date(s) for the event.

Right-click menu

When you right-click any event the system opens the right-click menu.

Figure 122. Right-click Events menu



This menu provides the same commands as the control buttons.

**NOTE:** Priority selections (right-click menu or in bottom buttons) only affect the list order for events in a Calendar Schedule—true priority applies only to special events (in weekly schedules).

Schedule Setup (calendar schedules) tab

This tab configures the global calendar schedules that you reference from regular schedules.

Figure 123. Schedule Setup tab

Summary	Scheduler	Schedule Setup	Special Events	Access Rights	Intrusion Pins
Default Output	Access {ok} »				
Cleanup Expired Events	<input type="checkbox"/> true ▼				
Scan Limit	<input type="text" value="090"/> d <input type="text" value="00"/> h <input type="text" value="00"/> m [1day - +inf]				
Last Modified	21-Jun-18 5:01 PM IST				
Out Source	<div>Default Output</div>				
Out	Access {ok}				
In	- {null} »				
Next Time	19-Sep-18 6:00 PM IST				
Next Value	Access {ok}				
Usage	<input type="text"/>				»
True Text	<input type="text" value="Access"/>				»
False Text	<input type="text" value="No Access"/>				»

You access this tab by clicking **Controller (System) Setup > Schedules > Calendar Schedules > Schedule Setup**.

Property	Value	Description
Default Output	drop-down list	Configures the default value for output: for example: Granted/Denied, True/False.
Cleanup Expired Events	true or false	<p>Manages expired events.</p> <p>true configures the system to delete one-time special events that will not occur again. When a special event is deleted, a message is sent to the schedule log, and that special event no longer appears on the Special Events tab.</p> <p>false configures the system to retain one-time events even though they will not occur again.</p>
Scan Limit	day, hours, minutes	Defines how far into the future the system looks when calculating the Next Time or Next Value property. Make sure that this value is always positive and always greater than 24 hours.
Last Modified	read-only	Indicates the last time that the schedule was modified.
Out Source	read-only	Displays the day of the week, for example: Week: Thursday
Out	read-only	Indicates the result of an action based on the schedule. For example, the action may be to allow access to a building only during business hours. The system returns "true" if the individual scans their badge during business hours, and "false" if the individual attempts to enter outside of business hours. The True Text and False Text properties define the message the person sees.
In	read-only	Displays the current input value.
Next Time	Baja AbsTime format, for example: 03-Feb-05 5:00 PM	<p>Reports the time of the next scheduled output change for the component. If the time is more than a year away, this value is null.</p> <p>A typical application is for informational display. If needed,</p>

Property	Value	Description
		you can link slots into control logic. For example the TimeDifference and CurrentTime objects (kitControl, Timer) also provide AbsTime slots.
Next Value	(defaults to {ok})	<p>Reports the next scheduled output value. Values are <code>false</code> or <code>{ok}</code>.</p> <p>This value is meaningless if <code>Next Time</code> is <code>null</code>.</p>
Usage	chooser	Selects the type of schedule: access right, door unlock, door override, and custom.
True Text	text	Sets up the word or phrase to display when the schedule permits entry.
False Text	text	Sets up the word or phrase to display when the schedule denies entry.



# Chapter 6. User management

A user can be a person who configures and manages a station or a software program that accesses a station without requiring human intervention (machine-to-machine user). The personnel function does not manage users, and user names are not the same as person names. Persons access the building. Users access the system that manages the building.

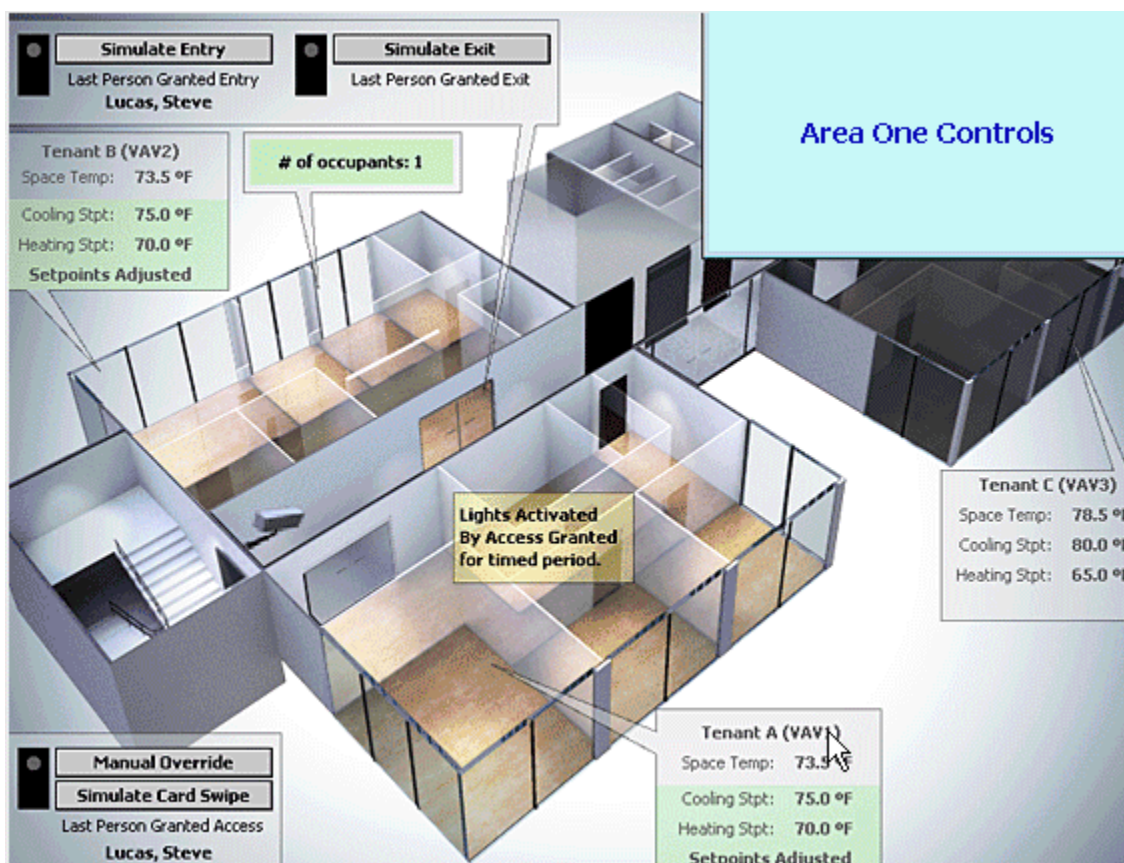
User management involves editing the default users provided by the system and creating additional users as needed. User configuration sets up credentials, authentication scheme, home page, cell phone number, and other properties.

Creating a obix user to access a station via the Obix Network is an example of setting up a machine-to-machine user. This user requires the HTTPBasicScheme and is often given the user name: obix.

## View Graphic

This view represents the inside of a building.

**Figure 124.** Example graphic view



You access this view from the Graphics view by double-clicking the Display Name record in the Graphics view

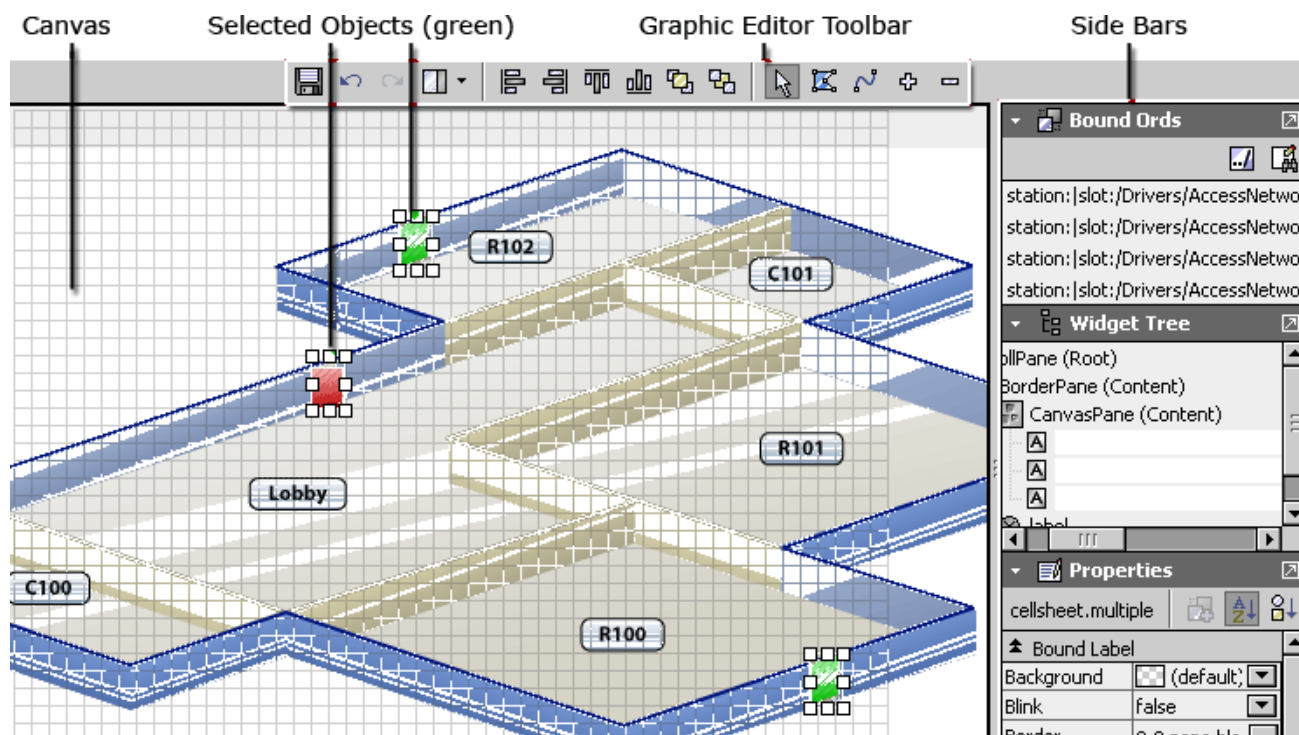
or by selecting the record and clicking the View Graphic button (  ).

You create custom graphics using the Graphics Editor view. Graphics can contain controls, links, and indicators related to building access and automation system controls. Graphics may be designed specifically for one of two **Target Media**: HxPxMedia or WorkbenchPxMedia.

## Graphic Editor view

The Graphic Editor view provides a three-dimensional canvas and properties, which you use to set up the graphic.

**Figure 125.** Graphic Editor view



You access this view from the main menu by clicking **Controller (System) Setup > Miscellaneous > Graphics >**

**Graphics Management** followed by clicking the New button (  ) or selecting an existing graphic and clicking

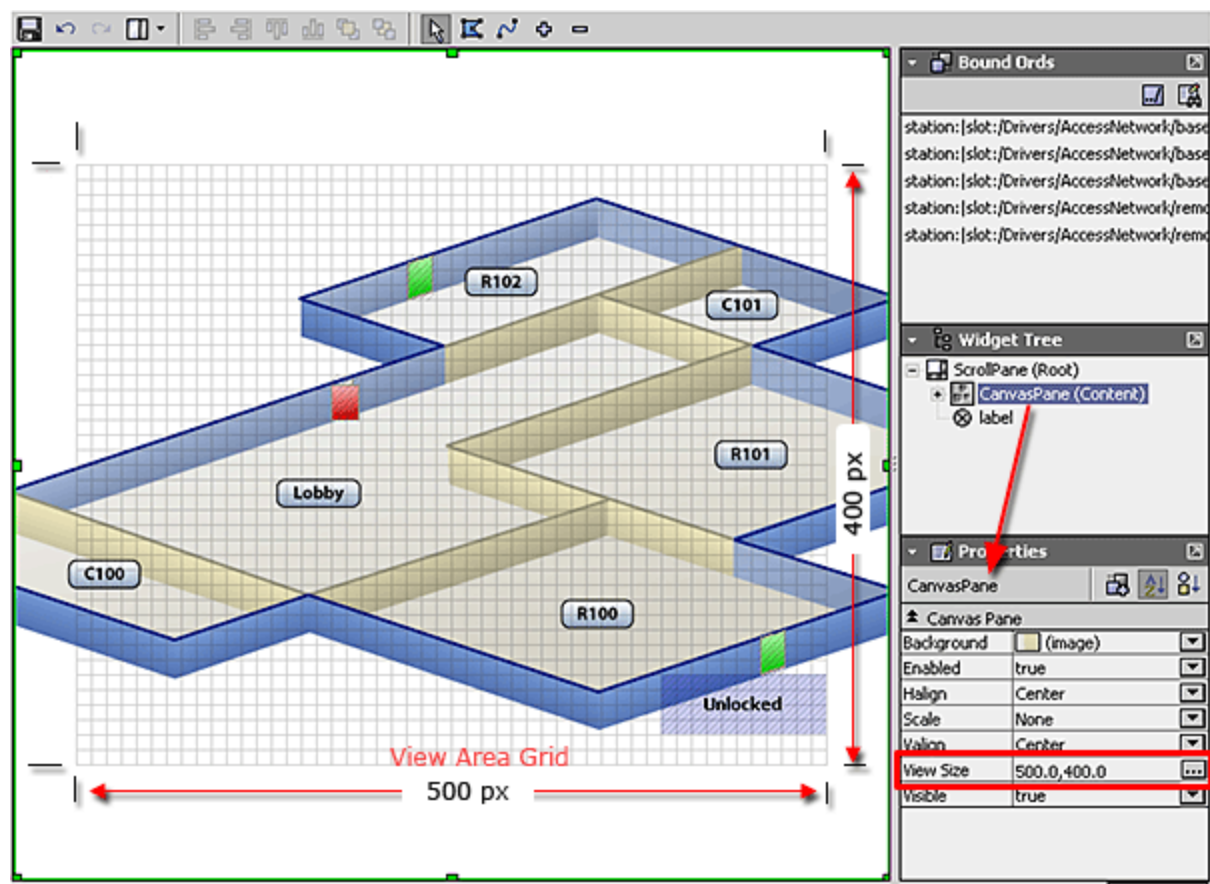
the Graphic Editor button (  )

### About the Graphic Editor canvas

The canvas is the largest area of the editor. It defines the visual boundaries of the graphic page and serves as your work area for previewing the graphic file as you develop it using the tools in the Graphic Editor.

You place widgets on the canvas and edit them and bind data to them using one or more of the side bars and additional windows, which are documented elsewhere. Most of the time, the canvas provides a live view of any widgets you add—without having to return to the Graphics Viewer. However, some graphic features may only appear in the Graphics Viewer.

Figure 126. Graphic Editor canvas



The Canvas has the following optional work aids:

- The grid provides a visual aid for graphical alignment. The grid lines display vertical and horizontal lines as well as define the visible area of the page.
- Hatching is an area of light-gray diagonal lines that define the boundaries of items that are placed on the canvas.
- View area

The view area is defined by the **View Size** property in the Canvas pane property pane. Visually, the view area is defined by the grid that displays in the editor only. The Graphic viewer clips off any part of the graphic that appears outside of the view area (when you select the view under the **Console** node of the navigation tree).

Property	Value	Description
Background	drop-down list for .png file	Selects the image of your facility to use as the background.
Enabled	drop-down list, defaults to <code>true</code>	Starts the functioning of components that make up the graphic.
Halign	drop-down list, defaults to <code>Center</code>	Aligns the background image horizontally.

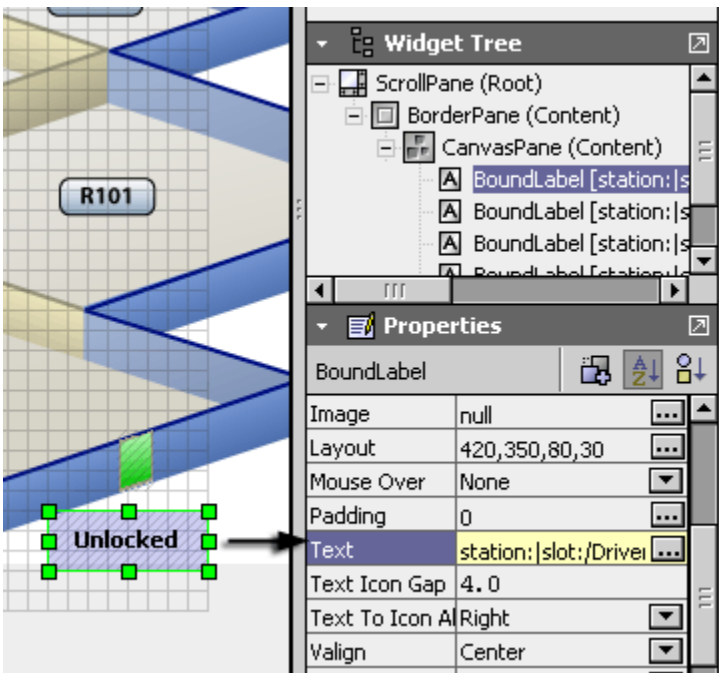
Property	Value	Description
Scale	drop-down list, defaults to <code>None</code>	Increases and decreases the background image proportionally.
Valign	drop-down list, defaults to <code>Center</code>	Aligns the background image vertically.
View Size	Chooser	Defines the dimensions of the background graphic.
Visible	drop-down list, defaults to <code>true</code>	Turns the graphic view on and off.

About Graphic Editor objects (widgets)

These objects, called widgets, represent the information to visualize in the graphic. Configuring widget properties defines the features, behaviors and appearance characteristics of widgets.

You view these properties when you right-click the canvas and select a bound label.

Figure 127. Widget properties



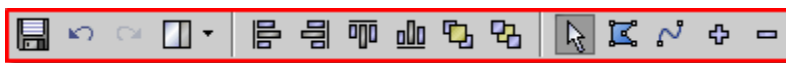
Property	Value	Description
Image	chooser (defaults to <code>null</code> )	Selects an image to include in the graphic.
Layout	chooser (pixels)	Defines the size of the graphic in pixels (picture elements).
Mouse Over	drop-down list (defaults to <code>None</code> )	Selects what to do when passing the

Property	Value	Description
		cursor over the graphic.
Padding	chooser (defaults to zero (0))	Defines space around the graphic.
Text	ORD	Identifies the location in the station of a text file.
Text Icon Gap	number (defaults to 4.0)	Defines the distance between the selected icon and the text box that describes it.
Text to Icon Alignment	drop-down list	Defines horizontal alignment: Right, Left, Center
Valign	drop-down list	Defines vertical alignment: Top, Bottom, Center

## About the Graphic Editor toolbar

This collection of buttons at the top of the view includes the **Save** and **Undo** buttons, as well as several other context-sensitive graphic alignment and drawing tools. Toolbar functions vary depending on the context. When you first open the Graphic Editor view to create a new graphic the following tools are available.

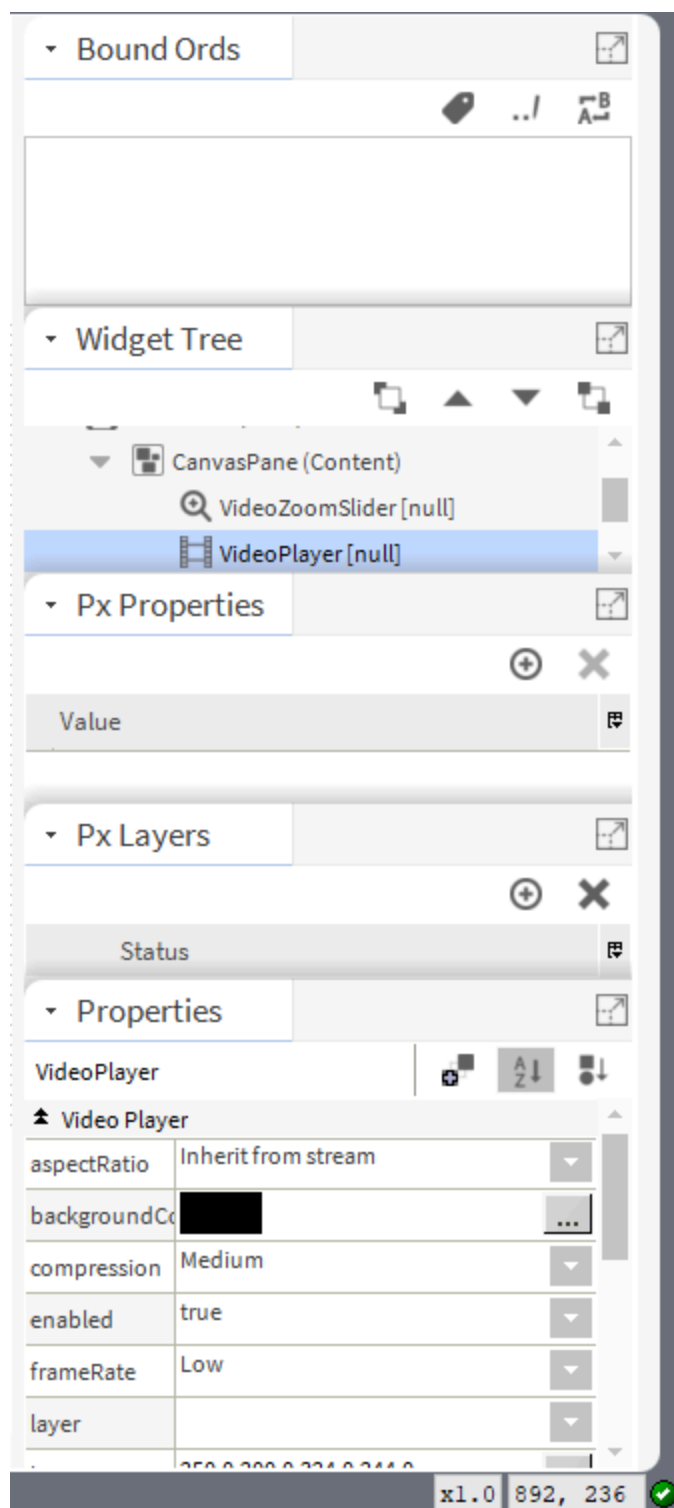
**Figure 128.** Default Graphic Editor Toolbar buttons



- Save saves the graphic in the station database.
- Undo and Redo perform the tasks their names imply.
- Right side bar menu opens a drop-down menu of side bar options for the Graphic Editor.
- Alignment options align the selected widgets and objects at their left, right, top and bottom edges.
- The To Top and To Bottom icons adjust the position of object in relationship to each other.
- Select activates the pointer tool for selecting objects.
- Add Polygon adds a square, rectangle, etc.
- Add Path allows you to draw free-form lines.
- Add Point adds a point on a line or to a polygon.
- Delete Point removes the selected point from a path or polygon.

## About the side bar pane

This pane appears on the right side of the view pane when **Show Side Bar** is selected from the **Pane** menu on the Graphic Editor Toolbar. Use this menu to hide or display individual side bars and to show or hide the Graphic Editor side bar pane. The side bars provide the properties for creating graphics.

**Figure 129.** Graphics side bar

- The Bound ORD side bar lists all the bound ords in the current graphic. An ORD is the path to the data, which the graphic displays.
- The Widget Tree displays the hierarchy of widgets (panes, labels, graphic elements, and so on) in the



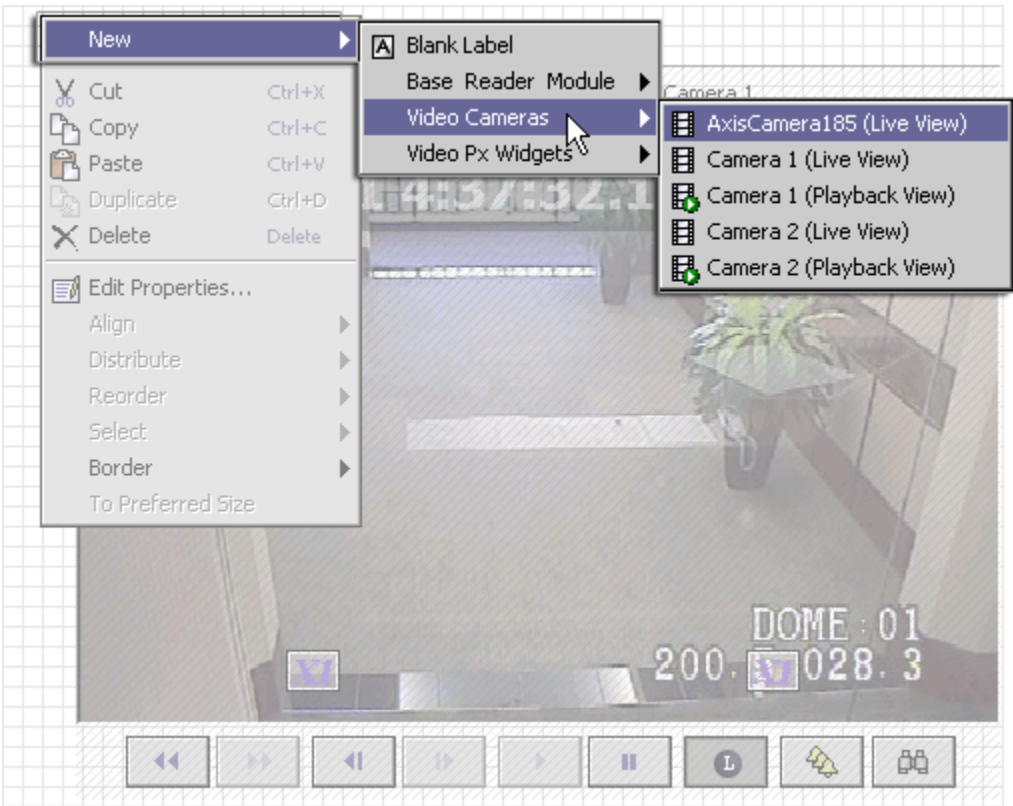
current Px view.

- Px Properties relate to the specific widget.
- Px Layers group objects in the Px Editor.
- Properties populate based on the type of widget.

Graphic Editor pop-up menu - available video cameras

This popup (right-click) menu includes context-sensitive menu items.

**Figure 130.** Graphic Editor popup menu - available video cameras



**Figure 131.** New menu items

Menu item	Description
Blank Labels	Selects a standard Px label widget, which you use to annotate the graphic.
Base Reader Module, Remote Reader Module	These menus are context sensitive and list widgets that represent the devices available under each module. Adding one to the graphic adds a representation of the device to the graphic.
Video Cameras	This list of widgets represents the camera(s) connected to your

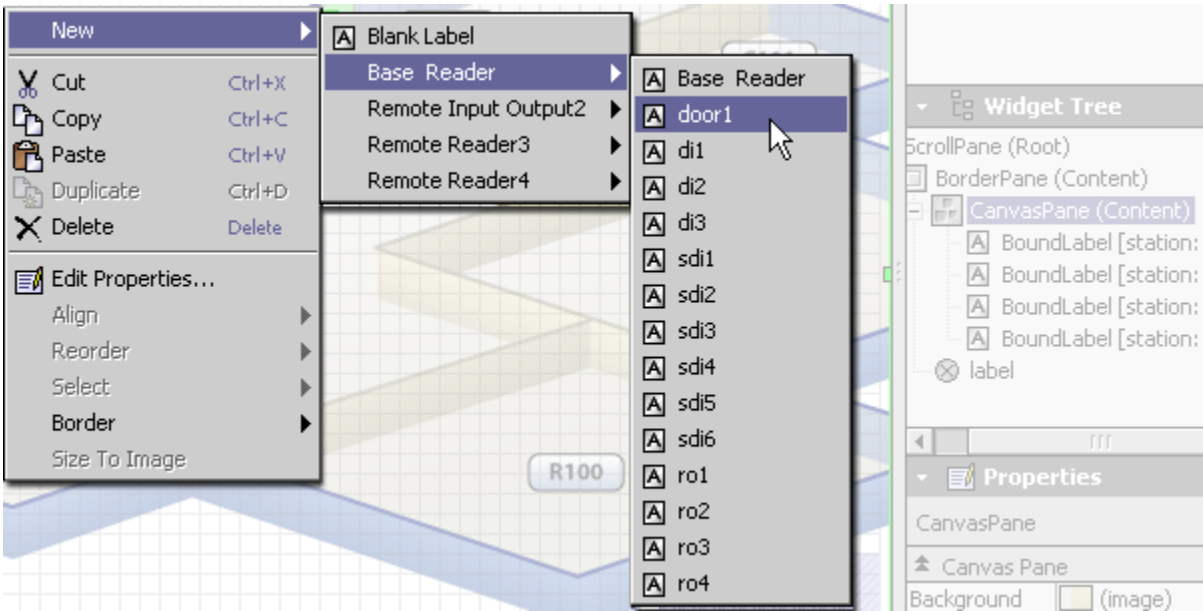
Menu item	Description
	Supervisor PC or subordinate controller. Each widget is labeled in the menu to indicate that the device it represents is either used to play back prerecorded video or to display live video. The playback icon also identifies playback widgets in the menu.
Video Px Widgets	A Supervisor station can support local or remote video graphics (using Px) and have them served by cameras that are attached to remote stations under the Supervisor's NiagaraNetwork. The following Px widgets support remote video:Live Video PlayerControl PanelPan Tilt JoystickZoom SliderCamera WidgetMouse Down WidgetVideo Multistream Pane

Refer to the “Video installation” chapter in the *Niagara Enterprise Security Installation and Maintenance Guide* for more about video devices and video.

Example: new Base Reader

The following is an example of the popup menu, Base Reader menu items.

Figure 132. Graphics Editor popup menus



The popup menu also provides many other context-sensitive commands, including the ability to add a border pane to a selected object.



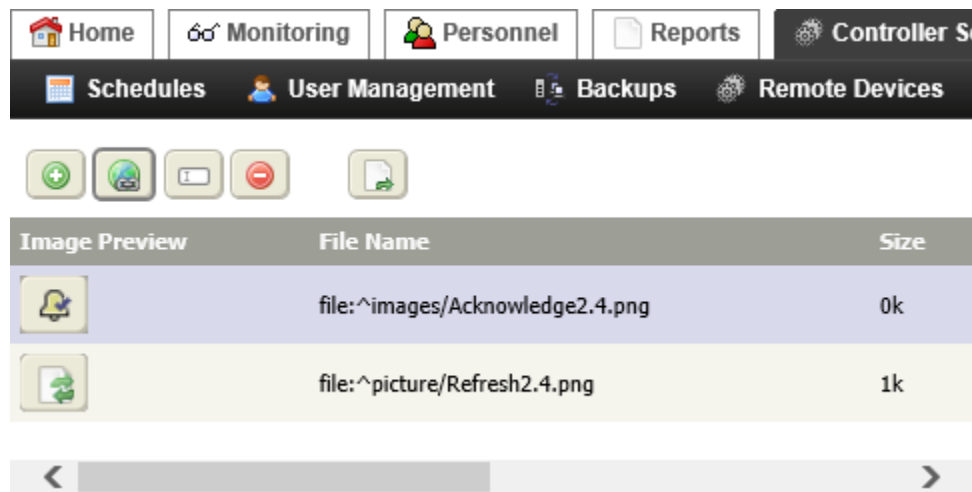
**NOTE:** If you add a door that is in an alarm condition, by default, the door blinks until the door is out of alarm and the alarm is acknowledged.

Images view

This view lists all the images available on the local station. These images are the artifacts to make the graphic look like your building. You can have a graphics artist draw these artifacts.

Buttons

Figure 133. Images view



This view displays when you select Images from the Controller (System) Setup > Miscellaneous > Graphics from the main menu.

The control buttons at the top of the view provide standard controls, including an Add control button () at the top of the view for adding a new image.


Columns


Column	Description
Image Preview	Provides a thumb-nail view of the image.
File Name	Identifies the name of the image file.
Size	Indicates the size of the image file.

Add New Image view

The properties in this view provide a way for you to add image files to a designated location on the controller (an images folder, by default). Images that are loaded on the controller are available for use in graphic views.

Figure 134. Add New Image view

 Save

 Images

File Path

File to Upload

Browse...

Property	Value	Description
File Path	file_path (defaults to ^images)	Defines the folder under the station for storing uploaded image files. The ^ character specifies the station root directory. If you change the file path, the station creates the directory on the controller at the designated location.
File to Upload	File chooser	Provides a way to browse to and select the desired image for transferring to the controller.

Display Image view


This view displays when you click the Hyperlink control button (  ) in the Images view. The view displays the file path as the view title directly above a link to the Images view. The single, selected image displays in the view.

Figure 135. Display Image view

file:^graphics/edit.png

 Images



Navigation Groups view

Nav Groups are custom menu items used to collect and organize graphic views. Once a nav group is created, you may assign child views to the group.

Figure 136. Navigation Groups view

Home

Monitoring

Personnel

Reports

Controller Setup

Threat Levels

Schedules

User Management

Backups

Remote Devices

Access Setup

Intrusion Setup

Display Name	Nav Name	Parent Path	Index
Daily Reports	Daily Reports	/	0
Welcome Guest	Welcome Guest	/	0
test	test	/monitoring	0

You access this view by expanding **Controller (System) Setup > Miscellaneous > Graphics** and clicking **Navigation Groups**.

A nav group displays in the menu under its assigned parent. This view displays a table of all the navigation groups that are available on the local station. This view is also where you initiate the process of adding a new navigation group using the Add control button at the top of the view.

### Add New (or edit) Nav Group view

This view configures Nav group properties.

Figure 137. Add New Nav Group view

Save

Nav Groups

Nav Group

Nav Name

Display Name

Parent Path

Home

Icon

module://icons/x16/folder.png

Index

0

You access this view from the main menu click **Controller (System) Setup > Miscellaneous**, expand the **Graphics** menu and click **Navigation Groups**.

Property	Value	Description
Nav Name	text	Defines an identifier for the nav group. This name appears in the menu if no <code>Display Name</code> is specified. You may want to use this property for a design-logical name and use the <code>Display Name as</code> a more user-friendly name.
Display Name (BFormat general)	text	<p>Defines a BFormat string used to format text by using values obtained from objects.</p> <p>You specify this string as normal text with embedded scripts identified by the percent (%) character. The driver maps calls within the script to an object's methods. Use the dot operator (.) to chain calls. To insert a percent symbol itself, use two percent symbols (%%).</p> <p>For examples, click the question mark icon next to this property.</p>
Parent Path	drop-down list	<p>Defines where in the hierarchy to place a new menu item. A hierarchy of options matches the current navigation structure. You can choose the menu or submenu here to specify where, in the overall system navigation hierarchy, to place your new menu item.</p> <p>For example, to place a menu item under the Remote Devices submenu, choose the Remote Devices option in this property.</p>
Icon	path	Defines where the icon used for this column is located.
Index (Snmpp)	number	Displays the value that corresponds to the column index of the object created for it in the Input or Output Table.

# Chapter 7. Controller (System) Setup–Backup views

These views manage Supervisor station and controller station backups.

Controllers and Supervisors have different backup views. Both views function in slightly different ways to create and manage backup files. The primary difference between them is that the Supervisor backup view can back up all subordinate stations, and the local Supervisor station, whereas, a controller can only back up its local station.

The following table identifies the primary differences between the two views:

Feature	Controller	Supervisor
Local Backup function	x	x
Restore function	x	x
Recent Backup History tab	x	x
System Backup function		x
Backup Schedule tab		x
Backup Archive tab		x

Another difference between Supervisor and controller backups involves the archive that results from making a backup. Archive files made from a Supervisor and subordinate stations have a \*.zip file extension. Local archives made from a single controller station have a .dist extension.

## Backups view

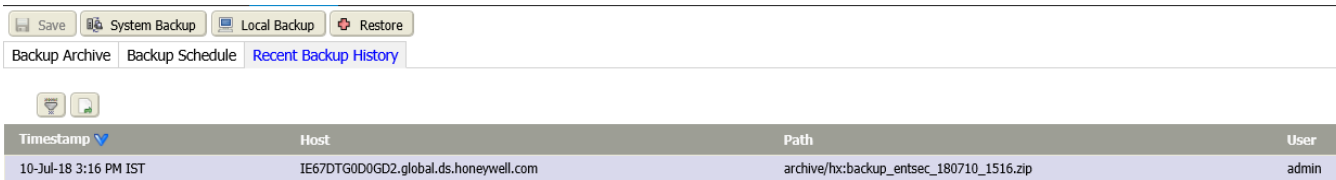
This view opens to the Backups tab, which lists the system and individual station backup files that have been created. You can use this view to initiate a backup job at any time. This view also provides a restore function. The views are slightly different between Supervisor and controller backups.

### Backup Archive columns

Column	Description
File Name	Displays the archived file name and path location. <b>NOTE:</b> Only files located under the default <code>station/backups</code> directory are displayed in this table. Backup files that you save to other locations are not displayed here.
Timestamp	Displays the date and time that the backup was saved.
Backup Type	Indicates what is in the backup file: <ul style="list-style-type: none"><li>Local: includes a Supervisor station only</li><li>System: includes a Supervisor and its subordinate stations</li></ul>
Size	Indicates the backup file size.

Controller backups

Figure 138. Controller Backups view



This view opens only when you select **Controller Setup > Backups** from the main menu of a controller station.

Buttons

The primary buttons are located below the view title at the top of the view:

- **Local Backup** initiates a manual backup of the local Supervisor station.
- **Restore** initiates a job to return all station data to the data stored in a previous backup.

Columns

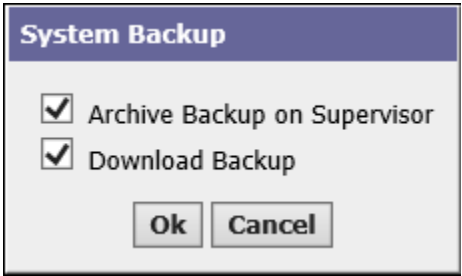
Table 46. Backup Archive columns

Column	Description
Timestamp	Displays the date and time that the backup was saved.
Host	Reports the host's IP address.
Path	Reports the path to the backup distribution (dist) file.
User	Identifies the person who made the backup.

System Backup/Local Backup window

This window provides Supervisor backup options.

Figure 139. Example of a System Backup window



This window opens when you click the **System Setup > Backups**, followed by clicking the **System Backup** or **Local Backup** button. The only difference between the **System Backup** and **Local Backup** windows is the window title.

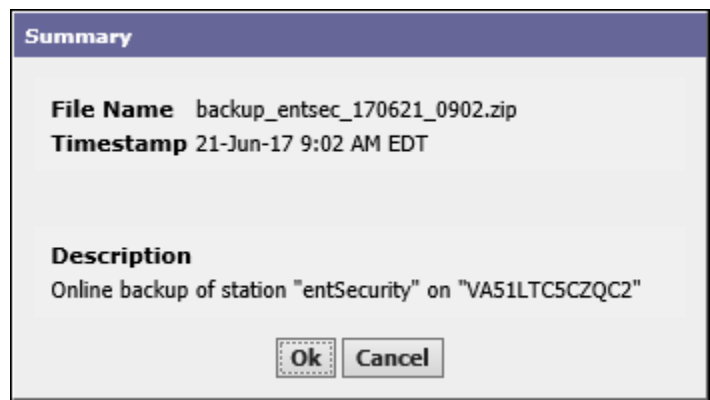
Property	Value	Description
Archive Backup on Supervisor	check box	Saves the backup file to a backups

Property	Value	Description
		folder under the <code>station</code> folder. If this folder does not exist, the system automatically creates it. The Backup Archive tab lists the backups stored in this folder.
Download Backup	check box	Windows-based systems saves the backup file in <code>Downloads</code> folder from where you can move it to another location.

Backup Archive tab Summary window

This windows provides summary information for a specific backup.

Figure 140. Supervisor backups Summary window




This window opens when you select a backup row in the Backups view and click the Summary button ().

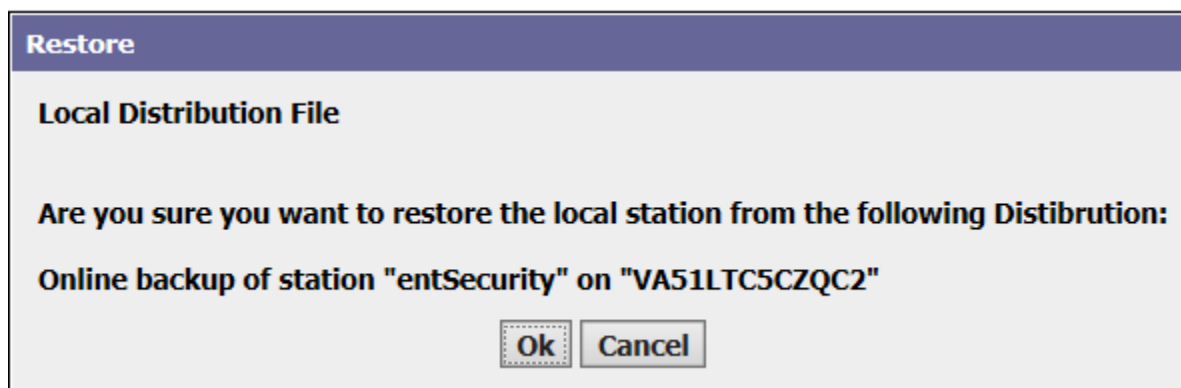
Table 47. Summary properties


Property	Description
File Name	Identifies the backup file name.
Timestamp	Reports when the backup was created.
Description	Provides additional information.

Backup Archive tab Restore windows

You may need to restore a station if data are corrupted or an error occurred. The Backup feature presents two Restore windows depending on the origin of the backup file.

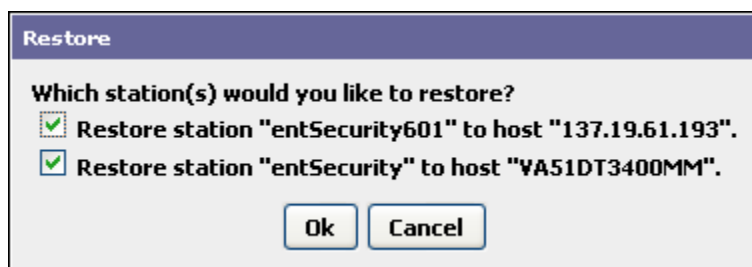
## Restore window — Supervisor


**Figure 141.** Restore window

This window opens when you navigate to **System Setup > Backups**, select a Supervisor station backup and click the Restore button (  ). It asks you to confirm the restoration to the local Supervisor station.

## Restore window — remote host

This window lists the backup files that are available to restore the station in a remote host (controller platform).

**Figure 142.** Restore window

This window opens when you navigate to **System Setup > Backups**, select a host station backup and click the Restore button (  ). It lists all the available backup files from which you may choose the file to restore to the remote host station. These files are stored in the Supervisor PC's `!backups` folder.

## Backup Schedule tab

This tab associates a schedule with the backup function. It is only available to a Supervisor station.

Scheduled backups occur when the attached schedule's output property transitions from a `false` to a `true` state. Performing a regular backup job is an important best practice.



Figure 143. Backup Schedule tab

Save

System Backup

Local Backup

Restore

Backup Archive

Backup Schedule

Recent Backup History

System Backup Schedule

None

»

Local Backup Schedule

None

»

Scheduled System Backup Limit

10

[1 - +inf]

Scheduled Local Backup Limit



10

[1 - +inf]

Alarm Info

Alarm Source Info »

You access this tab by clicking **System Setup > Backups**, followed by clicking the Backup Schedule tab.

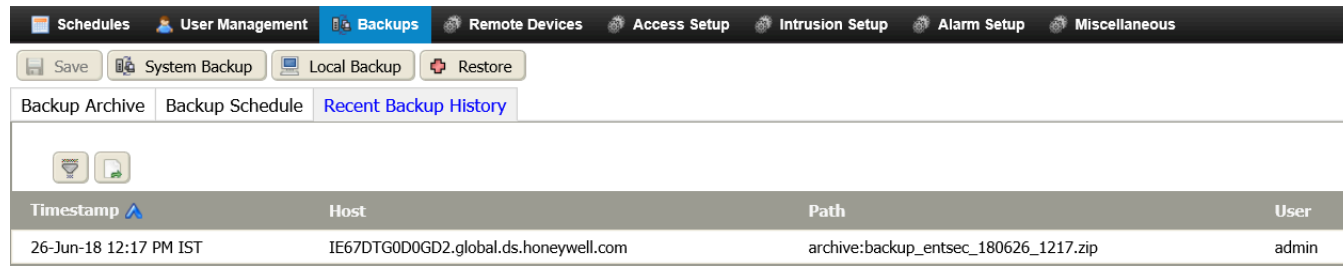
Property	Value	Description
System Backup Schedule	Ref Chooser	Assigns a schedule for system-type backups. When a schedule is assigned in this property you can click on the associated schedule icon  to navigate to the Edit Schedule view.
Local Backup Schedule	Ref Chooser	Assigns a schedule for local-type backups. When a schedule is assigned in this property you can click on the associated schedule icon  to navigate to the Edit Schedule view.
Scheduled System Backup Limit	number between one (1) and infinity; defaults to 10	Specifies the maximum number of scheduled System backups that are allowed. After this number is reached, subsequent backups are "rolled" so that the new backup overwrites the oldest existing backup.
Scheduled Local Backup Limit	number between one (1) and infinity; defaults to 10	Specifies the maximum number of scheduled Local backups that are allowed. After this number is reached, subsequent backups are "rolled" so that the new backup overwrites the oldest existing backup.
Alarm Source Info	additional properties	Links to a set of properties for

Property	Value	Description
		configuring and routing alarms. These properties are documented in the <i>Alarm Setup</i> topic of the PDF and in the help system (search for Alarm Source Info).

Recent Backup History tab

This tab displays a table of all the backup jobs run by the station. It is available on both the Supervisor and local station versions of the Backups view.

Figure 144. Recent Backup History tab



This view opens when you click the Recent Backup History tab on the Backups view.

Standard Filter (   ) and Export (  ) control buttons are provided.

Columns

Table 48. Recent Backup History columns

Column	Description
Timestamp	Identifies when the backup was saved.
Host	Identifies the host platform.
Path	Identifies the path where the backup is located.
User	Identifies the user who made the backup.

Recent Backup History tab Filter window

This window configures search criteria for limiting the number of backup files in the list.

Filter

☐ Timestamp

Time Range 

?

 to 

?

 >>

☐ Host

%

Must Include

☒ Case Sensitive

☐ Path

%

Must Include

☒ Case Sensitive

☐ User


%

Must Include

☒ Case Sensitive

Ok

Cancel

This window opens when you click the Filter button () on the Recent Backup History tab of the Backups view.

Criterion	Value	Description
Timestamp	drop-down list and Time chooser	Sets up start and end dates and times, days of the week or a schedule to use as filter criteria.
Host	wild card (%)	Sets up the host name as a criterion.
Path	wild card (%)	Sets up the path as a criterion.
User	wild card (%)	Sets up the associated user name (admin, operator, etc.) as a criterion.

### Restore from Backup Distribution File or System Backup File views

This view restores one or more station \*.dist backup files. It functions the same in a standalone controller and in a Supervisor station.

Figure 145. Supervisor Restore window

Home

Monitoring

Personnel

Reports

Controller Setup

Threat Level

Schedules

User Management

Backups

Remote Devices

Access Setup

Save

Restore Options

File

C:\Users\E522605\Documents\docEnterprise

Browse...

**NOTE:** Supervisor station backups that include more than one station are saved in a .zip file.

This view opens in a Supervisor or controller station when you click **Controller (System) Setup > Backups**,

followed clicking the **Restore** button. You do not have to select a file from the list.

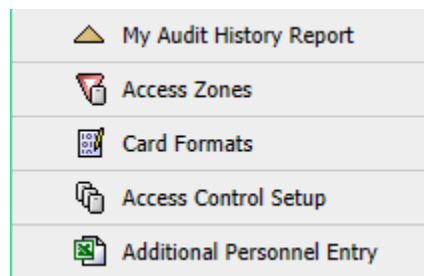
A single **Save** button is at the top of the view under the title.

A single property on the Restore Options tab, **File**, defines the backup file to restore. This property includes the path to the selected archive file. When you click in the **File** property, or click the **Browse** button, a file chooser window opens. Use it to browse to and select the file (\*.dist).

# Chapter 8. Controller (System) Setup–Access Setup

These views, tabs and windows configure areas within a building for the purpose of managing who may enter. These topics also document card reader formats and additional personnel data.

Figure 146. Access Setup menu



## Access Zones views

A defined access zone controls and monitors the entry and exit of personnel assigned to the zone, manages the occupancy levels for the zone, and configures anti-passback controls based on occupancy and the time of day.

### Buttons



Figure 147. Access Zones view

Zone Name	Station Name	Fallback Enforcement
Lobby	entSecurity801	Off

This view opens when you click **Controller (System) Setup > Access Setup > Access Zones** in a remote host. It includes a tabular display of all existing access zones, including zones from all peer and subordinate stations.

- You cannot add or edit an access zone from a Supervisor view. To add or edit, use the controller station Access Zone views.
- From a Supervisor, you can see all system-wide access zones after you join and replicate subordinate controller zones.
- To view the detailed configuration (doors, entry readers, exit readers, and other devices) of an individual access zone, you must connect to the controller directly.
- Using the Grouping tab of a specific access zone view, you can join entry and exit stations into a single access zone.

In addition to the standard control buttons (Summary, Delete, Rename, Filter, Column Chooser, Refresh, Manage Reports, and Export), these buttons provide specific access features:

-  Add creates a new access zone. The view it opens defines activity alert extensions, occupants, supervisors, entry readers, exit readers, and groups.
-  Hyperlink opens the access zone summary view.

Columns

Table 49. Access Zone columns

Column	Description
Zone Name	Displays the name of the Access Zone.
Station Name	Displays the name of the primary station associated with the Access Zone. It is possible to have card readers from more than one station in a company-wide access zone.
Fallback Enforcement	Displays the current state of fallback enforcement (Off, Soft, or Hard) that is assigned for the displayed zone.

Add New (or edit) Access Zone view

This view creates or edits new access zones one zone at a time.

Links

Figure 148. Access Zone view/tab

Display Name

Access Zone

Summary	Access Zone	Activity Alert Exts	Occupants	Supervisors	Entry Readers	Exit Readers	Grouping
Occupancy Count	0 {ok}						
Occupied	false {ok}						
Lock Down	false						
Occupancy Criteria	Any						
Passback Mode	Hard						
Above High Threshold Enforcement	Off						
At High Threshold Enforcement	Off						
Below Low Threshold Enforcement	Off						
At Low Threshold Enforcement	Soft						
Supervisor Required Enforcement	Off						
Pending Time	00 m 15 s [10secs - 1min]						
Passback Timeout	00000 h 00 m 00 s [0ms - 1day]						
Reset Occupancy Enabled	false						
Reset Occupancy Time	12 :00 AM EDT						
High Threshold	100						
Low Threshold	-1						

This view opens from the main menu of a remote host when you click **Controller (System) Setup > Access**

**Setup > Access Zones**, followed by clicking the Add button () in the Access Zones view.

To edit an existing access zone record, double-click a row in the Access Zones view, and click the Access Zone tab.

The **Save** link in the top left corner of the view saves changes to the station database. The **Access Zones** link returns to the Access Zones view.

### Access Zone tab properties

Property	Value	Description
Display Name	text	Provides a unique name for the zone.
Occupancy Count	read-only	Displays the number of personnel currently in the zone.
Occupied	read-only	Indicates if the access zone is currently occupied.
Lock Down	true or false (default)	<p>Enables and disables a lock down, which prohibits immediate access to the zone regardless of how the enforcement rules are configured:</p> <p>false allows normal operation.</p> <p>true disables (locks down) the zone.</p>
Occupancy Criteria	drop-down list (defaults to Any)	<p>Keeps track of who is in the zone:</p> <p>Any counts all personnel, including supervisors. This option applies no criteria regarding who must be present.</p> <p>Supervisors indicates that a supervisor (person) must be present.</p>
Passback Mode	drop-down list (defaults to Hard)	<p>Determines how to handle passback activity alerts. Personnel who leave an access zone and return to the zone are said to pass back to the zone. This property can limit their ability to return to the zone:</p> <p>Off disables passback mode, which allows personnel to exit and return as often as they wish.</p> <p>Soft grants return access again to the zone, but generates an</p>

Property	Value	Description
		alarm.  <b>Hard</b> denies return access to the zone and generates an alarm.
Above High Threshold Enforcement	drop-down list (defaults to <b>Off</b> )	Specifies the type of enforcement to use when occupancy exceeds the high threshold setting:  <b>Off</b> disables above-high-threshold enforcement.  <b>Soft</b> allows access and generates an alarm.  <b>Hard</b> denies access and generates an alarm.
At High Threshold Enforcement	drop-down list (defaults to <b>Off</b> )	Specifies the type of enforcement to use when occupancy meets the high threshold setting:  <b>Off</b> disables enforcement.  <b>Soft</b> grants access and generates an alarm.
Below Low Threshold Enforcement	drop-down list (defaults to <b>Off</b> )	Specifies the type of enforcement to use when occupancy falls below the low threshold setting:  <b>Off</b> disables below-low-threshold enforcement.  <b>Hard</b> grants access and generates an alarm.
At Low Threshold Enforcement	drop-down list (defaults to <b>Off</b> )	Specifies the type of enforcement to use when occupancy meets the low threshold setting:  <b>Off</b> disables below-low-threshold enforcement.  <b>Soft</b> grants access and generates an alarm.
Supervisor Required Enforcement	drop-down list	Denies access to all non-supervisory persons unless a supervisor is already an occupant.









Property	Value	Description
		<p><b>Off</b> disables the requirement for a supervisor.</p> <p><b>Soft</b> requires a supervisor. Grants access even though a supervisor is not present but generates an alarm.</p> <p><b>Hard</b> denies access when a supervisor is not present and generates an alarm.</p>
Pending Time	minutes, seconds	Defines the time allowed for a second person to swipe a badge to prevent a threshold alarm. If a second badge is not swiped in the specified time, the system generates an occupancy alarm and may deny access.
Passback Timeout	hours, minutes, seconds	Specifies a time (timeout) after which a badge may be re-scanned at the reader without causing a passback alarm.
Reset Occupancy Enabled	true or false (default)	Clears the zone of people who did not scan their badges when they left the building. This prepares the zone so that people can enter again in the morning. You may reset occupancy at night or when you know that no one is actually in the zone.
High Threshold	number (defaults to 100 )	Defines the maximum number of occupants allowed in an access zone.
Low Threshold	number (defaults to -1 )	Defines the minimum number of occupants allowed in an access zone.

### Add new Access Zone Summary tab

This tab is present, but does not display updated information until you create an access zone. This view may also include a context-appropriate list of floors, people and card readers that are associated with the access zone.

**Figure 149.** Add New Access Zone Summary tab

<b>Summary</b>	Access Zone	Activity Alert Exts	Occupants	Supervisors	Entry Readers	Exit Readers	Grouping
----------------	-------------	---------------------	-----------	-------------	---------------	--------------	----------

 Mapped Ord: **Station Unavailable**  
 Type:  Access Zone  
 Zone Name:  
 Station Name:  
 Fallback Enforcement: Soft

To access this view, click **Controller Setup > Access Setup**, followed by double-clicking an existing access zone in the Access Zones view, and clicking the Summary tab.









Property	Description
Mapped Ord	Links the to the Access Zone view for the access right.
Type	Identifies the record as defining an access zone.
Zone Name	Reports the name of the access zone.
Station Name	Reports the name of the station under the control of which the event occurred.
Fallback Enforcement	Reports the current state of fallback enforcement ( <i>Off</i> , <i>Soft</i> , or <i>Hard</i> ), which is assigned to the zone.
Occupancy Count	Reports the number of people currently in the access zone.

### Access zone Activity Alerts Ext tab

This tab configures what happens when an access event triggers an alert. It includes configuring video for each alert.

**Figure 150.** Activity Alert Exts on a reader

<b>Display Name</b> <input type="text" value="Access Zone"/>	
Summary	Access Zone <b>Activity Alert Exts</b>
Occupants	Supervisors
Entry Readers	Exit Readers
Grouping	

<b>Anti Passback Violation Alert</b>	<b>Alarm Class</b> <input type="text" value="Medium"/>	 Video Setup	<input checked="" type="checkbox"/> <b>Enable Logging</b>
<b>Access Zone Disabled Alert</b>	<b>Alarm Class</b> <input type="text" value="Medium"/>	 Video Setup	<input checked="" type="checkbox"/> <b>Enable Logging</b>
<b>Occupancy Violation Alert</b>	<b>Alarm Class</b> <input type="text" value="Medium"/>	 Video Setup	<input checked="" type="checkbox"/> <b>Enable Logging</b>
<b>Supervisor Required Alert</b>	<b>Alarm Class</b> <input type="text" value="Medium"/>	 Video Setup	<input checked="" type="checkbox"/> <b>Enable Logging</b>
<b>Granted But Anti Passback Violation Alert</b>	<b>Alarm Class</b> <input type="text" value="Medium"/>	 Video Setup	<input checked="" type="checkbox"/> <b>Enable Logging</b>
<b>Granted But Occupancy Violation Alert</b>	<b>Alarm Class</b> <input type="text" value="Medium"/>	 Video Setup	<input checked="" type="checkbox"/> <b>Enable Logging</b>
<b>Granted But Access Zone Disabled Alert</b>	<b>Alarm Class</b> <input type="text" value="Medium"/>	 Video Setup	<input checked="" type="checkbox"/> <b>Enable Logging</b>
<b>Granted But Supervisor Required Alert</b>	<b>Alarm Class</b> <input type="text" value="Medium"/>	 Video Setup	<input checked="" type="checkbox"/> <b>Enable Logging</b>

You access this tab from the main remote host menu by clicking **Controller Setup > Access Setup > Access**

**Zones**, followed by creating a new zone or double-clicking an existing zone and clicking the Activity Alert Ext tab.

### Alerts

Alert	Description
Anti Passback Violation Alert	Configures what to do when <b>Passback Mode</b> on the Access Zone tab is set to <b>Hard</b> and someone has attempted to re-enter the zone after leaving the zone.
Access Zone Disabled Alert	Configures what to do when <b>Lock Down</b> on the Access Zone tab is set to <b>true</b> , and an attempt has been made to enter the zone.
Occupancy Violation Alert	Configures what to do when the maximum occupancy as defined by <b>High Threshold</b> on the Access Zone tab has been reached, and someone has been prevented from entering the zone.
Supervisor Required Alert	Configures what to do when <b>Occupancy Criteria</b> on the Access Zone tab is set to <b>Supervisor</b> , and no supervisor has entered the zone.
Granted But Anti Passback Violation Alert	Configures what to do when <b>Passback Mode</b> on the Access Zone tab is set to <b>Soft</b> and someone has re-entered the zone after leaving the zone.
Granted But Occupancy Violation Alert	Configures what to do when the maximum occupancy as defined by <b>High Threshold</b> on the Access Zone tab has been reached, and someone has entered the zone.
Granted but Access Zone Disabled Alert	Configures what to do when <b>Lock Down</b> on the Access Zone tab is set to <b>true</b> and someone has left the zone.
Granted but Supervisor Required Alert	Configures what to do when <b>Occupancy Criteria</b> on the Access Zone tab is set to <b>Supervisor</b> and no supervisor has entered the zone.

### Properties

Property	Value	Description
Alarm Class	text	Defines alarm routing options and priorities. Typical alarm classes include <b>High</b> , <b>Medium</b> and <b>Low</b> . An alarm class of <b>Low</b> might send an email message, while an alarm class of <b>High</b> might trigger a text message to the department manager.
Video Setup	button	Opens the Video Setup window. Refer to <i>Video Setup window</i> in the <i>Controller (System) Setup–Alarm Setup</i> chapter.
Enable Logging	check box (defaults to checked)	Disables logging to the activity log (when the check mark is removed).

### Related reference

- [Video Setup window](#)
- [Controller \(System\) Setup–Alarm Setup](#)

### Occupants tab

This tab displays a list of all people currently occupying the access zone. Using a discover process, you can use this view to manually add or remove people from the access zone. It is always available in the access zone views, but the information it provides is based on settings from the access zone master station.

Buttons




Figure 151. Occupants tab



**NOTE:** The Occupants tab does not display in a Supervisor station.

You access this tab from the main menu by clicking **Controller Setup > Access Setup > Access Zones**, followed by creating a new zone or double-clicking an existing zone and clicking the Occupants tab.

The buttons in this view provide standard features (Summary, Filter, Export and Discovery). In addition, these buttons provide occupancy-related features:

-  Delete removes the selected person from the access zone, Newly Assigned pane.
-  Add moves a discovered person’s record from the Unassigned pane to the Newly Assigned pane.
-  Hyperlink in either pane opens the **Personnel > People Summary** tab for the selected person.

Columns

Table 50. Occupants columns






Column	Description
Last Name	Identifies the last name of the occupant.
First Name	Identifies the first name of the occupant.
Department	Identifies the occupant’s department.
Person Type	Identifies the type of person.
Tenant Name	Identifies the name of the building tenant.

Access Zone Supervisors tab

This tab assigns and unassigns a person (department supervisor) to the current access zone. It is always available in the access zone views, but the information it contains is based on settings from the access zone master station.

Buttons




Figure 152. Access Zone Supervisors tab

Summary	Access Zone	Activity Alert Exts	Occupants	Supervisors	Entry Readers	Exit Readers	Grouping	
Newly Assigned								
<div></div>								
Last Name	First Name	Department	Person Type	Tenant Name				
Sanders	Randy			A Company				

In a remote controller, you access this tab by navigating to **Controller Setup > Access Setup > Access Zones**, followed by creating a new zone or double-clicking an existing zone and clicking the Supervisors tab.

- This tab is available when you are connected to the master controller station. The controllers pass access zone information to a Supervisor station, as appropriate, but entry and exit readers may not be configured and are not visible from the Supervisor.
- Only stations that are joined in a peer role relationship are available for grouping.

The buttons in this view provide standard features (Summary, Filter, Export and Discovery). In addition, these buttons provide supervisor-related features:

-  Delete removes the selected person from the Newly Assigned pane. This person is no longer designated as a supervisor.
-  Add moves the selected person from the Unassigned pane to the Newly Assigned pane. This designates the selected person as a supervisor.
-  Hyperlink in either pane opens the **Personnel > People Summary** tab for the selected person.

Columns

Except for the title, this tab contains the same columns as does the Occupants tab.

Table 51. Supervisors tab columns

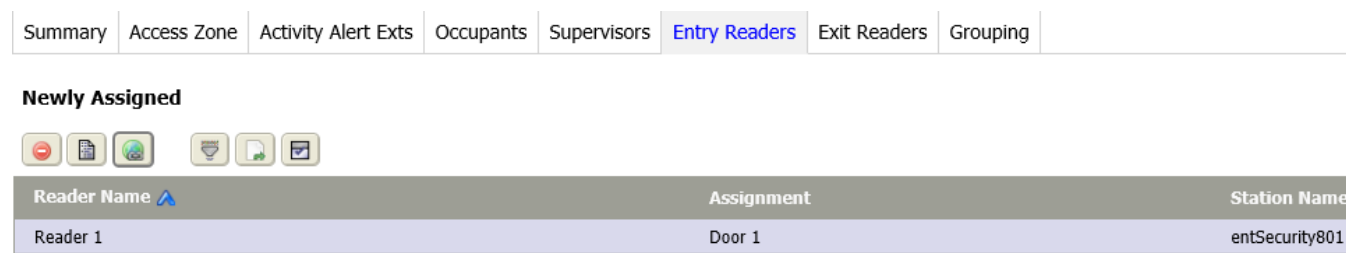
Column	Description
Last Name	Identifies the last surname of the supervisor.
First Name	Identifies the first given name of the supervisor.
Department	Identifies the organizational group to which the supervisor belongs.
Person Type	Reports the value of the Person Type property associated with the person’s personnel record.
Tenant Name	Reports the value of the Tenant property associated with the person’s personnel record.

Entry Readers tab

This tab displays the local card readers connected to this controller, which are used to enter the access zone. You can only add readers to access zones when you are connected to the reader’s assigned remote station. Readers are not visible and cannot be configured from remotely-grouped stations.

Buttons

Figure 153. Entry Readers tab






You access this tab from the main menu of a remote host station by clicking **Controller Setup > Access Setup > Access Zones**, followed by creating a new zone or double-clicking an existing zone and clicking the Entry Readers tab.

**NOTE:** In a company-wide system, entry readers are available from more than one controller.

Remote stations pass entry reader information to a Supervisor station, as appropriate, but you cannot configure these readers, nor are they visible from the Supervisor station.

The buttons in this view provide standard features (Summary, Filter, Export and Discovery). In addition, these buttons provide entry-reader-related features:

-  Delete removes the selected entry reader from the Newly Assigned pane.
-  Add moves the selected entry reader from the Unassigned pane to the Newly Assigned pane.
-  Hyperlink in either pane opens the Summary tab for the selected entry reader.

Columns

Table 52. Entry Readers columns

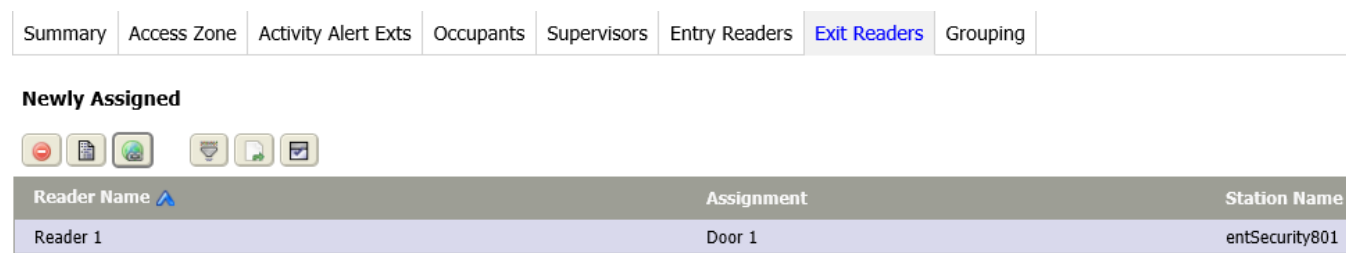
Column	Description
Reader Name	Identifies the name of the entry reader.
Assignment	Identifies the name of the door to which the entry reader is attached.
Station Name	Identifies the remote host station name that manages the door and entry reader.

Exit Readers tab

This tab provides a way to manually assign or unassign exit readers to the current access zone. It displays only local exit readers. You can only add readers to access zones when you are connected to the reader’s assigned station. Readers are not visible, nor can they be configured from remotely-grouped stations.

Buttons

Figure 154. Exit Readers tab






You access this tab from the main menu by clicking **Controller Setup > Access Setup > Access Zones**, followed by creating a new zone or double-clicking an existing zone and clicking the Exit Readers tab.

**NOTE:** In a company-wide system, exit readers are available from more than one controller.

The remote station passes exit reader information to a Supervisor station, as appropriate, but exit readers cannot be configured, nor are they visible from the Supervisor station.

Except for the title, this tab contains similar information to that contained in the Entry Readers tab.

The buttons in this view provide standard features (Summary, Filter, Export and Discovery). In addition, these buttons provide entry-reader-related features:

-  Delete removes the selected exit reader from the Newly Assigned pane.
-  Add moves the selected exit reader from the Unassigned pane to the Newly Assigned pane.
-  Hyperlink in either pane opens the Summary tab for the selected exit reader.

Columns

Table 53. Entry Readers columns

Column	Description
Reader Name	Identifies the name of the exit reader.
Assignment	Identifies the name of the door to which the exit reader is attached.
Station Name	Identifies the remote host station name that manages the door and exit reader.

Grouping tab






This tab adds stations to the displayed access zone and, thereby, extends the zone to the readers assigned to those stations. It is only available when you are connected to the master controller station. In addition to extending the access zone physically, grouping shares access zone naming, occupancy, and supervisor information.

Buttons

Figure 155. Grouping tab

SummaryAccess ZoneActivity Alert ExtsOccupantsSupervisorsEntry ReadersExit ReadersGrouping

Newly Assigned





Display Name	Status	To Display Path String
Station1	{down}	/Drivers/NiagaraNetwork/Station1

You access this tab from the main menu by clicking **Controller Setup > Access Setup > Access Zones**, followed by creating a new zone or double-clicking an existing zone and clicking the Exit Readers tab.

Only stations that are joined in a peer relationship are available for grouping. You can only add readers to access zones when you are connected to the reader’s assigned station. Readers are not visible nor can they be configured from remotely-grouped stations.

In addition to the standard features (Delete, Filter and Export) this view supports grouping with these buttons:

-  Hyperlink in either pane opens the **Personnel > People** Summary tab for the selected person.
-  Assign Mode buttons open and close the Unassigned pane.

Columns

Table 54. Grouping tab columns

Column	Description
Display Name	Identifies the name of the group.
Status	Reports the status of the group.
To Display Path String	Indicates the station in the network with which this intrusion zone is grouped.






Card Formats view






This view displays a listing of all Wiegand formats that are defined for the system. You might use this feature if you deleted a format and want it back or if you upgraded your system and do not already have these formats available.




Buttons

Figure 156. Card Formats view








Wiegand Format Name 	Bit Length	Format
26-Bit Wiegand Format (HID-H10301)	26	PFFFFFFFFNNNNNNNNNNNNNNNNNNP
34-Bit Northern Wiegand Format	34	0FFFFFFFFFFFFFFFFNNNNNNNNNNNNNNNNNP
37-Bit Wiegand Format (HID-H10302)	37	PNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNP
40-Bit Wiegand Format	40	PNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNP
55-Bit Wiegand Format	55	PNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNP
test	26	N-----

To access this view from the main menu in a remote host station, click **Controller Setup > Access Setup > Card Formats**.

In addition to the standard control buttons (Summary, Delete, Filter, Column Chooser, Refresh, Manage Reports and Export), these buttons support card formats:

-  Add creates a new card format.
-  Hyperlink opens the Card Format view for the selected card with the Summary tab selected.
-  Add From Default Card Formats button opens a window for choosing one or more default card formats. Any default formats that are not already in the list appear in the window. You add the format by selecting the appropriate check box.

Columns

Table 55. Card Formats view columns


Column	Description
Wiegand Format Name	Provides a descriptive title for the Wiegand Format.
Bit Length	Specifies the card format total bit length. This number is the total of all data bits and all parity bits. <b>NOTE:</b> This system supports up to 256-bit Wiegand format.
Format	Displays the layout of all the bits.


Wiegand Format Editor view, Wiegand Format tab

This view configures new Wiegand format properties.

**NOTE:** You cannot edit a card format that is in use. Card formats that are not currently used by any badges display in the Wiegand format editor view and may be edited.

**Figure 157.** Wiegand Format Editor view

 Save

 Wiegand Formats

Summary

Wiegand Format

Wiegand Format Name

Default Facility Code

Validation Bits

All

▼

Bit Length

26

[0 - 256]

Parity Bits

0

[0 - 5]

Facility Start

0

Facility Length

0

Credential Start

0

Credential Length

1

Format

N-----

This view opens from the main menu when you click **Controller Setup > Access Setup > Card Formats**,

followed by clicking the Add button () in the Add New Wiegand Format view.

To edit an existing format, double-click the format row in the Card Formats view.

**NOTE:** You cannot edit a card format that is in use. Card formats that are not currently used by any badge display in the Wiegand format editor view and may be edited.

Links

A **Save** link and a **Wiegand Formats** view link are located at the top of the view.

**NOTE:** A maximum of 256-bit Wiegand format size (card bit length) is supported.

Wiegand Format tab properties

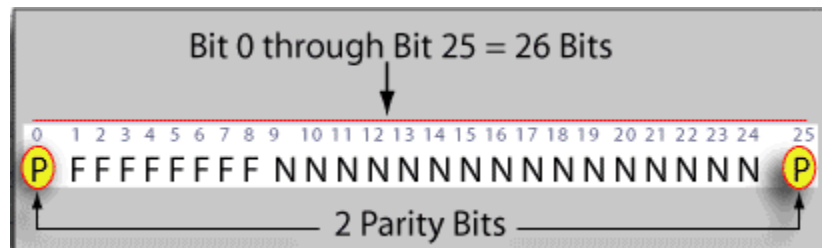
Property	Value	Description
Wiegand Format Name	text	Provides a descriptive title for the Wiegand Format.
Default Facility Code	text	Sets the default Facility Code property when assigning a format to

Property	Value	Description
		a badge. It does not need to match the <b>Facility Length</b> property and can be used to pre-load a prefix to be completed during badge creation.
Validation Bits	drop-down list	Selects the level of validation to use with the format. Three options are available: <b>All</b> , the most restrictive or secure, validates bits representing all possible areas of the format. <b>Credential and Facility Code only</b> validates the Credential and Facility Code bits. <b>Credential Only</b> , the least restrictive or secure, only validates the Credential bits.
Bit Length	number (0-256)	Specifies the card format total bit length. This number is the total of all data bits and all parity bits.
Parity Bits	number (0-5)	Specifies how many parity bits are in the format, not the location of the bits. Refer to <a href="#">Format property</a>
Facility Start	number	Specifies the bit position that holds the first bit of the facility code. Refer to <a href="#">Format property</a>
Facility Length	number	Specifies the total number of bits that are dedicated to facility code. Refer to <a href="#">Format property</a>
Credential start	number	Specifies the bit position that holds the first bit of the credential numbers. Refer to <a href="#">Format property</a>
Credential Length	number	Specifies the total number of bits that are dedicated to credential numbers. Refer to <a href="#">Format property</a>
Format	text	<p>Specifies the layout of all the bits, which must agree with the information in the previous parity, facility, and credential properties. Valid Format characters include:</p> <p>P–parity bit (an extra bit added for error detection)</p> <p>F–facility code bit</p> <p>N–credential number bit</p> <p>0–constant character of 0 (zero)</p>

Property	Value	Description
		1—constant character of 1 (one)  Refer to <a href="#">Format property</a>
Parity Layout	one or more additional format properties	Define the expected parity: Odd or Even. Refer to <a href="#">Format property</a>

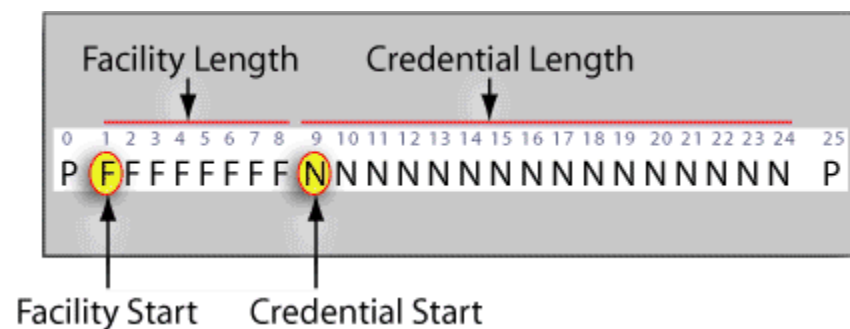
### Format property

**Parity Bits** may be located anywhere in the format.

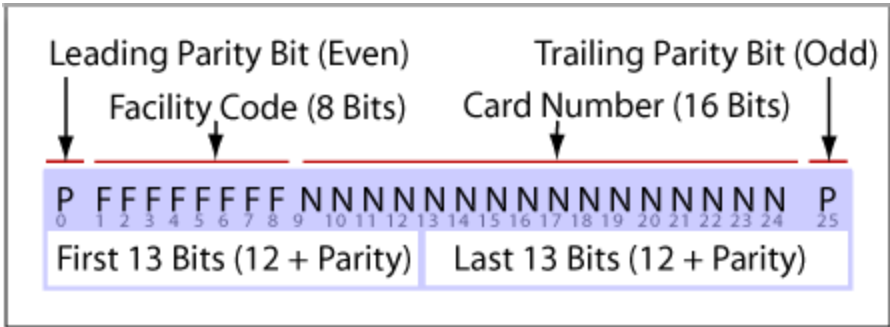


The example **Format** above has two parity bits. It specifies the location of these bits: one in the leading position, and the other in the trailing position.

**Facility Start**, **Facility Length**, **Credential Start** and **Credential Length** identify where the information starts in the **Format**, and how many characters are involved.

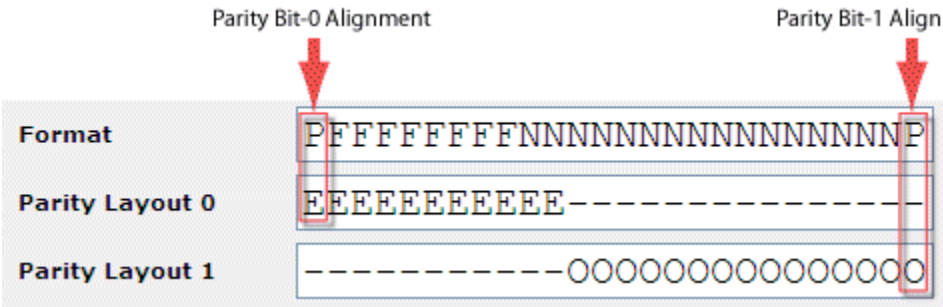


The **Format** property identifies the purpose of each bit, which must agree with the **Parity Bits**, **Facility** and **Credential** properties.



For example, if the **Parity Bits** value is “3,” three instances of the letter “P” must appear in the **Format**.

Based on the number of **Parity Bits**, additional **Parity Layout** properties appear below the **Format** property. If the value of **Parity Bits** is zero (0), no Layout properties appear. **Parity Layout** properties indicate the expected parity: Odd or Even.



The locations of the “E” and “O” characters in the **Parity Layout** property designate the bits that are used to calculate the parity sum. Follow these rules as you enter these characters:

- E – indicates that an even number of ones (1) is required to verify transmission accuracy.
- O – indicates that an odd number of ones (1) is required to verify transmission accuracy.
- Do not combine “E” and “O” characters in a single **Parity Layout** definition.
- In each **Parity Layout** definition, at least one parity bit character must align vertically beneath a credential bit or facility code bit. Additional characters are not required to align with any particular character, however, at least one character must be below a data field (**Facility Code** or **Credential Number**).
- Position the first “E” or “O” directly below the “P” in the **Format** property (Parity Bit-0 Alignment and Parity Bit-1 Alignment for right-to-left validation). Add additional characters of the same type, as required by the parity format definition.
- Align an additional “E” or “O” vertically under any additional parity bit (P) in the **Format** and add additional characters of the same type as required by the definition.

Wiegand Format Summary tab

This tab summarizes the properties for the selected Wiegand format.

**Figure 158.** Wiegand format Summary tab

[illegible]

This view opens from the main menu when you click **Controller Setup > Access Setup > Card Formats**, followed by double-clicking on a card format in the Card Formats view.

This tab is present but displays no pertinent information until you save the new Wiegand format. The tab shows the format title, primary properties, and a lists of badges that are using this format. Links to the Wiegand Formats and Badges views are included. When you save the data, this tab displays by default in the Edit: Wiegand Format view. It includes links to the Wiegand Formats and Badges views.

## Access Control Setup view

This view configures the Access Control Service.

## Properties

**Figure 159.** Access Control Setup view

Access Control Service	
Status	{ok}
Fault Cause	
Cache Status	Active
Enabled	true ✓
Display Unknown Wiegand Formats	false ✓
Has Pin Duress	false ✓
Pin Duress Offset	1
Remote Validation	false ✓

To access this view from the main menu of a remote host controller station, click **Controller Setup > Access Setup > Access Control Setup**.

In addition to the standard properties (**Status**, **Fault Cause** and **Enabled**), these properties support access control configuration.

Property	Value	Description
Cache Status	read-only	Indicates if cache is currently being used. Caching speeds up access. If access is slow, check this property value to see if caching is currently inactive or failed. Cache is normally temporarily disabled during a join process.
Display Unknown Wiegand Formats	true or false (default)	Turns off (false) unknown Wiegand messaging.
Has Pin Duress	true or false (default)	Turns the PIN duress alarm feature on and off.
Pin Duress Offset	text	When PIN Duress is enabled, sets a number used for incriminating a PIN value to indicate duress. For example, if a PIN number is 1234 and the Pin Duress Offset value is 2, a PIN number of 1236 causes a duress alarm if the <b>Pin Duress Enabled</b> property is set to <b>true</b> .
Remote Validation	true or false (default)	Controls the validation of user credentials at a remote location. Remote validation usually takes less than five seconds. However, if a Supervisor station is busy or has a large database, remote validation can take much longer, or may not be successful at all. In this situation, a card holder may walk away prior to the door unlocking, creating a security risk. For these reasons, this property defaults to <b>false</b> . If it is disabled on either the Supervisor or remote station, remote validation does not occur.

## Additional Personnel Entry — Import Info tab

This view appends new personnel record data, including Photo ID images to the existing station database.

Links

**Figure 160.** Additional Personnel Entry view

SaveExport

Import Info

Tenant

None»

Wiegand Format

None»

User Pass Key

••••••••

File

Browse...

To access this view from the main menu of a remote host station, click **Controller Setup > Access Setup > Additional Personnel Entry**.

The **Save** link in the top left corner of the view saves changes to the station database. The **Export** link opens the **Export Personnel Records** window.

Properties

Property	Value	Description
Tenant	Ref Chooser	Defines the tenant company for whom the person works.
Wiegand Format	Ref Chooser	Indicates the Wiegand format that is associated with the badge for this person. Wiegand format values are case-sensitive fields and are allowed as input data.
User Pass Key	text	On export, protects the exported file by creating a unique string. On import, the system requires this string.
File	filename	On export, defines the name of the .zip file to create. On import, locates the exported file.

Data to import

This topic lists some commonly-used valid properties you can import using the Additional Personnel Entry (import from CSV file) tab. These properties may be arranged in any order and only a last name for each person is required for a successful import.



**Figure 161.** Example CSV file for data import

	B	C	D	E	F	G	H	I	J	K	O	P	Q	R	S	T
1	FirstName	MiddleI	PinNumbe	Tenant	PersonTyp	Supervisor	Departmen	WiegandFormat0	Credential0	FacilityCoc	AccessRight0	StartDate0	EndDate0	AssignedThre	AccessRight1	StartDate
2	Bruce				Emergency	FALSE					Bldg.2-Emergency Responder					
3	Todd			Afton Remote		FALSE	Engineering				Bldg.1-Interior Doors			7		
4	Tracy	L				FALSE										
5	Randy			Afton Remote		FALSE	Engineering				Bldg.1-Interior Doors					
6	Robert		AHrPlmXE	Afton Remote		FALSE	Sales	37-Bit Wiegand For	3744365	0	Bldg.1-Perimeter Doors					
7	Steven				Police	FALSE					Bldg.2-Police Responder					
8	Theodore	N	AHsXlmVgXh2GEBGItxi+vgXEC6			FALSE		26-Bit Wiegand For	0	0	Bldg.1-Interior Doors				Bldg.1-Perimeter Doors	
9	Sandeev			Acme Phai	Operator	FALSE	Tracking	40-Bit Wiegand For	123456789	0	Bldg.1-Interior Doors				Bldg.1-Perimeter Doors	
10	Sneepie					FALSE		37-Bit Wiegand For	3744367	0	AA Night				Bldg.1-Interior Doors	
11	John		AH9dlmXlI0fGfFd2QI8	Administra		FALSE	District	37-Bit Wiegand For	3744366	0	Bldg.2-Perimeter Doors				Bldg.1-Interior Doors	
12	Wendy				Employee	FALSE	Faculty				Bldg.2-Perimeter Doors				Bldg.2-Interior Doors	
13	Chris				Employee	FALSE	Administra	26-Bit Wiegand For	0	0	Bldg.2-Perimeter Doors			7	Bldg.2-Interior Doors	

Property	Value	Description
First Name (optional)	text	Defines the employee's first given name.
Last Name (required)	text	Defines the employee's second name.
Middle Initial (optional)	text	
PIN Number (optional)	numeric, no spaces allowed	Defines a Personal Identification Number to import only. The export file displays the encoded number in the PIN column if one exists.
Tenant (optional)	Ref Chooser	Defines the tenant company for whom the employee works.
Person Type (optional)	text	For example: Male, Female, Unknown
Supervisor (optional)	true or false	Identifies if the person functions in a supervisory role.
Department (optional)	text	Defines the department, such as Accounting, Personnel, Manufacturing, Sales, etc.
Wiegand Format (optional)	Ref Chooser	Indicates the Wiegand format that is associated with the badge for this record. Wiegand format values are case-sensitive fields and are allowed as input data.
Credential (optional unless a Facility Code is also provided)	text	Provides a unique badge number.
Facility Code (optional)	text; the default is defined in the Wiegand format	If this property is left blank, the default is used.
Access Right (optional)	text	Defines one or more access rights to

Property	Value	Description
		link with the personnel record.
Portrait (optional)	.jpg or .png	Defines the photo used on a Photo ID.

Data that are not supported for import

The following types of data are NOT supported by Additional Personnel Data import and export:

- Badge data
  - Description
  - Status
  - Issue Date
  - Threat Level Group
  - Assigned Level
- Person data
  - Trace Card
- Access Right data
  - Description
  - Schedule
  - Threat Level Group
  - Threat Level Operation
  - Default Assigned Threat Level
  - Niagara Integration ID
  - Readers

Export Personnel Records window

Exports the additional personnel data to a comma-delimited file.

Figure 162. Export Personnel Records window

Export Personnel Records

File Name

personnelBackup\_vykonSecurity\_6\_19-Apr-17

User Pass Key

Ok

Cancel

This window opens from the Additional Personnel Entry view when you click the **Export** button.

Property	Value	Description
File Name	text	Defines the name of the file to create.

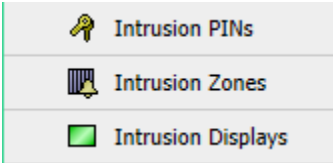
Property	Value	Description
User Pass Key	text	Defines the password the system will require when importing this data back into the database.



# Chapter 9. Controller (System) Setup–Intrusion Setup

Intrusion Setup views configure intrusion PINs, zones and displays that manage the building’s alarm system. These views are available to both Supervisor and controller stations.

Figure 163. Intrusion menu

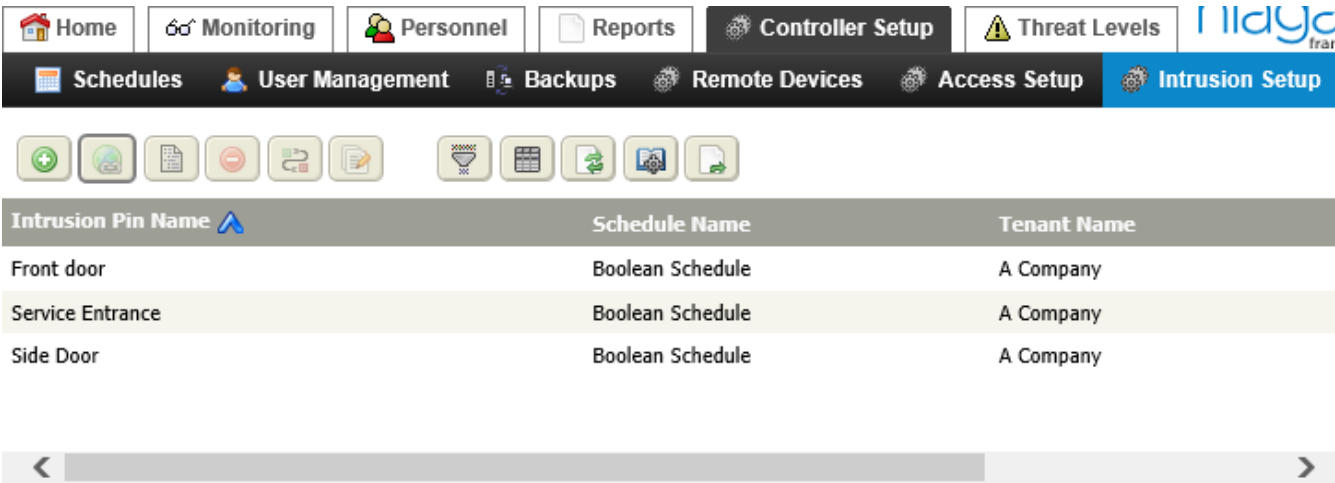


A Supervisor station does not include the Intrusion Displays menu item.

## Intrusion Pins view

An intrusion PIN (personal identification number) is a number that is required to arm and disarm an intrusion zone. This view provides a tabular display of all existing intrusion PINs.

Figure 164. Intrusion Pins view





To access this view from the main menu, click **Controller (System) Setup > Intrusion Setup > Intrusion PINs**.

### Buttons

In addition to the standard control buttons (Summary, Delete, Filter, Column Chooser, Refresh, Manage Reports, and Export, these buttons serve special functions for intrusion configuration:

-  Add opens the Add New Intrusion Pin view.

-  Hyperlink opens the Intrusion Pin view to the Summary tab.
-  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.


## Columns

Column	Description
Intrusion Pin Name	This links to a listing of the names of each of the current PINs. Double-clicking on the PIN description displays the appropriate Edit Existing PIN view.
Schedule Name	Displays the name of any schedule that is assigned to the PIN.
Tenant Name	Displays the name of any tenant assigned to the PIN.

## Add New (or edit) Intrusion Pin view, Intrusion Pin tab

This view and tab sets up new intrusion PIN (Personal Identification Number) one at a time.

**Figure 165.** Intrusion Pin tab

To access this tab from the main menu, click **Controller (System) Setup > Intrusion Setup > Intrusion PINs**, and click the Add button ().

To edit an existing intrusion PIN, double-click the PIN row in the Intrusion Pins view, and click the Intrusion Pin tab.

## Links

A **Save** link is located in the top left of the view and an **Intrusion Pins** link returns to the Intrusion Pins view.

## Properties

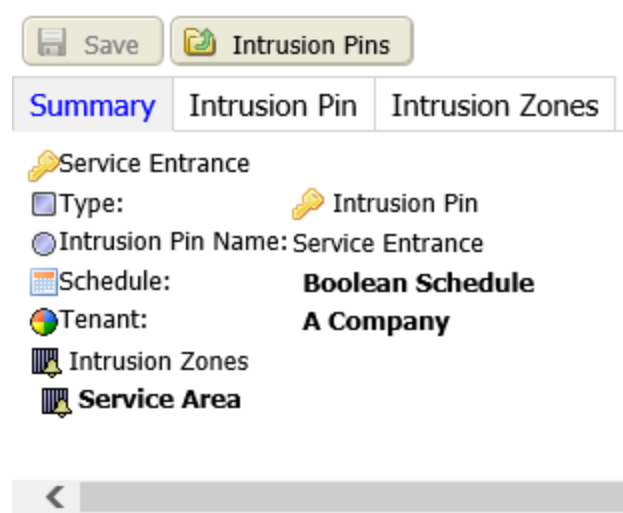
Property	Value	Description
Intrusion Pin Name	text	Defines a name for the intrusion PIN.
Schedule	Ref Chooser	Opens a Ref Chooser for associating a schedule with the PIN.

Property	Value	Description
Tenant	Ref Chooser	Opens a Ref Chooser for associating a tenant with the PIN.
PIN	number	Defines the PIN.

Intrusion Pins Summary tab

This tab displays a read-only list of information about the selected PIN.

Figure 166. Summary tab



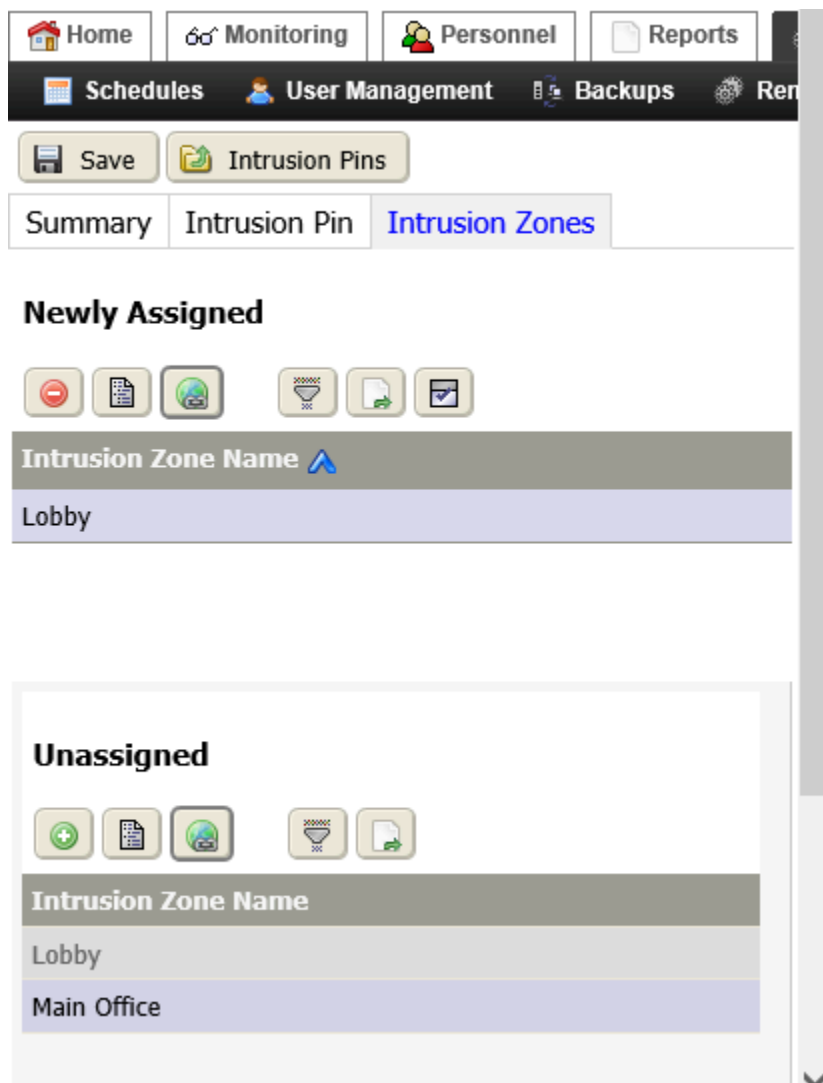
This view opens when you save changes made in another PIN tab. Display properties include the PIN Name, associated schedules, and tenants. Located at the bottom of the tab is a list of all the associated intrusion zones currently associated with the PIN.

Property	Description
Type	Identifies the type of record as defining to an Intrusion PIN.
Intrusion Pin Name	Provides a name for the PIN.
Schedule	Identifies the schedule associated with the PIN.
Tenant	Identifies the tenant company associated with the PIN.
Intrusion Zones	Identifies the intrusion zone(s) associated with this PIN.

PIN Intrusion Zones tab




This tab associates and disassociates intrusion zones from the currently displayed intrusion PIN using the assign mode, the assign and unassign buttons.

## Buttons

**Figure 167.** Intrusion Zones tab

This view opens when you navigate to **Controller (System) Setup > Intrusion Setup > Intrusion Pins**, double-click an existing row in the table and click the **Intrusion Zones** tab.

In addition to the standard buttons (Delete, Summary, Filter and Edit), these buttons support intrusion zones tab under the Intrusion Pins view:











-  Hyperlink opens the Intrusion Zone view to the Summary tab.
-   Assign Mode buttons open and close the Unassigned pane.



## Intrusion Zones views

Intrusion zones combine multiple sensors into a logical grouping for monitoring and alarming in a defined space (zone) within a building.




**Figure 168.** Intrusion Zones view

Schedules  User Management  Backups  Remote Devices  Access Setup <b>Intrusion Setup</b> Alarm Setup  Miscellaneous				
<div><div></div><div></div></div>				
Display Name	Zone Status	Time Delay	Warning Time	To Display Path String
Intrusion Zone	Disarmed	20secs	5secs	/Services/AlarmService/Intrusion Zone

You access this view from the main menu by clicking **Controller Setup > Intrusion Setup > Intrusion Zones**.

### Buttons

In addition to the standard control buttons (Delete, Rename, Refresh, Column Chooser, Filter, Reports Manager, and Export), these buttons support intrusion zones.

-  Add opens the Add New Intrusion Pin view.
-  Hyperlink opens an existing intrusion pin record.
-  Manual Override opens a window from which to select one of four options for manually overriding access to an intrusion pin.

### Columns



Column	Description
Display Name	Reports the name that describes the event or function.
Zone Status	Reports the last value written using device facets. Applies only to writable points.
Time Delay	Reports the length of time the system waits after someone sets the alarm before it arms the zone.
Warning Time	Reports the length of time the system sounds a warning before arming a zone.
To Display Path String	Defines the station path for this zone.

## Add New (or edit) Intrusion Zone view

This view provides configures an intrusion zone.

## Links

**Figure 169.** Intrusion Zone view/tab

 Save
  Intrusion Zones

**Display Name**

**Intrusion Zone** | Recipients | Relay Links

**Ack Required** ☐ Normal ☒ Offnormal ☒ Fault ☒ Alert

**Priority** Offnormal  Fault  Normal  Alert

**Total Alarm Count**

**Open Alarm Count**

**In Alarm Count**

**Unacked Alarm Count**

**Time Of Last Alarm**       IST

**Escalation Level1 Enabled**

**Escalation Level1 Delay**  h  m [1min - +inf]


**Escalation Level2 Enabled**


**Escalation Level2 Delay**  h  m [2mins - +inf]

**Escalation Level3 Enabled**

**Escalation Level3 Delay**  h  m [3mins - +inf]

**Zone Enabled** false {ok}

**Zone Schedule**  None »

**Zone Input**  None »

**Zone Status** Disarmed

**Arming Test Status** Success {ok}

**Time Delay**  h  m  s [0ms - +inf]

**Warning Time**  h  m  s [0ms - +inf]

**Count Down** 0 sec

**Last Activity**       IST

To access this view from the main menu, click **Controller (System) Setup > Intrusion Setup > Intrusion Zones** the

Add button ().

To edit an existing intrusion zone, double-click the zone row in the Intrusion Zones view or select the row and

click the Hyperlink button (.

A **Save** link is located in the top left of the view and an **Intrusion Zones** link returns to the Intrusion Zones view.

**Intrusion Zone tab**

This tab configures the properties of a new intrusion zone.

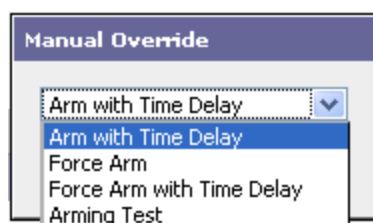
Property	Value	Description
Ack Required	check boxes	Sets the requirements for an alarm acknowledgment in this intrusion zone. Alarm acknowledgments are required only for selected options.
Priority	number between 1 (highest priority) and 255	Sets an importance level for each of the listed priority categories: Offnormal, Fault, Normal, and Alert alarms.
Total Alarm Count	number	Returns the total number of alarms of any state that are associated with the intrusion zone.
Open Alarm Count	number	Returns the number of open alarms. An alarm is considered open when it is not acknowledged and normal or not acknowledged and in alert.
In Alarm Count	number	Returns the number of alarms that are currently in an alarm state.
Unacked Alarms	number	Returns the number of alarms that require acknowledgment and have not yet been acknowledged.
Time of Last Alarm	read-only time	Indicates when the latest alarm occurred.
Escalation Level(n) (where n is 1, 2, or 3)	true or false	Enables and disables alarm escalation at this level.
Escalation Level (n) Delay (where n is 1, 2, or 3)	time (minimum: one minute)	Defines the amount of time to allow an unacknowledged alarm to remain unacknowledged before you escalate it to the next level.
Zone Enabled	read-only true or false	Indicates the status of the intrusion zone: enabled ( <code>true</code> ) or disabled ( <code>false</code> ).
Zone Schedule	Ref Chooser	Arms and disarms an intrusion zone according to a schedule. Clicking  delete (  ) removes an assigned schedule.
Zone Input	Ref Chooser	Designates the input to use for zone communication. Clicking delete (  ) removes an assigned input.

Property	Value	Description
Zone Status	read-only	Displays the status of the intrusion zone: Armed, Disarmed, or Arming.
Arming Test Status	read-only <code>true</code> or <code>false</code>	Indicates if the last arming test was successful ( <code>true</code> ) or unsuccessful ( <code>false</code> ).
Time Delay	hours, minutes, seconds, and milliseconds	Defines the time between when an alarm is set and when the zone is actually armed. For example, a Time Delay of 45 seconds allows occupants to leave promptly without setting off the alarm. During this time delay period, the intrusion zone is in an arming state.
Warning Time	hours, minutes, seconds, and milliseconds	Defines when the system begins signaling to warn occupants that it is about to arm the zone. This value may be less than or equal to the Time Delay. For example, if the Time Delay is 45 seconds and the Warning Time is 10 seconds, 35 seconds after beginning to arm the zone, the warning signal, such as a beeper, sounds for the final 10 seconds of the arming state.
Count Down	hours, minutes, seconds, and milliseconds	Displays the time remaining before the system arms the intrusion zone.
Last Activity	read-only	Reports the last arming or disarming event.

## Manual Override window

This window selects an option for manually arming or disarming an intrusion zone.

**Figure 170.** Manual Override window



The window opens when you click the **Manual Override** button on the edit intrusion zone view.

Table 56. Manual Override options

Option	Description
Arm with time delay	Arms the intrusion zone using the time delay set in the Time Delay field. The zone does not alarm if there are any open alarms in the zone.
Force Arm	Arms the intrusion zone immediately with no time delay and regardless whether or not there open alarms in the intrusion zone.
Force arm with time delay	Arms the intrusion zone using the time delay set in the Time Delay field. Open alarms in the zone do not prevent force arming.
Arming Test	Checks for points in an active alarm state before arming the intrusion zone. You cannot arm an intrusion zone that has points in an active alarm state. The test reports that the zone is ready to arm, or it displays a list of points that are in alarm. <b>NOTE:</b> Make sure that the request-to-exit properties on all doors in an intrusion zone are inactive before initiating the arming test. An active request to exit inhibits the associated door sensor and, allowing the sensor to bypass the test.

Intrusion Zone Summary tab

This tab reports the main properties currently configured for the intrusion zone.


Figure 171. Intrusion Zone Summary tab


Summary

Intrusion Zone


Intrusion Pins


Intrusion Displays


 Intrusion Zone

 Mapped Ord:


/Services/AlarmService/Intrusion Zone

 Type:


 Intrusion Zone

 Intrusion Zone Name:


Intrusion Zone

 Zone Status:

Disarmed

 Time Delay:

20secs

 Warning Time:

5secs

This view opens when you click **Controller (System) Setup > Intrusion Setup > Intrusion Zones** and double-click a zone in the table.

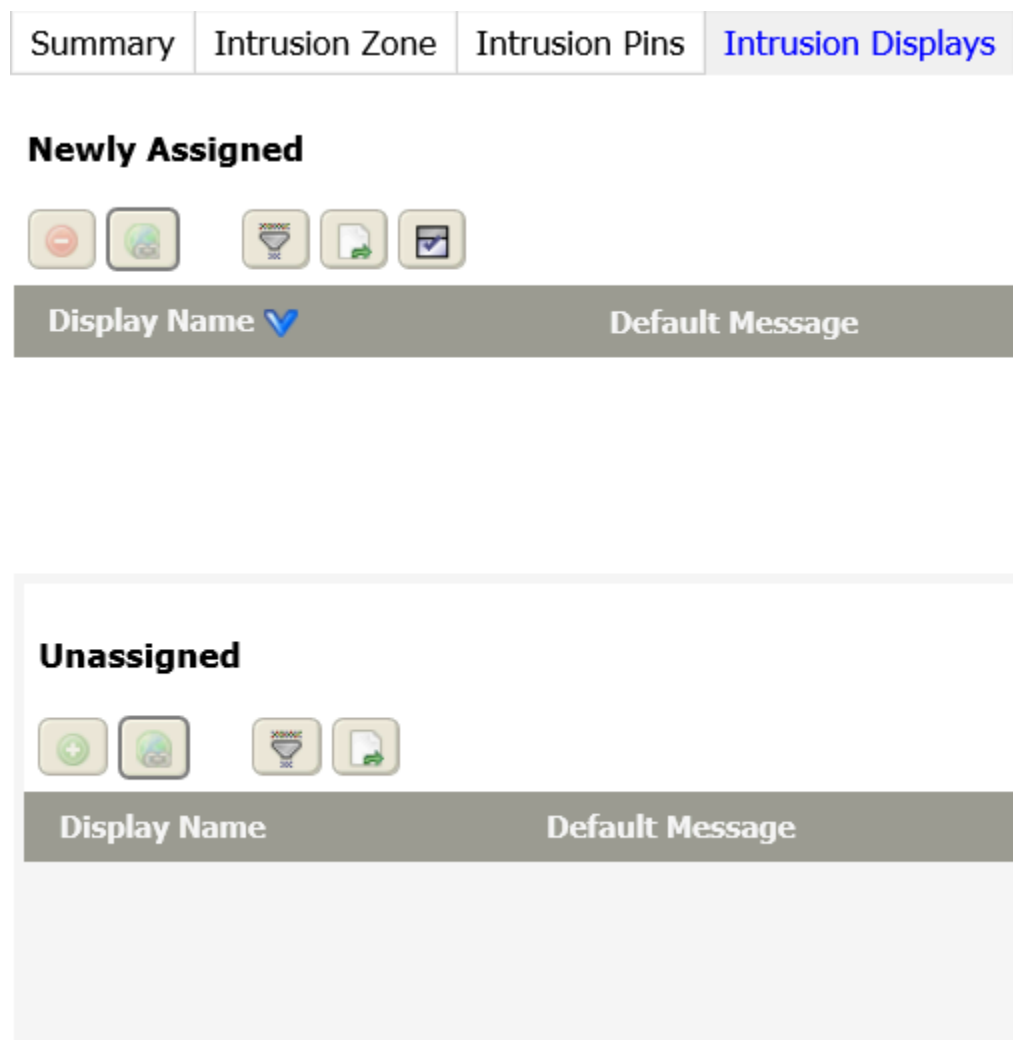
Property	Description
Mapped Ord	Reports the address of the intrusion zone.
Type	Reports the type of zone.
Intrusion Zone Name	Reports the name of the current intrusion zone.
Zone Status	Reports the condition of the zone.
Time Delay	Reports any delay.
Warning Time	Indicates the amount of time prior to an alarm that a alarm warning beep is sounded. For example, if Door Held Open Limit is 60 seconds, 30 seconds after the door opens the warning beep sounds and stops either when the door closes or when the door sensor goes into an alarm condition.

Intrusion Displays tab (learn mode)

This tab displays a list of all of the intrusion monitors that are assigned to the currently-selected intrusion zone, and provides a way to manually assign and unassign monitors.

Links

**Figure 172.** Intrusion Displays tab



This tab opens when you click **Controller (System) Setup > Intrusion Setup > Intrusion Zones**, double-click a zone in the table, and click the **Intrusion Displays** tab.

The **Manual Override** link opens the **Manual Override** window.

Buttons

In addition to the standard buttons (Delete, Filter and Export), these buttons support intrusion displays:

-  Hyperlink opens the Intrusion Display view at the Summary tab.

Columns

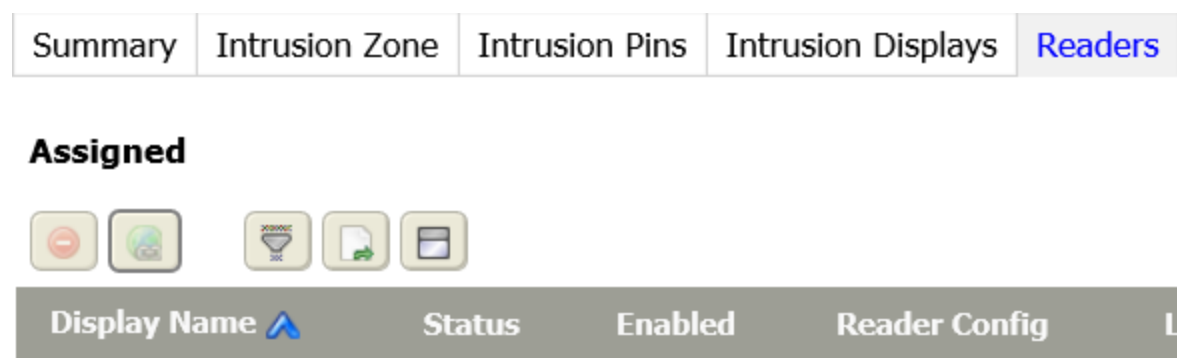
Column	Description
Display Name	Reports the name of the intrusion display.
Default Message	Reports the default message for this display.

Column	Description
Smart Key Device	Reports the name of the connected SmartKey device.
Address	Reports the URL of the display.
Status	Reports the current condition of the display.
Intrusion Zones	Reports the intrusion zone(s).

Readers tab

This tab provides a way to manually assign and unassign readers to the current intrusion zone.

Figure 173. Readers tab



This tab opens when you click **Controller (System) Setup > Intrusion Setup > Intrusion Zones**, double-click a zone in the table and click the Readers tab.

You add items to the currently-displayed intrusion zone using the assign mode, assign and unassign buttons.

Note the following about readers and intrusion zones:

- Readers may be used to arm and disarm intrusion zones.
- A single reader may be assigned to more than one intrusion zone and it arms and disarms all zones that it is assigned to.
- A single reader cannot be assigned to BOTH a door and an intrusion zone at the same time.
- In a company-wide system, entry readers may be available from multiple controllers.

Points tab

This tab lists all the points that are assigned to the currently-selected intrusion zone and provides a way to manually assign or unassign points to the zone. The assigned, points define the zone and, in a company-wide system, may include more than one controller.



Figure 174. Points tab



This tab opens when you click **Controller (System) Setup > Intrusion Setup > Intrusion Zones**, double-click a zone in the table and click the Points tab.

Entry points are points (already assigned under the Points tab), which are associated with a location that may need a delay for arming or disarming. A value of `true` under the Entry column in the table identifies the entry points.

In addition to the assign mode, assign and unassign, filter and export buttons, this tab provides these buttons:

-  Edit Entry Point designates a point as an entry point. The window it opens provides a single property used to enable (`true`) and disable (`false`) the use of the point as an entry point.  
**NOTE:** Door alarm points (for example, Door Held Open Alarm, Door Forced Open Alarm, and Supervised Fault Alarm) cannot be assigned under the intrusion zone Entry Points tab and, therefore, they do not appear in the **Assign Points** window.
-  Edit Always Armed Points configures a point to always be armed, even if the intrusion zone they are assigned to is disarmed. The window it opens provides a single property used to enable (`true`) and disable (`false`) the always-armed condition.  
**NOTE:** When always armed, intrusion Timeout Alarm points and the points that are already added to the Entry Point tab are not available. They do not appear in the **Assign Points** window.

Columns

Column	Description
Source Name	Displays the point source.
Display Name	Displays the name of the point.
Entry	Indicates if the point is an entry point that requires a delay ( <code>true</code> ) or not ( <code>false</code> ).
Always Armed	Indicates if the point is to remain armed after disarming the zone ( <code>true</code> ) or not ( <code>false</code> ).
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.

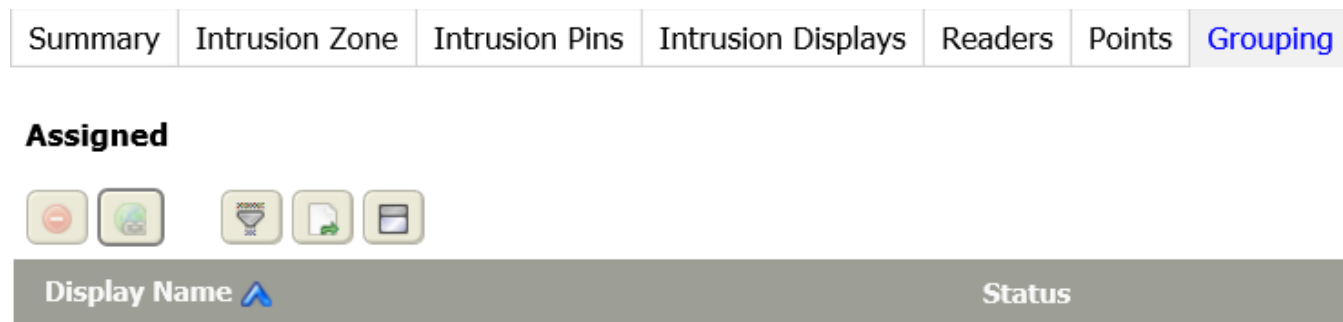


Grouping tab

This tab manually assigns and unassigns more than one remote station to the current intrusion zone. Using the assign mode, assign and unassign buttons, peer, Supervisor, and subordinate stations may be included in the zone.

Buttons

Figure 175. Grouping tab



This tab opens when you click **Controller (System) Setup > Intrusion Setup > Intrusion Zones**, double-click a zone in the table and click the Grouping tab.

This tab provides standard control buttons.

Columns

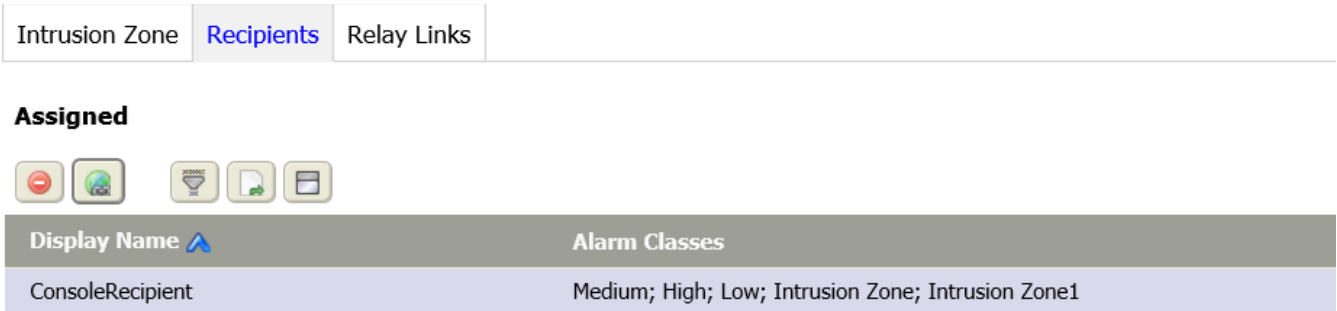
Column	Description
Display Name	Reports the name that describes the event or function.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
To Display Path String	Defines the station path for this zone.

Recipients tab

This tab provides a way to assign alarm recipients to the selected intrusion zone and remove assignments. Alarm recipients receive alarm notification as specified by the specific alarm recipient properties.

Buttons

**Figure 176.** Intrusion Zone Recipients tab





To access this view from the main menu, click **Controller (System) Setup > Intrusion Setup > Intrusion Zones** then click the Recipients tab.

The title of the view indicates the currently-selected intrusion zone.

You add items to the displayed view using the assign mode and the assign and unassign buttons.

**NOTE:** You cannot save an Intrusion Zone unless it has an assigned console recipient.

In addition to the standard control buttons (Delete, Filter, and Export) these buttons are important for managing intrusion zone recipients:

-  Hyperlink opens the monitoring view associated with the intrusion zone.
-  Assign Mode buttons open and close the Unassigned pane.

Columns

**Table 57.** Recipients columns

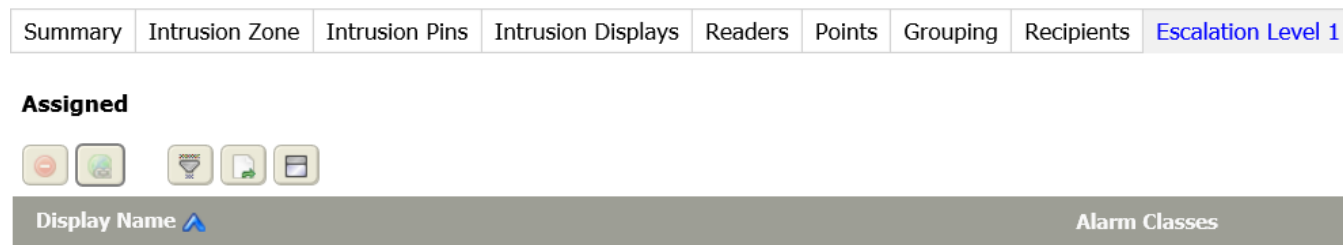
Column	Description
Display Name	Reports the name that describes the event or function.
Alarm Classes	Reports the <code>Display Name</code> of the alarm class associated with the point, recipient or other component.

Escalation Level tabs

These tabs manually assign and unassign alarm recipients to an escalation level. Assigned alarm recipients receive alarm escalation notification when the system escalates a corresponding alarm as specified by the specific alarm recipient properties.

Buttons

**Figure 177.** Escalation Level tab





This tab opens when you click **Controller (System) Setup > Intrusion Setup > Intrusion Zones**, double-click a zone in the table and click the EscalationLevel tab.

An Escalation Level tab displays for each escalation level that is enabled on the Intrusion Zone tab. No Escalation Level tab is displayed when escalation levels are not enabled (set to `false`).

You add items to the currently-displayed intrusion zone escalation level using the assign mode and the assign and unassign buttons.

In addition to the standard control buttons (Delete, Filter, and Export) these buttons are important for managing intrusion zone recipients:

-  Hyperlink opens the escalation level associated with the intrusion zone.
-  Assign Mode buttons open and close the Unassigned pane.

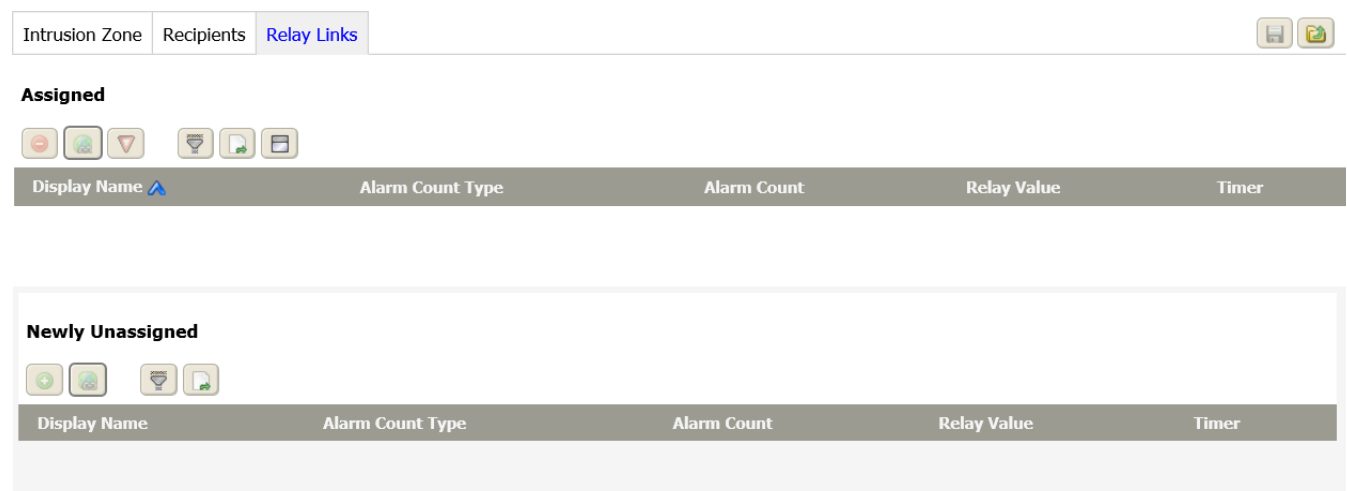
Columns

Column	Description
Display Name	Provides escalation level name.
Alarm Classes	Defines the alarm classes associated with the zone.

Relay Links tab

This tab assigns and unassigns output relays to the selected intrusion zone for the purpose of communication output. This output relay is active whenever the intrusion zone is in an armed state.

Figure 178. Intrusion zone Relay Links tab






To access this view from the main menu, click **Controller (System) Setup > Intrusion Setup > Intrusion Zones** then click the Relay Links tab.

The title of the view indicates the currently-selected intrusion zone.

You add items to the currently displayed intrusion zone using the assign mode and the assign and unassign buttons.

Buttons

In addition to the standard control buttons (Delete, Filter, and Export), these buttons apply to relay links:

-  Hyperlink opens the Alarm Count to Relay tab for the selected intrusion zone.
-  Assign Mode buttons open and close the Unassigned pane.
-  Turn Off Relays manually disables an output relay.

Columns

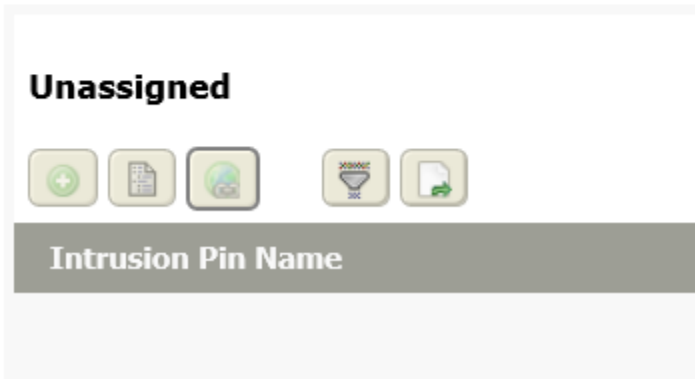
Column	Description
Display Name	Reports the name of the relay link.
Alarm Count Type	Identifies the count type configured (in the Add New Alarm Count to Relay view) to activate the relay. Unacked Alarm Count activates the relay for the length of the time defined by <b>Timer</b> or until the alarm is acknowledged. Open Alarm count activates the relay for the length of the time defined by <b>Timer</b> or until the alarm is cleared from the console. In Alarm Count activates the relay for the length of time defined by <b>Timer</b> or until the alarm returns to normal. Total Alarm Count activates the relay or the length of time defined by <b>Timer</b> when an alarm occurs.
Alarm Count	Reports the number of alarms for the configured count type that activated the relay.
Relay Value	Indicates if the output relay is on (true) or off (false).
Timer	Reports the maximum amount of time that the relay is energized.

## Edit Existing Intrusion Pin view

An Intrusion Pin (Personal Identification Number) is used to authorize the arming and disarming of an intrusion zone when the reader associated with the intrusion zone is configured as an intrusion keypad. This tab uses the assign mode to assign, unassign, and link to existing intrusion PINs.

### Links

**Figure 179.** Intrusion Pins tab




This tab opens when you click **Controller (System) Setup > Intrusion Setup > Intrusion Zones**, double-click a pin in the table and click the Intrusion Pins tab.


The **Manual Override** link opens the **Manual Override** window.

The panes contain the standard Newly Assigned-Unassigned control buttons.

### Buttons

In addition to the standard buttons (Delete, Filter and Export), these buttons support intrusion displays:

-  Hyperlink opens the Intrusion Pin view at the Summary tab.

-  Assign Mode buttons open and close the Unassigned pane.

Columns

Column	Description
Intrusion Pin Name	Reports the name associated with the intrusion pin.
Schedule Name	Reports the name of the schedule associated with the intrusion pin.
Tenant Name	Reports the tenant name.

Intrusion Displays views

Intrusion displays present information about the status of an intrusion zone and let users interact with the zone using a keypad, touch pad, or other means of data input. The Intrusion Displays view shows a table of all of the available intrusion displays. Double-click on the display name entry to view and edit details about the particular display.

Buttons

Figure 180. Intrusion Displays view



You access this view from the main menu by clicking **Controller Setup > Intrusion Setup > Intrusion Displays**.

The control buttons provide the standard functions.

Columns

Column	Description
Display Name	Displays the name of the intrusion display
Default Message	Shows the text that displays on an intrusion display device or on the Virtual Display.
Smart Key Device	Displays the name of any assigned Smart Key device.
Address	Shows the ID of the device (SmartKey) assigned to the intrusion display.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Intrusion Zones	Displays the name of the intrusion zone that the display is assigned to.

Add New (or edit) Intrusion Display view

This view creates a new intrusion display. A similar view edits existing intrusion displays.

Links

Figure 181. Add New Intrusion Display view

Display Name

Intrusion Display

Intrusion Display

Activity Alert Exts

Intrusion Zones

Default Message

Intrusion Keypad

x

Smart Key Device

None

Scroll Start Delay

00000

h

00

m

01

.

250

s

[0ms - +inf]

Scroll Column Delay

00000

h

00

m

00

.

150

s

[0ms - +inf]

Change Delay

00000

h

00

m

03

.

000

s

[0ms - +inf]

Inactivity Time

00000

h

01

m

00

s

[0ms - +inf]

Status Beep

true

Arming Pin Required

false

Status Pin Required

false

Point Display

Normal Path

Default Page

Time

In Alarm Beep

false

In Alarm Max Beep

00000

h

00

m

30

s

[0ms - +inf]

You access this view by clicking **Controller (System) Setup > Intrusion Setup > Intrusion Displays**, followed by clicking the Add button (  ).

To edit an existing intrusion display, double-click the display row in the table.

A **Save** button and an **Intrusion Displays** view link are located directly above a **Display Name** property at the top of the view.

Intrusion Display properties

These properties configure the new intrusion display.

Property	Value	Description
Default Message	text	Defines what to display on the default Time screen, at the top of the display.
SmartKey Device	drop-down list (defaults to None)	Lists the SmartKey devices that are available to be assigned to the

Property	Value	Description
		current intrusion display. <b>NOTE:</b> This list displays as a read-only field in the Add New Intrusion Display view, but is available in the Edit Intrusion Device view.
Scroll Start Delay	minutes, seconds, and milliseconds	Sets the amount of time before a text line on the display starts scrolling. (When a text field is too long (wide) to fit completely in the display, it scrolls continuously across the screen, horizontally.)
Scroll Column Delay	minutes, seconds, and milliseconds	Specifies how fast scrolling display text moves across the display screen.
Change Delay	minutes, seconds, and milliseconds	Specifies how long to pause between messages when there is more than one message to display, and the desired time to wait between scrolling each sequential message.
Inactivity Time	minutes and seconds	Defines when to revert to the default menu and low-power mode if there is no activity at the SmartKey device for a certain amount of time.
Status Beep	true or false	Turns on (true) and off (false) a single beep at the SmartKey device when the intrusion zone status changes from armed to disarmed status.
Arming Pin Required	true or false	Requires (true) or does not require (false) a valid PIN when arming an intrusion zone.
Status Pin Required	true or false	Requires (true) or does not require (false) a valid PIN when displaying intrusion zone status using the SmartKey device.
Point Display	drop-down	Determines how to display any fault message on the display screen (and virtual display) when initiating an arming action using the SmartKey device. <b>No Path</b> displays the fault message without identifying the point. For example: Supervisor Fault Detected. <b>Normal Path</b> displays the fault message followed by the point identity. For example: Door1.Sensor.Supervisor Fault Detected. <b>Reverse Path</b> displays the point identity followed by the fault message. For example: Supervised

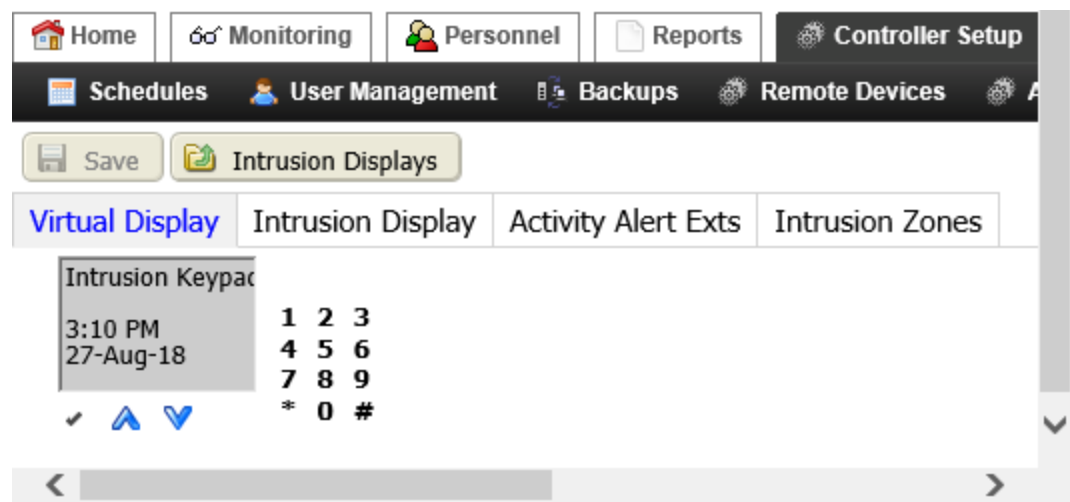


Property	Value	Description
		Fault Detected.Sensor.Door1
Default Page	drop-down list	Assigns a default display page for the SmartKey device. This page opens at the end of the <b>Inactivity Time</b> and is, typically, the initial screen that a user sees at the SmartKey device. <b>Summary</b> sets the Summary screen as the default screen. This screen displays zone identification and status information about the assigned intrusion zone as well as a menu of actions to control arming and disarming the zone. <b>Time</b> sets the Time screen as the default screen. This screen displays the default message as well as the current date and time. Pressing the SmartKey device F1, F2, or F3 changes the display to the Summary screen.
In Alarm Beep	true or false	Turns on (true) and off (false) a single beep when there is an intrusion zone alarm.
In Alarm Max Beep	hours, minutes, seconds	Defines how long the alarm beep lasts when <b>In Alarm Beep</b> is set to true.

Virtual Display tab

This tab contains a virtual SmartKey device that consists of a display and keypad with controls and indicators that function the same as the SmartKey device.

Figure 182. Virtual Display tab



Intrusion Display tab (configuration)

This tab provides access to the intrusion display properties.

Display Name		Intrusion Display	
Intrusion Display		Activity Alert Exts	
Intrusion Display		Intrusion Zones	
Default Message	Intrusion Keypad x		
Smart Key Device	None v		
Scroll Start Delay	00000	h 00 m 01 . 250	s [0ms - +inf]
Scroll Column Delay	00000	h 00 m 00 . 150	s [0ms - +inf]
Change Delay	00000	h 00 m 03 . 000	s [0ms - +inf]
Inactivity Time	00000	h 01 m 00	s [0ms - +inf]
Status Beep	true v		
Arming Pin Required	false v		
Status Pin Required	false v		
Point Display	Normal Path v		
Default Page	Time v		
In Alarm Beep	false v		
In Alarm Max Beep	00000	h 00 m 30	s [0ms - +inf]

These properties are described in the *Add New Intrusion Display view* topic.

Intrusion displays Activity Alert Exts tab

This tab configures alarm class priorities and video alarms. For more information, refer to *Alarm Extensions view* in the *Controller (System) Setup - Alarm Setup* chapter.

Alerts

**Figure 183.** Activity Alert Exts on an intrusion display



You access this view by clicking **Controller (System) Setup > Intrusion Setup > Intrusion Displays**, followed by clicking the Add button (



) or double-clicking an existing display in the table, and clicking the Activity Alert Exts tab.

Alert	Description
Invalid Pin Number Alert	Configures what to do when a person enters an invalid PIN.
No Active Schedule Alert	Configures what to do if no schedule is associated with the zone.

Alert properties

Property	Value	Description
Alarm Class	drop-down list	Sets the priority of an alarm generated by an alert.
Video Setup	link	Opens the Video Setup window. Refer to <i>Video Setup window</i> in the <i>Controller (System) Setup-Remote Devices</i> chapter.

Related reference

- [Alarm Extensions view](#)
- [Video Setup window](#)

Related information

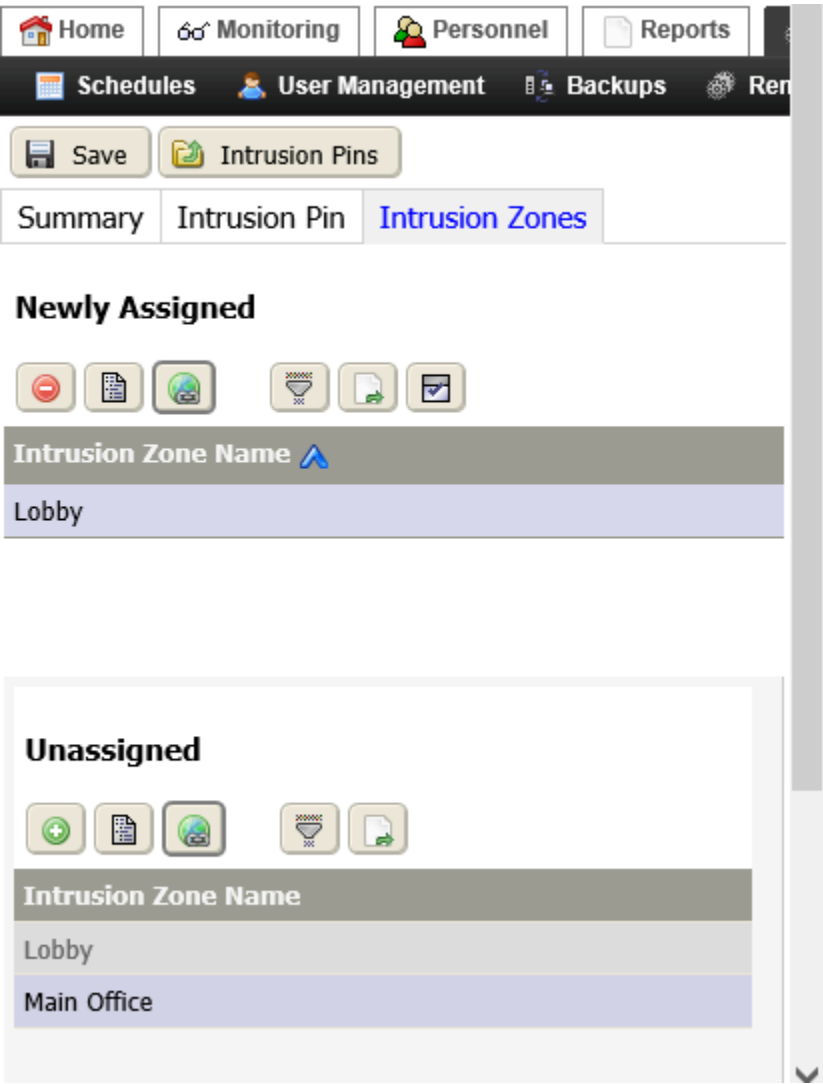
- [Controller \(System\) Setup–Alarm Setup](#)

Display Intrusion Zones tab

This tab manually associates and disassociates intrusion zones with the intrusion display using the assign mode, the assign and unassign buttons..

Buttons

**Figure 184.** Display Intrusion Zones tab



You access this view by clicking **Controller (System) Setup > Intrusion Setup > Intrusion Displays**, followed by clicking the Add button (



) or double-clicking an existing display in the table, and clicking the Intrusion Zones tab.

**NOTE:** This configuration of an intrusion display cannot be saved unless at least one intrusion zone is assigned to it.

In addition to the standard buttons (Hyperlink Filter, and Export, the assign mode, assign and unassign buttons configure the association.

### Columns

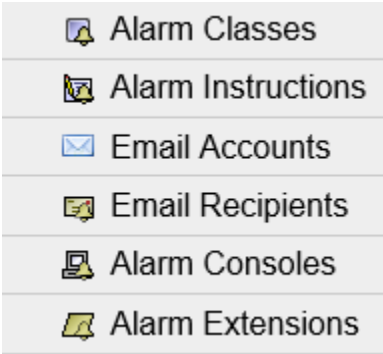
Column	Description
Display Name	Reports the name that describes the event or function.
Zone Status	Reports the last value written using device facets. Applies only to writable points.
Time Delay	Reports the length of time the system waits after someone sets the alarm before it arms the zone.
Warning Time	Reports the length of time the system sounds a warning before arming a zone.
To Display Path String	Defines the station path for this zone.



# Chapter 10. Controller (System) Setup–Alarm Setup

Setup views include displays that are related to configuring system components and network properties, as well as user preferences and other variables.

Figure 185. Alarm Setup menu



## Alarm Classes views

Alarm classes allow you to group alarms into categories and assign them alarm priority levels.

Figure 186. Alarm Classes view

Display Name	Priority	Total Alarm Count	Open Alarm Count	In Alarm Count	Unacked Alarm Count	Time Of Last Alarm
High	250	0	0	0	0	null
Low	150	0	0	0	0	null
Medium	150	16	16	15	16	29-Jun-18 3:39 PM EDT



This view opens when you click the Alarm Classes submenu, under the System Setup > Alarm Setup menu.

### Buttons

In addition to the standard buttons: Column Chooser, Filter, Manage Reports, and Export these control buttons manage this view:

- Add opens a view or window for creating a new record in the database.
- Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
- Edit Priority changes the numerical priority level of any selected alarm class.

**NOTE:** To configure multiple alarms with the same priority, select and edit more than one alarm class record at a time.

-  Delete removes the selected record (row) from the database table. This button is available when you select an item.
-  Rename opens the Rename window with which to change the name of the selected item.

## Columns

The following are the columns in the Alarm Classes table.

**Table 58.** Alarm Class columns

Column	Description
Display Name	Reports the name that describes the event or function.
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to <i>Offnormal</i> , from normal to <i>Fault</i> , from <i>offnormal</i> , <i>fault</i> or <i>alert</i> to <i>Normal</i> , and from normal to <i>Alert</i> ).The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Total Alarm Count	Displays the total number of alarms assigned to the alarm class from all sources.
Open Alarm Count	Displays the total number of current alarms. An alarm is considered to be open when it is not acknowledged and normal or not acknowledged and in alarm.
In Alarm Count	Displays the total number of alarm sources.
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Reports the time that the system generated the last alarm assigned to this alarm class.

## Add New (or edit) Alarm Class view

Alarm classes manage alarm priority and which alarm requires acknowledgment. This view configures, name and save alarm classes. You link alarm classes with alarm recipients.



Figure 187. Add New Alarm Class

HomeMonitoringPersonnelReportsSystem SetupThreat Levels

SchedulesUser ManagementBackupsRemote DevicesAccess SetupIntrusion SetupAlarm

SaveAlarm Classes

Display NameAlarm Class

Alarm ClassRecipientsRelay Links

Ack Required☐ Normal☒ Offnormal☒ Fault☒ Alert

PriorityOffnormal255Fault255Normal255Alert255

Total Alarm Count0

Open Alarm Count0

In Alarm Count0

Unacked Alarm Count0

Time Of Last Alarm31Dec196907:00PMEST

Escalation Level1 Enabledfalse


Escalation Level1 Delay00000h05m[1min - +inf]

Escalation Level2 Enabledfalse

Escalation Level2 Delay00000h15m[2mins - +inf]

Escalation Level3 Enabledfalse

Escalation Level3 Delay00000h30m[3mins - +inf]

To access this view, click **Controller (System) Setup > Alarm Setup** and click the Add control button (  ) at the top of the Alarm Classes view or double-click an existing alarm class (to edit its properties).

You can move among tabs without losing unsaved data, however, you must click the **Save** button before leaving the view or data is lost and no new record is added to the database.

**NOTE:** When you create a new alarm class, you must assign at least one alarm recipient and one alarm class to it before saving it.

Links

A **Save** button and an Alarm Classes view links are located directly above a **Display Name** property at the top of the view. This property provides a unique name for the alarm class.

Properties

Property	Value	Description
Ack Required	true or false	Indicates that any alarm assigned to this alarm class requires acknowledgment. Only selected component state transitions (normal to offnormal, fault or alert) require acknowledgment.

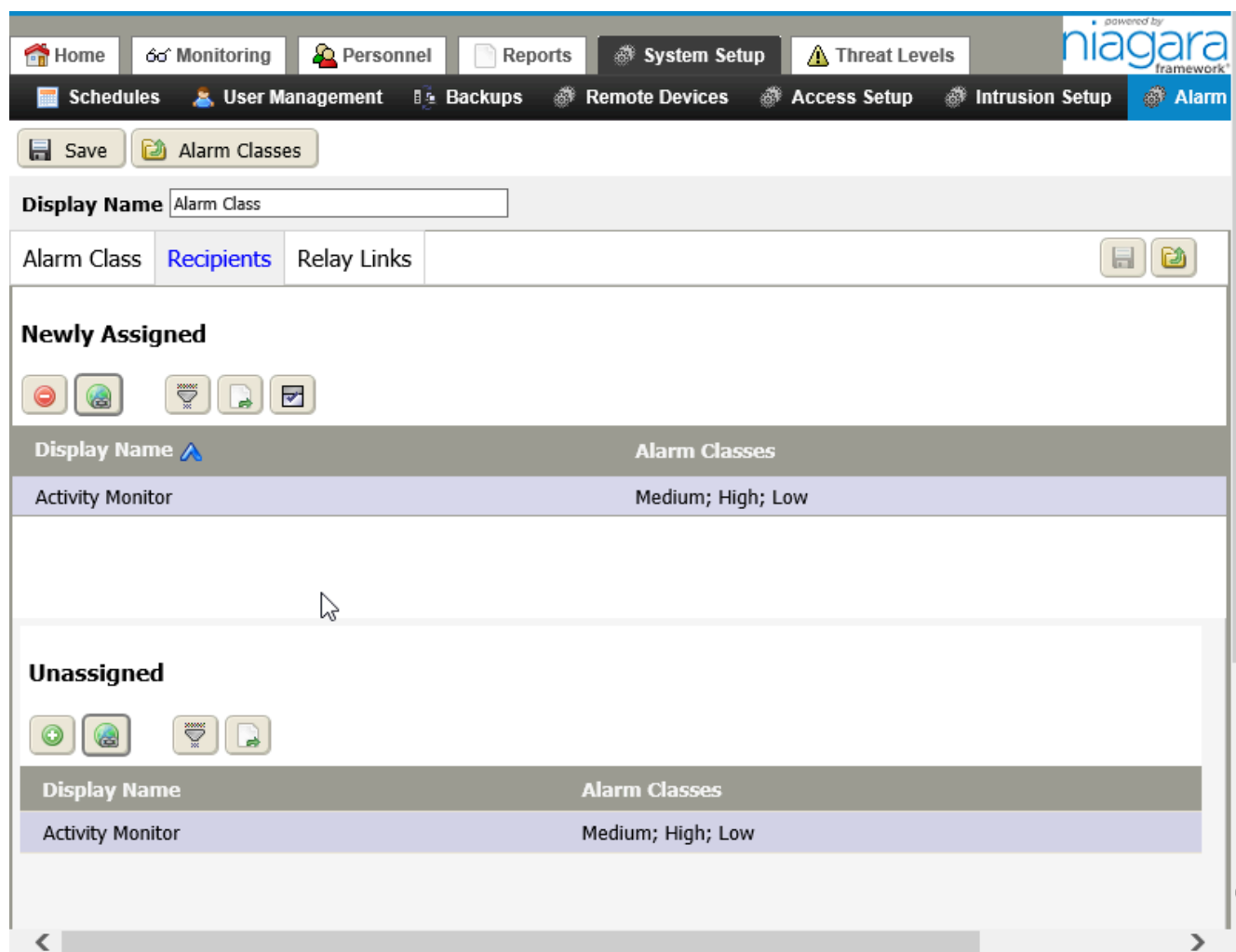
Property	Value	Description
Priority	number for each of four component states	<p>Define the priority level to assign to the alarm class for each component state transition (from normal to offnormal, from normal to fault, from normal to alert, from offnormal to fault and from alert to normal.</p> <p>The lower the number, the more significant the alarm. The highest priority alarm is number 1.</p>
Total Alarm Count	read-only	Displays the total number of alarms assigned to the <code>Alarm class</code> from all sources.
Open Alarm Count	read-only	Displays the total number of current alarms. An alarm is considered to be open when it is not acknowledged and normal or not acknowledged and in alarm.
In Alarm Count	read-only	Displays the current total number of alarms that are unacknowledged and normal or unacknowledged and an alert.
Unacked Alarm Count	read-only	Displays the total number of unacknowledged alarms.
Time of Last Alarm	read-only	Displays when the system generated the last alarm assigned to this <code>Alarm class</code> .
Escalation Level1n Enable, where n is 1, 2 or 3	true or false	Turns on (true) and off (false) escalation of the alarm at this priority level.
Escalation Leveln Delay, where n is 1, 2 or 3	hours and minuets (One minute is the smallest increment you can set.)	Defines the amount of time to allow an unacknowledged alarm to remain unacknowledged before the system escalates it to the next level.

## Recipients tab

This tab provides a way to manually assign or unassign alarm recipients to the alarm class.

If there is only one console recipient, the system automatically assigns it to the class or zone when creating a new alarm class or intrusion zone. If additional console recipients are available, you must manually choose and assign the console recipient using the Recipients tab before saving the new alarm class or intrusion zone.





Alarm recipients receive alarm notification as specified by the specific alarm recipient properties. You can add items to the currently displayed alarm class using the learn mode and the Assign and Unassign buttons.

**Figure 188.** Edit Alarm Class (Recipients tab)

You access this view from the main menu by clicking **Controller (System) Setup > Alarm Setup > Alarm Classes**, double-clicking an alarm class row in the table, and clicking the Recipients tab.

#### Buttons

In addition to the standard buttons: Filter and Export, these buttons serve the Recipients tab:

-  Assign moves a discovered item from the Unassigned view to the Assigned view.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  Assign Mode identifies all unassigned console recipients and displays them at the bottom of the view.
-  Assign Mode buttons open and close the Unassigned pane.

Columns

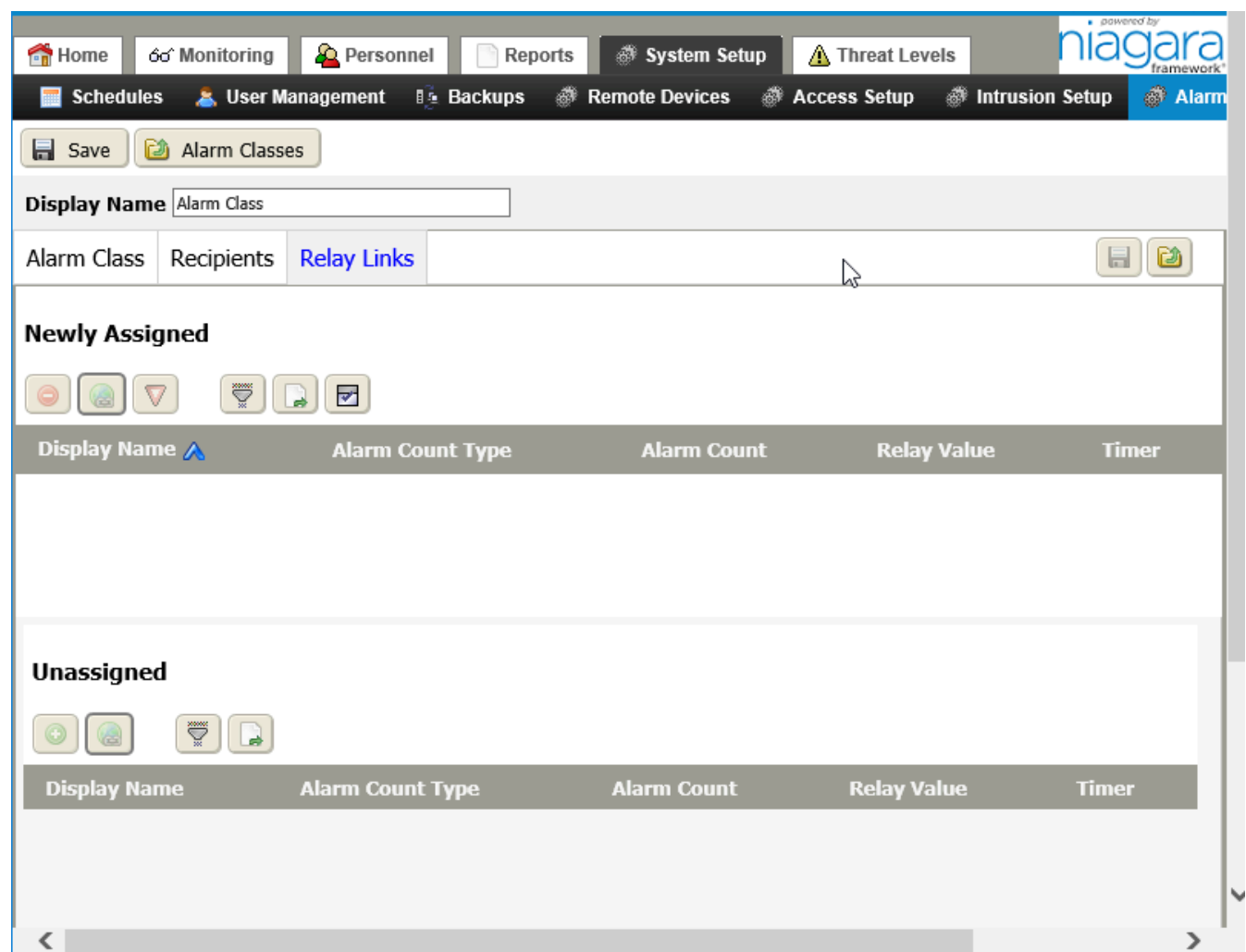
Table 59. Recipients tab columns

Column	Description
Display Name	Identifies the name of the recipient.
Alarm Classes	Lists the alarm classes.

Relay Links tab

This tab manually assigns or unassign output relays to the alarm class. You add items to the currently displayed alarm class using the learn mode and the Assign and Unassign buttons.





Figure 189. Relay Links tab



You access this view from the main menu by clicking **Controller (System) Setup > Alarm Setup > Alarm Classes**, followed by clicking the Relay Links tab.

Buttons

In addition to the standard Filter and Export buttons, these buttons serve this tab:

-  Delete removes the selected record (row) from the database table. This button is available when you select an item.
-  opens an selected relay link.
-  Turn Off Relays turns Off Relays manually disables an output relay.
-  Assign Mode buttons open and close the Unassigned pane.

Columns

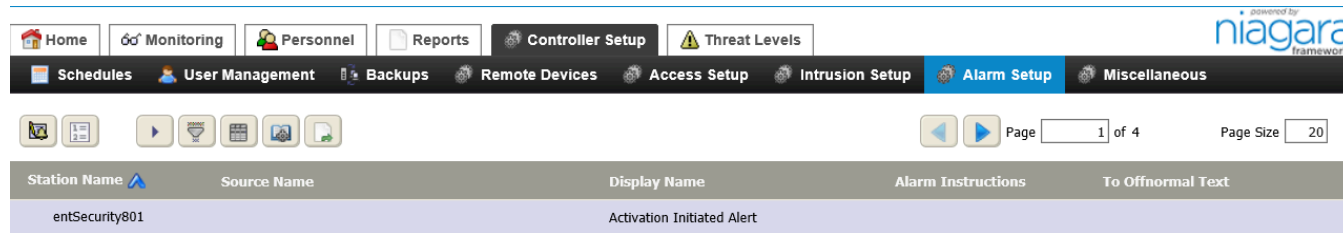
Column	Description
Display Name	Identifies the name of the alarm class.
Alarm Count type	Identifies one of four alarm states that are counted and used to generate an action. Alarm Count Type is configured using the Add New Alarm Count to Relay view.  Unacked Alarm Count reports the number of alarms that have not been acknowledged.  Open Alarm count reports the number of alarms that have not been cleared from the console.  In Alarm Count reports the number of alarms that have not yet returned to normal.  Total Alarm Count reports the number of all alarms regardless of alarm state.
Alarm Count	Displays the current alarm count for alarms of the type specified in the Alarm Type Count property.
Relay Value	Displays a boolean output value (true or false) for linking into a relay control component.
Timer	Displays a value that identifies how long the Relay Out values is being held in the active (true) state.

Alarm Instructions view

This view displays a standard table-type report that provides a way to view, assign, and edit alarm instructions in the system.

Buttons

Figure 190. Alarm Instructions view



This view opens when you click the Alarm Instructions submenu, under the Controller (System) Setup > Alarm Setup menu.

In addition to the standard buttons (Filter, Column Chooser, Manage Reports, and Export), these buttons support alarm instructions:



- Edit Instructions opens the **Edit Instructions** window for the selected instruction row.



- Master Alarm Instructions opens the **Master Instructions** window.

## Columns

Column	Description
Station Name	Reports the name of the station under the control of which the event occurred.
Source Name	Reports the component that transitioned from normal to offnormal, fault, or alert. If defining search criteria, you can use wild cards here.
Display Name	Reports the name that describes the event or function.
Alarm Instructions	Displays the actual alarm instruction text.
To Offnormal Text	Displays the text that displays when an Offnormal alarm condition occurs.
Path	Identifies the system path to the location of the source point alarm extension.

## Edit Instructions window

To open this window, select a single row in the Alarm Instructions table and click the Edit Instructions control button.

**Figure 191.** Edit Instructions window

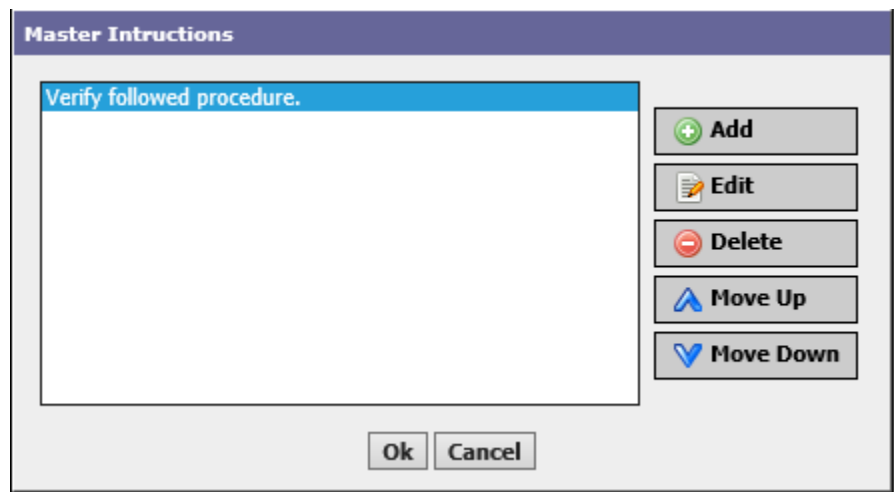
Access this view by selecting **Controller Setup > Alarm Setup > AlarmInstructions**. Then select a row and right click Or select a row and click on edit button on left above the table

Use the **Add**, **Edit**, **Delete**, **Move Up**, and **Move Down** buttons to edit, arrange, and add alarm instructions to the desired alarm extensions.

Master Instructions window

Master alarm instructions are a list of saved text that you select and assign to one or more points (in other views). This window displays a list of all existing Master Alarm Instructions.

Figure 192. Master Instructions window



Use the **Add**, **Edit**, **Delete**, **Move Up**, and **Move Down** buttons to edit, arrange, and add alarm instructions to the desired alarm extensions.

Alarm Relays view (Alarm Count Relays)

Alarm relays provide a way for you to create a relay output action in response to a specified number of alarms. For example, you may want to have a light or a beeper turn on after three unacknowledged alarms. You would use an alarm relay for this purpose.

Buttons

Figure 193. Alarm Relays view

SchedulesUser ManagementBackupsRemote DevicesAccess SetupIntrusion SetupAlarm SetupMiscellaneous

Display Name	Alarm Count Type	Alarm Count	Relay Value	Timer
Alarm Count To Relay	Open Alarm Count	0	false {ok}	2mins
Alarm Count To Relay1	Total Alarm Count	0	false {ok}	2mins

This view opens when you select the **Alarm Count Relays** submenu, under the **System Setup > Alarm Setup** menu.

This view displays standard controls across the top and a table of all alarm relay configurations in the lower part.

Columns

Each entry in the Alarm Relays table represents a single alarm-count-to-relays configuration. The columns in the


table include a Name, Alarm Count Type (total alarms, unacked alarms, and others), Alarm Count, Relay Value, Timer setting, and any other columns that you have added to customize the display.


### Add New (or edit) Alarm Count To Relay view


This view configures alarm count to relay options.

Links

**Figure 194.** Add New Alarm Count to Relay view

 Save

 Test

 Alarm Count To Relays

Alarm Count To Relay

Alarm Classes

Relays

Relay Out

false {ok}

Timer

+

▼

00000

h

02

m

00

s

Alarm Count Type

Open Alarm Count ▼

To access this view, click **Controller (System) Setup > Alarm Setup > Alarm Count Relays**, click on the Add

button () or double-click an existing count relay to open an existing alarm-count-to-relay record.

If you are editing an existing record, the alarm-count-to-relay configuration name displays in the title of the view over the **Save**, **Test**, and **Alarm Count To Relays** links.

You can move among tabs without losing unsaved data, however, you must click the **Save** button before leaving the view or data is lost and no new record is added to the database.

The **Test** button causes the relay to cycle on and off. The **Alarm Count To Relays** link returns to the Alarm Count To Relays view.

Properties

Property	Value	Description
Relay Out	read-only	Displays the current relay output value and status.
Timer	minutes seconds milliseconds	Sets the active duration of the relay output.
Alarm Count Type	drop-down list	Defines the type of alarm states that are counted and used to generate an action. <b>Unacked Alarm Count</b> counts alarms that have not been acknowledged. <b>Open Alarm count</b> counts alarms that have not been cleared from the console. <b>In Alarm Count</b> counts alarms that have not yet returned to normal. <b>Total Alarm Count</b> counts all alarms regardless of



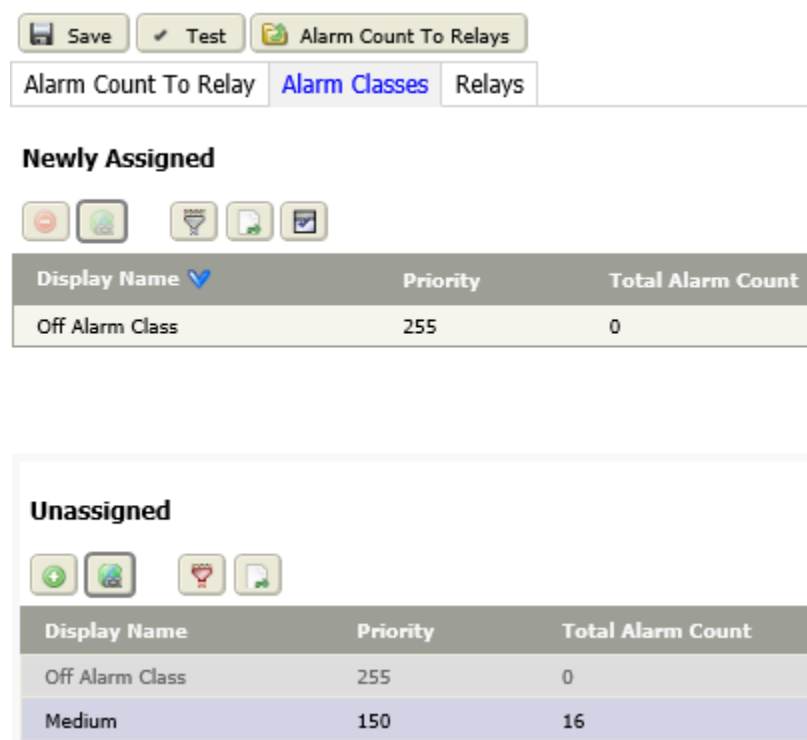
Property	Value	Description
		state.


Alarm Classes tab

This tab manually assigns and unassigns alarm classes to the current alarm-count-to-relay action.



Buttons

**Figure 195.** Add New Alarm Count To Relay view Alarm Classes tab



To access this view, click **Controller (System) Setup > Alarm Setup > Alarm Count Relays**, click on the Add button (  ) or double-click an existing count relay and click the Alarm Classes tab.

In addition to the standard buttons (Filter, and Export), these buttons support Alarm Relay Alarm Classes:

-  Hyperlink opens an existing class.
-  Assign Mode buttons open and close the Unassigned pane.

Columns

Column	Description
Display Name	Reports the name that describes the event or function.
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to Offnormal, from normal to Fault, from

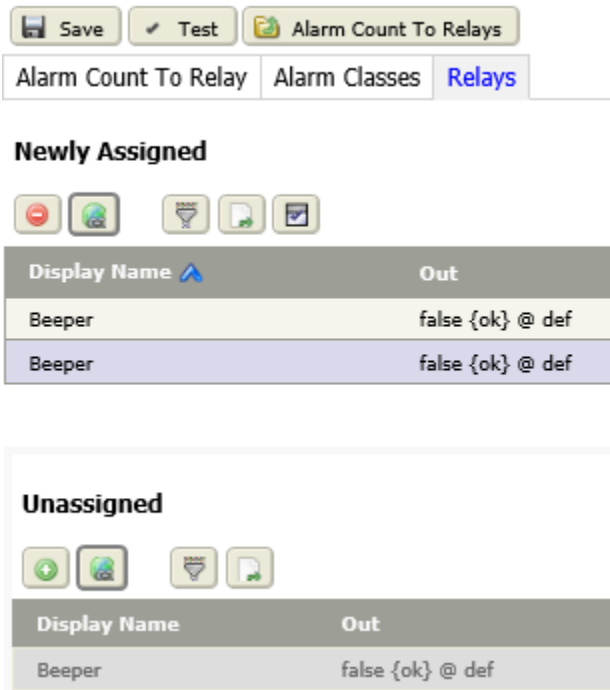
Column	Description
	offnormal, fault or alert to <b>Normal</b> , and from normal to <b>Alert</b> ).The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Total Alarm Count	Displays the total number of alarms assigned to the alarm class from all sources.
Open Alarm Count	Displays the total number of current alarms. An alarm is considered to be open when it is not acknowledged and normal or not acknowledged and in alarm.
In Alarm Count	Displays the total number of alarm sources.
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Reports the time that the system generated the last alarm assigned to this alarm class.


Relays tab

This tab is to provides a way to manually assign or unassign relays to the current alarm-count-to-relay action.



Buttons

Figure 196. Add New Alarm Count To Relays tab



To access this view, click **Controller (System) Setup > Alarm Setup > Alarm Count Relays**, click on the Add button (  ) or double-click an existing count relay and click the Relays tab.

**NOTE:** If you assign a relay that is already assigned, an error message appears when you save the configuration.

This view uses standard control buttons. You add relays to the currently-displayed configuration using assign mode, the assign and unassign buttons ( ).


Column	Description
Display Name	Reports the name that describes the event or function.
Out	Reports the slot output value.
In10	Reports input control points value for the relay.
In16	Reports input control points value for the relay.
To Display Path String	Defines the station path for this zone.


EmailService view (Email Accounts)

This view manages email accounts, which are used as alarm recipients.

Links

Figure 197. EmailService view

 Save

 Manage Accounts

Email Service

Outgoing Account

Incoming Account

Status

{disabled}

Fault Cause

Enabled

false ▼

This view opens when you select the **Email Accounts** menu item under the **System Setup > Alarm Setup** menu.

The default view displays a title over the **Save** and **Manage Accounts** buttons. If no email accounts are set up, the view contains only a single **Email Service** tab. Use the **Manage Accounts** button to add and remove email accounts. A tab appears for each email account you add to the view.

Properties

Property	Value	Description
Status	read-only	Reports the condition of the entity or process at last polling.  {ok} indicates that the component is licensed and polling successfully.  {down} indicates that the last check was unsuccessful, perhaps because of an incorrect property, or possibly loss of network connection.

Property	Value	Description
		<p><code>{disabled}</code> indicates that the <b>Enable</b> property is set to <code>false</code>.</p> <p><code>{fault}</code> indicates another problem. Refer to <b>Fault Cause</b> for more information.</p>
Fault Cause	read-only	Indicates the reason why a system object (network, device, component, extension, etc.) is not working (in fault). This property is empty unless a fault exists.
Enabled	true or false	Activates ( <code>true</code> ) and deactivates ( <code>false</code> ) use of the object (network, device, point, component, table, schedule, descriptor, etc.).

Outgoing Account tab

This tab displays all the properties for the outgoing account associated with the EmailService.

Properties

Figure 198. Outgoing Account properties

SaveManage Accounts

Email ServiceOutgoing AccountIncoming Account

Hostname

Port

25

[-1 - +inf]

Account

Password

••••••••

Pollrate

00000

h

01

m

00

s

[1sec - +inf]

Enabled

false

Status

{disabled}

Last Poll Success

31

Dec

1969

07

:

00

PM

EST

Last Poll Failure

31

Dec

1969

07

:

00

PM

EST

Last Poll Failure Cause

Debug

false

Use Ssl

false

Use Start Tls

false

Transport

Smtpt

Connection Timeout

+

00000

h

00

m

10

s

Use Authentication

false

Reply To

Persistent

false

Persistence Directory

file:^email

Allow Disabled Queueing

false

Queue Size

0

Max Queue Size

100

[1 - +inf]

Number Sent

0

Max Sendable Per Day

100

[1 - +inf]

Number Discarded

0

Last Discard

31

Dec

1969

07

:

00

PM

EST

Last Discard Cause

To access this view, click **Controller (System) Setup > Alarm Setup > Email Accounts**, followed by clicking the **Outgoing Account** tab.

In addition to the standard properties (**Enabled** and **Status**), these properties support an outgoing account.

Property	Value	Description
Hostname	text	Identifies the name of the mail server. For example, mail.acme.com could be a Hostname.
Port	number from -1 to infinity; defaults	Identifies the port number

Property	Value	Description
	to 25	associated with the email account. Typically, this value is "25", however, if you set it to "-1" the system searches for and uses a valid port.
Account	text	Identifies the name of the distinct account that is authorized for access to the <code>Hostname</code> mail server. For example, if you are using an email account named "myemail@acme.com" on the host described above, the account name is simply "myemail". The <code>Hostname</code> in this case could be "mail.acme.com".
Password	text and special characters	Defines the login credential for the Account.
Pollrate	hours minutes seconds	Specifies how often the account executes a send action. Increasing the pollrate value increases the time between polls. During the time between polls, emails may be queued (up to the max queue size) until the next poll time. At the next poll time all queued emails are sent.
Last Poll Success	read-only	Indicates the time (in hours and minutes) of the last polling success.
Last Poll Failure	read-only	Indicates the time (in hours and minutes) of the last polling failure
Last Poll Failure Cause	read-only	Provides an error message to indicate a reason for polling failure.
Debug	true or false (default)	Turns Debug mode on and off. When on, a station's standard output view (Workbench Platform > Application Director) displays debug information when the station tries to send or receive email. This can be used to troubleshoot accounts and faults.
Use Ssl	true or false (default)	Enables (true) and disables (false) Ssl (Secure Sockets Layer) for communication with a host email server that requires it.
Use Start Tls	true or false (default)	Enables (true) and disables (false) Tls (Transport Layer Security) for a host email server that requires it.
Transport	drop-down list	Selects from available options for

Property	Value	Description
		email communication. The default setting and most common is SMTP.
Connection Timeout	hours minutes seconds	Controls how long the station waits for a response from the mail server before generating an exception and setting the fault cause. It waits for the next scheduled poll and attempts to contact the mail server again at that frequency.
User Authentication	true or false (default)	Specifies that login credentials are required for sending any email. Sometimes authentication is not required for emails routed to recipients in the same domain. Setting this property to true makes the login credentials mandatory for any email
Reply To	text	Specifies the contents of the From: property in the email that is sent.
Persistent, Persistence Directory	true or false (default)	true saves each queued email as an xml file in the designated persistence directory. Once the emails are actually sent, the xml files are deleted from the directory. The purpose of this is to keep a copy of the emails in the queue, which would be lost if the station was stopped prior to the emails being sent. When the station restarts, emails are loaded from the "Persistent Directory" back to the queue.
Allow Disabled Queuing	true or false (default)	Emails reside in a queue while they wait to be sent. Assuming that the Account Status is {ok}, typically, the length of time an email is in the queue depends on the Pollrate setting. Several properties relate to the queue and email management. A setting of true) allows emails to reside in the queue even when the Enabled status is set to false.
Queue Size	read-only	Indicates how many emails are currently in the queue (waiting to be sent).
Max Queue Size	number from 1 to infinity; default = 100	Specifies how many emails are allowed to occupy the queue.
Number Sent	read-only	Displays the number of emails that have been sent.

Property	Value	Description
Max Sendable Per Day	number	Specifies how many emails may be sent in one day.
Number Discarded	read-only	Indicates how many emails did not successfully send.
Last Discard	read-only	Indicates when the last email did failed to send.
Last Discard Cause	read-only	Displays an error message that indicates the cause of the last email send failure.

## Incoming Account tab

This tab displays all the properties for the incoming account associated with the account.

### Properties

**Figure 199.** Incoming Account tab

Save

Manage Accounts

Email Service

Outgoing Account

Incoming Account

Hostname

Port

110

[-1 - +inf]

Account

Password

••••••••

Pollrate

00000

h

01

m

00

s

[1sec - +inf]

Enabled

true

Status

{disabled}

Last Poll Success

31

Dec

1969

07

:

00

PM

EST

Last Poll Failure

31

Dec

1969

07

:

00

PM

EST

Last Poll Failure Cause

Debug

false

Use Ssl

false

Use Start Tls

false

Store

Pop3

Delivery Policy

Delete

Email To Read

Unread Email

To access this view, click **Controller (System) Setup > Alarm Setup > Email Accounts**, followed by clicking the Incoming Account tab.



**CAUTION:** With the default configuration (refer to **Delivery Policy** property, below) the incoming email account deletes all emails from the mail server when it checks the account to retrieve new email, even if the emails are already marked as read by another email client. If permanent retention of the emails is required then do one of the following: (1) change the Delivery Policy setting from **Delete** to **Mark As Read** or **Mark as Unread** OR (2) configure a second service account which the mail server forwards emails to and configure the station's incoming account to check the second service account.

In addition to the standard properties (**Enabled** and **Status**), these properties support an incoming account.

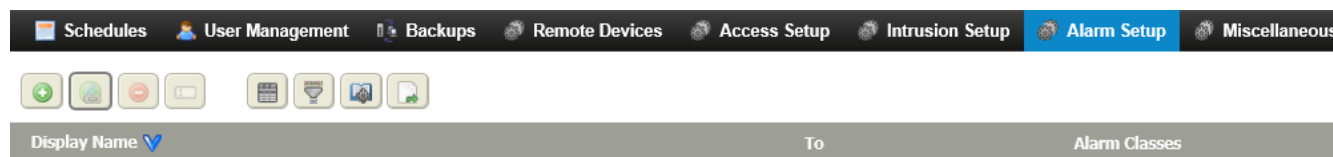
Property	Value	Description
Hostname	text	Identifies the name of the mail server. For example, mail.acme.com could be a Hostname.
Port	number from -1 to infinity; defaults to 110	Identifies the port associated with the email account. Typically, this number is 110, however, to set -1 the system searches for and uses a valid port.
Account	text	Identifies the name of the distinct account that is authorized for access to the <b>Hostname</b> mail server. For example, if you are using an email account named controls@acme.com on the host described above, the account name is controls. The <b>Hostname</b> in this case could be mail.acme.com.
Password	text	This is the login credential for the account specified in the previous property.
Pollrate	hours minutes seconds	Specifies how often the account connects to the mail server and checks or unread mail messages. Increasing this value increases the time between polls.
Last Poll Success	read-only hours and minutes	Displays the time (of the last polling success).
Last Poll Failure	read-only hours and minutes	Displays the time (of the last polling failure).
Last Poll Failure Cause	read-only	Indicates a reason for polling failure.
Debug	true or false (default)	Turns Debug mode on and off. When on, a station's standard output view (Workbench Platform > Application Director) displays debug information when the station tries to send or receive email. This can be used to troubleshoot accounts and faults.

Property	Value	Description
Use Ssl	true or false (default)	Enables (true) and disables (false) Ssl (Secure Sockets Layer) for communication with a host email server that requires it.
Use Start Tls	true or false (default)	Enables (true) and disables (false) Tls (Transport Layer Security) for a host email server that requires it.
Store	drop-down list: Pop 3, Imap	Selects the mail retrieval standard. Choose the option that is in use by your host mail server.
Delivery Policy	drop-down list: Delete, Mark as Read, Mark as Unread	<p>Selects how the incoming email account handles incoming emails at the mail server.</p> <p>Delete removes all emails from the mail server when it checks the account to retrieve new email, even if the emails are already marked as read by another email client</p> <p>Mark As Read marks all emails as read on the mail server when it checks the account to retrieve new email.</p> <p>Mark As Unread marks all emails as unread on the mail server when it checks the account to retrieve new email.</p>

## Email Recipients view

The email recipient is like other alarm recipients except that the alarm may be formatted into an email message and delivered to another destination.

**Figure 200.** Email Recipients view



This view opens when you click the **Email Recipients** submenu under the **System Setup > Alarm Setup** menu.

The Email Recipients view displays a list of all existing email recipients.

Buttons

This view has standard controls across the top and a table of all existing email recipients in the lower part. Each existing recipient is listed in the table with a Name and To column, in addition to any other columns that you have added to customize the display.

Columns

Column	Description
Display Name	Displays the name of the email.
To	Indicates to whom the email was sent.
Alarm Classes	Reports the alarm class.

Add New (or edit) Email Recipient view

This view provides the properties to configure a new or existing email recipient record by using email routing parameters and assigning alarm classes.

Figure 201. Add New Email Recipient view

Save

Email Recipients

Display Name

Email Recipient

Email Recipient

Alarm Classes

Time Range

Start Time

12:00:00 AM EDT

End Time

12:00:00 AM EDT

Days Of Week

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Transitions

☒ Normal ☒ Offnormal ☒ Fault ☒ Alert

Route Acks

true

To

Cc

Bcc

Language

Email Account

None

Subject

Niagara Alarm From %alarmData.sourceName%

Body

Source: %alarmData.sourceName%  
Timestamp: %timestamp%  
State: %sourceState% / %ackState%  
Priority: %priority%  
Alarm Class: %alarmClass%  
Text: %alarmData.msgText%

To access this view, click **Controller (System) Setup > Alarm Setup > Email Recipients**, followed by clicking the

Add button (  ) to create a new recipient, or double-clicking the recipient row in the table to edit an existing recipient.

Links

A **Save** button and an **Email Recipients** view link are located directly above a **Display Name** property at the top of the view.

You can move between tabs without losing unsaved data, however, you must click the **Save** button before leaving the view or data is lost and no new schedule is added.

Properties

Property	Value	Description
Time Range	Two time properties: hours minutes	Set a limited period of time during a

Property	Value	Description
	seconds	day for the collection of alarms. <i>Start Time</i> defines when to begin alarm collection. <i>End Time</i> defines when to end alarm collection.
Start Time	Check Boxes	
End Time	Check Boxes	
Days Of Week	check boxes	Select specific days to collect alarms.
Transitions	Four check boxes	Select the specific alarm transitions to include or exclude as alarms to send to the alarm recipient. Only selected transitions are sent – even though all of the alarms are still saved into the alarm history.
Route Acks	true (default) or false	true routes Acks are to this recipient; false, routes only alarms (not Acks) to the recipient.
To, Cc, Bcc	text	Define to whom to send the message.
Language	text	Identifies the ISO 639 language code for the language associated with the line printer. This is a two letter code (lower-case preferred). Refer to the following link for the complete list of codes: <a href="http://www.loc.gov/standards/iso639-2/langcodes.html">http://www.loc.gov/standards/iso639-2/langcodes.html</a>
Email Account	drop-down list	Identifies the email account to use.
Subject	text	Defines the subject line of the email.
Body	additional properties	Refer to <a href="#">Email body</a>

### Email body

This property has the following editable default additional properties.

Property	Value	Description
Source	%alarmData.sourceName%	Sends the source name of the alarm to print on the first line.
Timestamp	%timestamp%	Sends the timestamp of the alarm to print on the second line.
State	%sourceState% / %ackState%	Sends the alarm state and the acknowledged state to print on the

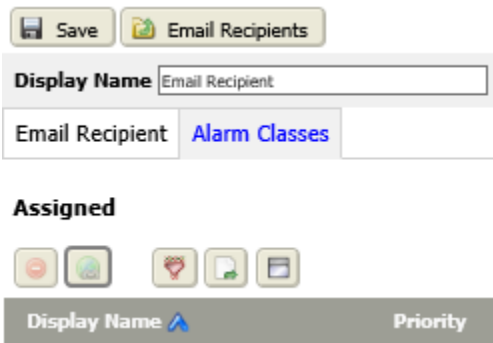
Property	Value	Description
		third line.
Priority	%priority%	Sends the alarm priority to print on the fourth line.
Alarm Class	%alarmClass%	Sends the alarm class to print on the fifth line.
Text	%alarmData.msgText%	Sends the alarm message to print on the sixth line.

Alarm Classes tab

This tab provides a way to manually assign or unassign alarm classes to the current Email Recipient.

Buttons

Figure 202. Edit Email Recipient view



To access this view, click **Controller (System) Setup > Alarm Setup > Email Recipients**, and click the **Alarm Classes** tab.

This view uses standard control buttons.

You can add items to the currently displayed configuration using the learn mode, the Assign and Unassign

buttons ( ).

Columns

Column	Description
Display Name	Reports the name that describes the event or function.
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to Offnormal, from normal to Fault, from offnormal, fault or alert to Normal, and from normal to Alert).The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Total Alarm Count	Displays the total number of alarms assigned to the alarm class from all sources.

Column	Description
Open Alarm Count	Displays the total number of current alarms. An alarm is considered to be open when it is not acknowledged and normal or not acknowledged and in alarm.
In Alarm Count	Displays the total number of alarm sources.
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Reports the time that the system generated the last alarm assigned to this alarm class.

Alarm Consoles view

Alarm consoles display information about all open alarms that are associated with (or routed to) the console. You can create one or more alarm consoles, which allows you to group alarms into categories and assign them priority levels. Each must have one or more alarm classes assigned to it.

Buttons




Alarm consoles are sometimes called Alarm Console Recipients. The term “recipient” indicates that an Alarm Consoles view is receiving the alarms, as opposed to another type of recipient, such as an email recipient or station recipient.

Figure 203. Alarm Consoles view



You open this view by clicking on the **Console List** button in the top right corner of the Console Recipient view (**Monitoring**) or by selecting the **Alarm Consoles** submenu, under the **System Setup > Alarm Setup** menu.

In addition to the standard control buttons (Delete, Rename, Column chooser, Manage Reports, and Export), this view provides control buttons for these functions:

-  Add opens a view or window for creating a new record in the database.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  Alarm Console opens the Alarm Console view.

Columns

Column	Description
Display Name	The name for the alarm console.
Alarm Classes	Lists the alarm classes to appear in this alarm console. Classes are separated by semi-colons (;).

## Add (or edit) Alarm Console view, Alarm Classes tab

This tab associates an alarm class with a console recipient.

### Buttons

**Figure 204.** Console Recipients Alarm Classes tab

Save

Console Recipients

Display Name

Console Recipient

Alarm Classes

Newly Assigned

Display Name	Priority	Total Alarm Count	Open Alarm Count	In Alarm Count	Unacked Alarm Count	Time Of Last Alarm
Arm/Disarm	255	0	0	0	0	null




Unassigned

Display Name	Priority	Total Alarm Count	Open Alarm Count	In Alarm Count	Unacked Alarm Count	Time Of Last Alarm
Arm/Disarm	255	0	0	0	0	null
High	250	0	0	0	0	null
Low	150	0	0	0	0	null
Medium	150	24	6	6	3	04-Aug-18 6:56 AM EDT

This tab opens when you click **Controller (System) Setup > Alarm Setup > Alarm Consoles**, and click the plus button (



In addition to the standard buttons (Delete, Filter and Export) these buttons support console recipient alarm classes:

-  Assign moves a discovered item from the Unassigned view to the Assigned view.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  Assign Mode buttons open and close the Unassigned pane.



## Columns

Column	Description
Display Name	Reports the name that describes the event or function.
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to <i>Offnormal</i> , from normal to <i>Fault</i> , from offnormal, fault or alert to <i>Normal</i> , and from normal to <i>Alert</i> ).The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Total Alarm Count	Displays the total number of alarms assigned to the alarm class from all sources.
Open Alarm Count	Displays the total number of current alarms. An alarm is considered to be open when it is not acknowledged and normal or not acknowledged and in alarm.
In Alarm Count	Displays the total number of alarm sources.
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Reports the time that the system generated the last alarm assigned to this alarm class.

## Add (or edit) Alarm Console view, Alarm Classes tab

This tab associates an alarm class with a console recipient.

Buttons

Figure 205. Console Recipients Alarm Classes tab

SaveConsole Recipients

Display NameConsole Recipient

Alarm Classes

Newly Assigned

Display Name	Priority	Total Alarm Count	Open Alarm Count	In Alarm Count	Unacked Alarm Count	Time Of Last Alarm
Arm/Disarm	255	0	0	0	0	null

Unassigned




Display Name	Priority	Total Alarm Count	Open Alarm Count	In Alarm Count	Unacked Alarm Count	Time Of Last Alarm
Arm/Disarm	255	0	0	0	0	null
High	250	0	0	0	0	null
Low	150	0	0	0	0	null
Medium	150	24	6	6	3	04-Aug-18 6:56 AM EDT

This tab opens when you click **Controller (System) Setup > Alarm Setup > Alarm Consoles**, and click the plus button (



).

In addition to the standard buttons (Delete, Filter and Export) these buttons support console recipient alarm classes:

-  Assign moves a discovered item from the Unassigned view to the Assigned view.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  Assign Mode buttons open and close the Unassigned pane.

Columns

Column	Description
Display Name	Reports the name that describes the event or function.
Priority	Reports the priority level assigned to the alarm class for each component


Column	Description
	state transition (from normal to Offnormal, from normal to Fault, from offnormal, fault or alert to Normal, and from normal to Alert).The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Total Alarm Count	Displays the total number of alarms assigned to the alarm class from all sources.
Open Alarm Count	Displays the total number of current alarms. An alarm is considered to be open when it is not acknowledged and normal or not acknowledged and in alarm.
In Alarm Count	Displays the total number of alarm sources.
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Reports the time that the system generated the last alarm assigned to this alarm class.


Video Alarm Classes (Video Alarm Recipient) view

The Video Alarm Recipient is a special class that is used to specify properties related to routing alarms to a video surveillance system. The video alarm recipient is similar to other alarm recipients except that the alarm turns on video monitoring.

Properties

Figure 206. Video Alarm Recipient view

 Save

 Alarm Setup

Video Alarm Recipient

Alarm Classes

Time Range

Start Time

12:00:00 AM EDT

End Time

12:00:00 AM EDT

Days Of Week

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Transitions

☒ Normal ☒ Offnormal ☒ Fault ☒ Alert

Route Acks

true

Status

{ok}

Fault Cause

Default Time Range

Time Range ? to ?

Preset On Normal

true

This view opens when you click the Video Alarm Classes submenu under the System Setup > Alarm Setup menu.

For related video information refer to the “Video Installation” chapter in the Niagara Enterprise Security Installation and Maintenance Guide.

In addition to the standard properties (**Status** and **Fault Cause**), these properties support an video alarm recipients.

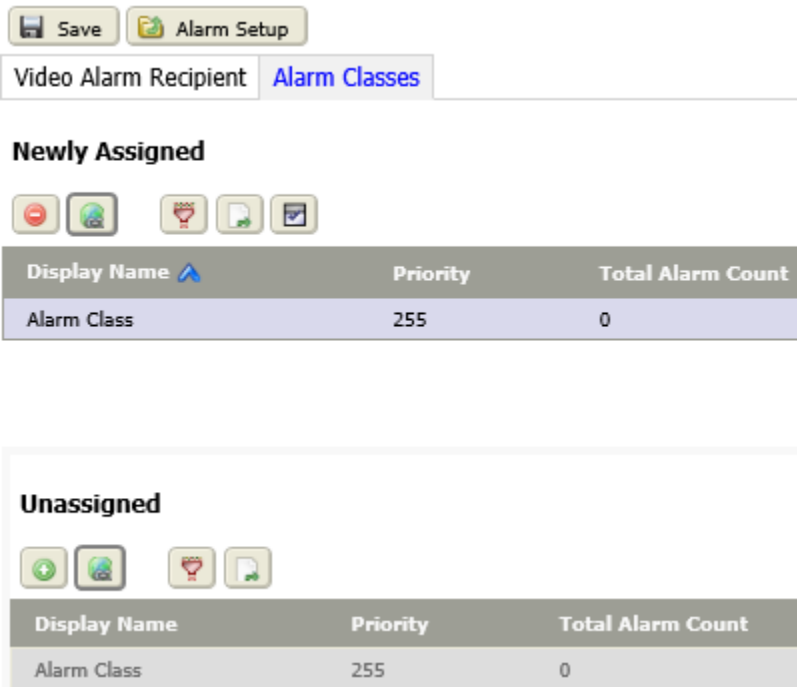
Property	Value	Description
Time Range	Start Time, End Time	Specify when during the day (start and stop times) this recipient receives alarms.
Days of Week	check boxes	Specifies the days of the week to include.
Transitions (general)	drop-down list	<p>Selects which alarm transitions to display in the console. Only those transitions selected display although the station saves all transitions in alarm history.</p> <p>Options are: toOffnormal, toFault, toNormal, toAlert</p>
Route Acks	true (default) or false	Enables (true) and disables (false) the routing of alarm acknowledgements to the recipient. The framework does not route trap (event notification) acknowledgements if you select false.
Default Time Range	drop-down list and additional properties	Suggests a variety of pre-defined time ranges.
Preset on Normal	true (default) or false	Moves the camera to a preset position when a video alarm returns to normal (true) or leaves the camera at the current position (false) .

## Alarm Classes tab

This tab provides a way to manually assign or unassign alarm classes to the recipient. Recipients receive alarm notification as specified by the specific alarm classes assigned to them.

Buttons

**Figure 207.** Video Alarm Recipient Alarm Classes tab



To access this view, click **Controller (System) Setup > Alarm Setup > Video Alarm Classes**, and click the **Alarm Classes** tab.

This view uses standard control buttons.

You can add items to the currently displayed configuration using the learn mode, the Assign and Unassign

buttons ( ).

Columns

Column	Description
Display Name	Reports the name that describes the event or function.
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to Offnormal, from normal to Fault, from offnormal, fault or alert to Normal, and from normal to Alert).The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Total Alarm Count	Displays the total number of alarms assigned to the alarm class from all sources.
Open Alarm Count	Displays the total number of current alarms. An alarm is considered to be open when it is not acknowledged and normal or not acknowledged and in alarm.
In Alarm Count	Displays the total number of alarm sources.
Unacked Alarm Count	Displays the total number of unacknowledged alarms.

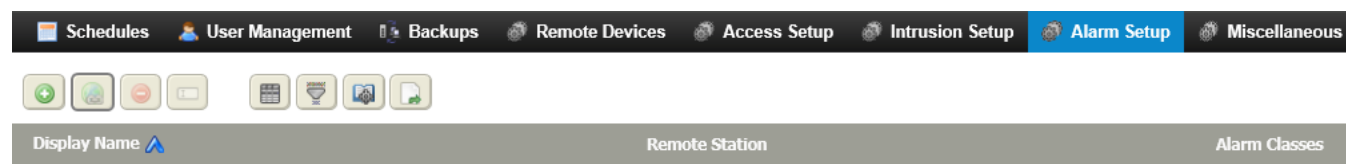
Column	Description
Time of Last Alarm	Reports the time that the system generated the last alarm assigned to this alarm class.

## Station Recipients views

The station recipient is like other alarm recipients (such as the email recipient) except that the alarm is routed directly to another station.




### Buttons

**Figure 208.** Station Recipients view



This view opens when you click the **Station Recipients** submenu under the **System Setup > Alarm Setup** menu. The Station Recipients view displays a list of all existing station recipients. Each existing recipient is listed in the table with a Name and a Remote Station column, in addition to any other columns that you have added to customize the display.

In addition to the standard buttons (Delete, Rename, Filter, Manage Reports, and Export), these buttons support station recipients:

-  Add creates a new station recipient record in the database.
-  Hyperlink opens an selected recipient.
-  Assign Mode buttons open and close the Unassigned pane.

## Add New (or edit) Station Recipient view

This view allows you to create and configure a new station recipient by choosing a station to route alarms to and assigning alarm classes.

**Figure 209.** Add New Station Recipient view

Save

Station Recipients

Display Name

Station Recipient

x


Station Recipient

Alarm Classes

Remote Station

Select Station...

To access this view, click **Controller (System) Setup > Alarm Setup > Station Recipients**, followed by clicking the

Add control button (  ) at the top of the view, or by double-clicking an entry in the table (to edit the recipient).

A **Save** button and an **Station Recipients** link are located directly above a **Display Name** text property at the top of the view. You can move between tabs without losing unsaved data, however, you must click the **Save** button before leaving the view or data is lost and no new schedule is added.

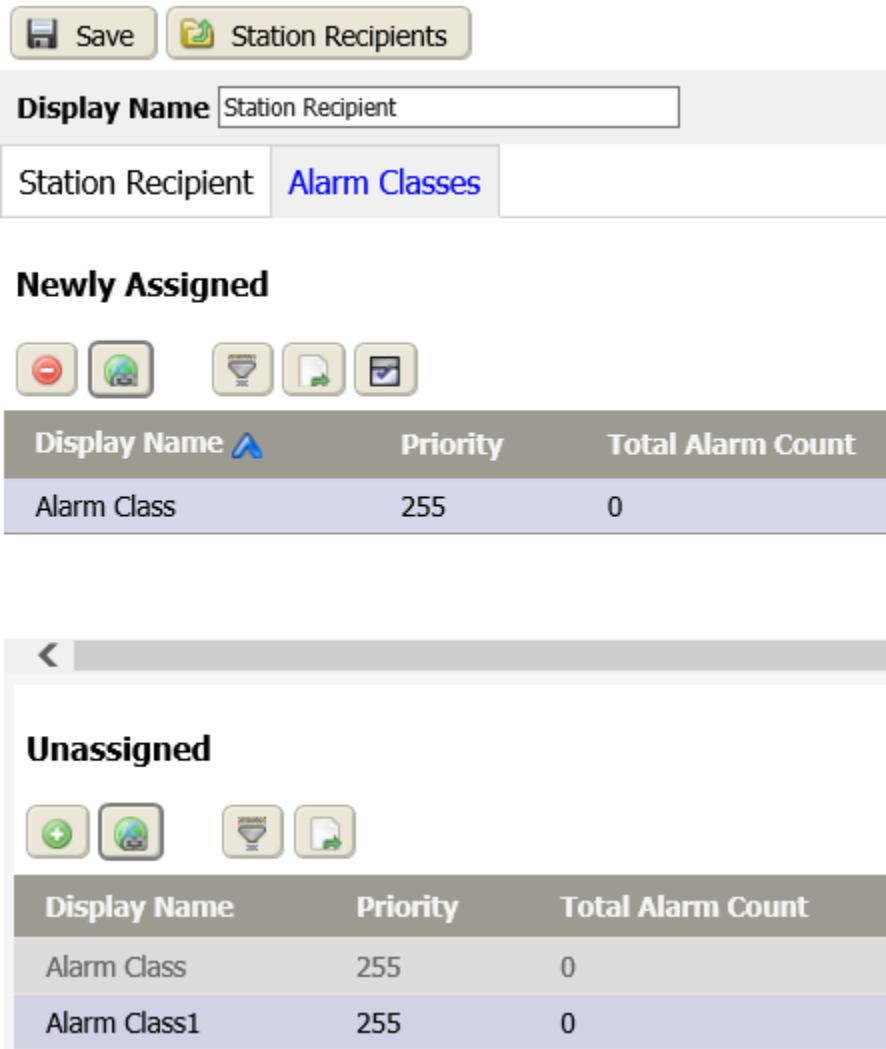
The **Remote Station** property specifies the station to route alarms to. Stations that are available on the system network are available in the option list.

**Alarm Classes tab**

This tab manually assigns and unassigns alarm classes to a station recipient. Recipients receive alarm notification as specified by the specific alarm classes assigned to them.

Buttons



**Figure 210.** Add New Station Recipient Alarm Classes tab



To access this view, click **Controller (System) Setup > Alarm Setup > Station Recipients**, followed by double-clicking a recipient row in the table and clicking the Alarm Classes tab.

**NOTE:** You cannot save an Alarm Console Recipient, Station Recipient, or Email Recipient unless that recipient has at least one alarm class or intrusion zone assigned to it.

This view uses standard control buttons.

You can add items to the currently displayed configuration using the learn mode, the Assign and Unassign buttons (   ).

Columns

Column	Description
Display Name	Reports the name that describes the event or function.



Column	Description
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to Offnormal, from normal to Fault, from offnormal, fault or alert to Normal, and from normal to Alert).The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.The lower the number, the more significant the alarm. The highest priority alarm (most significant) is number 1.
Total Alarm Count	Displays the total number of alarms assigned to the alarm class from all sources.
Open Alarm Count	Displays the total number of current alarms. An alarm is considered to be open when it is not acknowledged and normal or not acknowledged and in alarm.
In Alarm Count	Displays the total number of alarm sources.
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Reports the time that the system generated the last alarm assigned to this alarm class.

## Power alarm Setup (PlatformServices) view

This view configures the way your system monitors power sources for the associated controller.

### Links

**Figure 211.** Power Alarm Setup view

**PlatformServices**

Save

**Platform Service Container**

Platform Alarm Support »

**Alarm Class** Default Alarm Class ▼

**Source Name** %parent.displayName%

**Alert Text**

**To Fault Text** %lexicon(platPower:batteryTestFail)%

**To Offnormal Text**

**To Normal Text** %lexicon(platPower:batteryTestPassed)

**Hyperlink Ord** null

**Sound File** null

**Alarm Icon** null

**Meta Data** alarmType=nimhBattery

**Nimh Battery Alarm Support** Platform Alarm Support »

**Sla Battery Alarm Support** Platform Alarm Support »

**Power Alarm Support** Platform Alarm Support »

**Battery Alarm Support** Platform Alarm Support »

This view opens from the main menu when you select **Controller Setup > Alarm Setup > Power Alarm Setup**.

Each possible power source is listed on a single tab with a link that toggles to display the properties for each power source.

The view title displays in the top left corner above the **Save** button. Click the >> icons to expand and display the properties under each Platform Alarm Support type heading.

Property	Value	Description
Alarm Class	text	Defines alarm routing options and priorities. Typical alarm classes include <b>High</b> , <b>Medium</b> and <b>Low</b> . An alarm class of <b>Low</b> might send an email message, while an alarm class of <b>High</b> might trigger a text message to the department manager.
Source Name	text	Reports the name of the alarm source. If you use the default script setting (%parent.displayName%), the source name property shows the display name of the alarm extension parent. You can edit this script, or type in a literal string.
Alert Text	text	Defines a description that is associated with an alert.
To Fault Text	text	Enters the text to display when the component transitions to a Fault status. When applicable, text entered for <b>Fault Algorithm</b> , <b>High Limit Text</b> and/or <b>Low Limit Text</b> may override this text.
To Offnormal Text	text	Enters the text to display when the component transitions to an Offnormal (alarm) state. When applicable, text entered for <b>Fault Algorithm</b> , <b>High Limit Text</b> and/or <b>Low Limit Text</b> may override this text.
To Normal Text	text	Configures what displays when the component transitions to a normal status. When applicable, text entered for <b>Fault Algorithm</b> , <b>High Limit Text</b> and/or <b>Low Limit Text</b> may override this text.
Hyperlink Ord	ORD	Associates an ORD, BLQ query or path with an alarm state on the component. When an alarm is reported in the console, the Hyperlink button activates. Clicking this button links to the

Property	Value	Description
		location you specify here.
Sound File	file path	Configures the path to a sound file that plays when the current component is in an alarm state. Use the folder icon to browse to the file. Click the arrow icon to the right of the folder icon to test the path.
Alarm Icon	file path	Defines the path to a graphic file to add to the display in the Timestamp column of the alarm table in the Console Recipient view.
Meta Data	link	Opens a window for managing facet keys and values.

Alarm Extensions view

This view displays a table listing of all the existing alarm extensions, including their **Station Name**, **Source Name**, **Display name**, **Alarm Class**, **Alarm State**, and **Status**. You can also edit assigned alarm classes directly in this view.

Figure 212. Alarm Source Exts view with Edit Alarm Class window




Page 1 of 4

Page Size 20

Station Name	Source Name	Display Name	Alarm Class	Alarm State	Status
entSecurity801		Activation Initiated Alert	Medium	NULL	NULL

This view displays from the main menu when you select **System Setup > Alarm Setup > Alarm Extensions**.

The **Edit Alarm Class** control button () at the top of the view opens the **Edit Alarm Class** window. Use the drop-down list in this window to change the alarm class assigned to all selected alarm source extension(s).

Columns

Column	Description
Station Name	Reports the name of the station under the control of which the event occurred.
Source Name	Reports the component that transitioned from normal to offnormal, fault, or alert. If defining search criteria, you can use wild cards here.
Display Name	Reports the name that describes the event or function.
Alarm Class	Reports the <b>Display Name</b> of the alarm class associated with the point, recipient or other component.
Alarm State	Reports the current state of the alarm: normal, acknowledged, open (unacknowledged), or cleared.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down},

Column	Description
	{fault}, {ok}, {stale}, {unackedAlarm}.

### Edit Alarm Extension properties (Alarm Source Info tab)

Each alarm source extension has a set of properties that specify the alarming conditions and certain routing options.

#### Properties

**Figure 213.** Alarm extension properties

Save

Threat Level Setup

Alarm Source Exts

Alarm Source Info

Alarm Class

Medium

Source Name

Test

x

To Fault Text

To Offnormal Text

To Normal Text

Hyperlink Ord

null

Sound File

null

Alarm Icon

null

Alarm Instructions

Edit

Meta Data

Edit

[No configured facets]

This view opens from the main menu when you select **System Setup > Alarm Setup > Alarm Extensions**, and double-click on a row in the table or select the row and click the Hyperlink button ().

The view displays all the properties associated with the selected alarm source extension. Some of the properties are editable from this view, while others are read-only.

**NOTE:** Available alarm properties may differ, depending on the type of point to which the alarm extension is attached.

Property	Value	Description
Alarm Class	text	Defines alarm routing options and priorities. Typical alarm classes include <b>High</b> , <b>Medium</b> and <b>Low</b> . An alarm class of <b>Low</b> might send an email message, while an

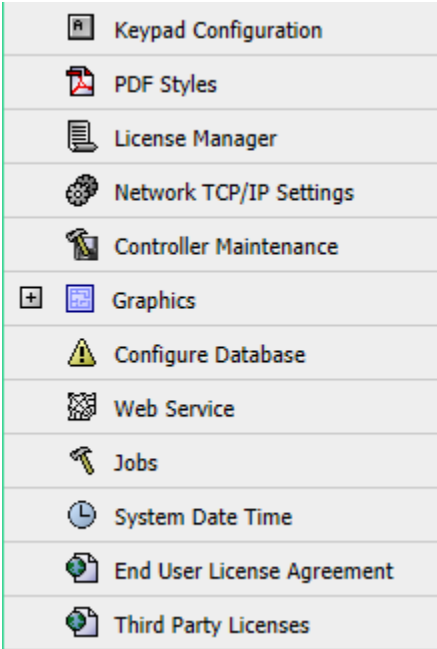
Property	Value	Description
		alarm class of <code>High</code> might trigger a text message to the department manager.
Source Name	text	Reports the name of the alarm source. If you use the default script setting ( <code>%parent.displayName%</code> ), the source name property shows the display name of the alarm extension parent. You can edit this script, or type in a literal string.
To Fault Text	text	Enters the text to display when the component transitions to a Fault status. When applicable, text entered for <code>Fault Algorithm</code> , <code>High Limit Text</code> and/or <code>Low Limit Text</code> may override this text.
To Offnormal Text	text	Enters the text to display when the component transitions to an Offnormal (alarm) state. When applicable, text entered for <code>Fault Algorithm</code> , <code>High Limit Text</code> and/or <code>Low Limit Text</code> may override this text.
To Normal Text	text	Configures what displays when the component transitions to a normal status. When applicable, text entered for <code>Fault Algorithm</code> , <code>High Limit Text</code> and/or <code>Low Limit Text</code> may override this text.
Hyperlink Ord	ORD	Associates an ORD, BLQ query or path with an alarm state on the component. When an alarm is reported in the console, the Hyperlink button activates. Clicking this button links to the location you specify here.
Sound File	file path	Configures the path to a sound file that plays when the current component is in an alarm state. Use the folder icon to browse to the file. Click the arrow icon to the right of the folder icon to test the path.

Property	Value	Description
Alarm Icon	file path	Defines the path to a graphic file to add to the display in the Timestamp column of the alarm table in the Console Recipient view.
Alarm Instructions	Edit button	Creates instructions that appear in the Alarm Record window regarding how to handle the alarm. This is a way to provide information that may be important or helpful to the person monitoring alarms.
Meta Data	link	Opens a window for managing facet keys and values.

# Chapter 11. Controller (System) Setup–Miscellaneous

Miscellaneous views are listed under the **Miscellaneous** menu. These views configure formats, PDF styles, TCP/IP settings, graphics, navigation groups, and a variety of views. In addition, they explain how to manage licenses and set the system date and time.

**Figure 214.** Miscellaneous menu

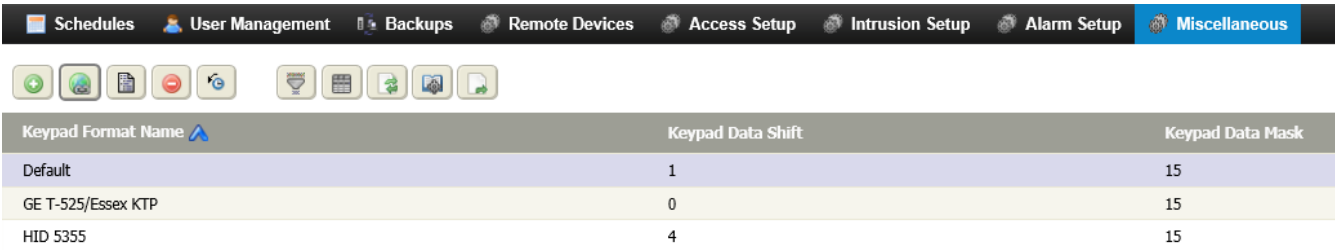


## Keypad Formats (Keypad Configuration) view

Keypads control building access at points of entry. One or more keypads may be associated with the system. The Keypad Formats view sets up each keypad.


### Buttons

**Figure 215.** Keypad Formats view

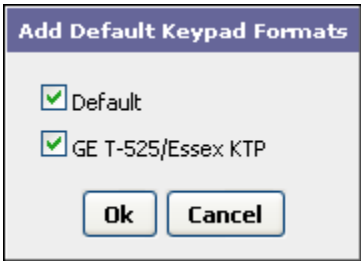


To access this view, select **Keypad Configuration** from the **Controller (System) Setup > Miscellaneous** menu.

This view consists of a tabular listing of the existing keypad formats. In addition to the standard control

buttons, the Add From Default Keypad Formats control button () opens a window for choosing one or more default keypad formats to add.

**Figure 216.** Add Default Keypad Formats window



Any default formats that are not already in the list appear in the window and are available for adding by selecting the appropriate check box. You might use this feature if you have deleted a format and want it back or if you have upgraded your system and do not already have these formats available.

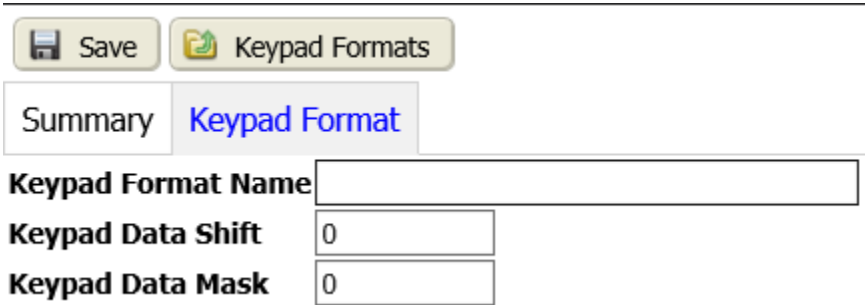
**Table 60.** Keypad Format columns


Column	Description
Keypad Format Name	Describes the keypad format. Double-click on the format record entry opens the keypad format in the Edit Keypad Format view.
Keypad Data Shift	Specifies the actual keypad format.
Keypad Data Mask	Lists the bit length of the keypad data mask.

### Add New (or edit) Keypad Format view

This view allows you to add new keypad formats. Keypad configuration is necessary to accommodate the various keypad manufacturers data transfer specifications.

**Figure 217.** Add New Keypad Format view

A screenshot of the "Add New Keypad Format view". It features a "Save" button and a "Keypad Formats" button at the top. Below these are two tabs: "Summary" and "Keypad Format", with "Keypad Format" being the active tab. The form contains three input fields: "Keypad Format Name" (a long text box), "Keypad Data Shift" (a box containing "0"), and "Keypad Data Mask" (a box containing "0").

To open this view, click **Controller (System) Setup > Miscellaneous > Keypad Configuration**, and click the Add button () or double-click the keypad format in the table (to edit an existing format).



The view title displays in the top left corner above the **Save** and **Keypad Formats** links.

**NOTE:** Refer to the keypad manufacturer for details on your keypad data shift and data mask parameters.

Property	Value	Description
Keypad Format Name	text	Provides a unique name for the format.
Keypad Data Shift	number	Specifies the actual keypad format.
Keypad Data Mask	number	Lists the bit length of the keypad data mask.

Summary tab









This tab displays a read-only list of information about a single keypad format. It opens any time you save changes made in the Edit Keypad Format view. Display properties include: Type (Keypad Format), Format Name, Data Shift, Data Mask.

Pdf Styles view

A Pdf Style is a set of properties that you can configure and save to apply (like a template) to any file that you export in the PDF format.

Buttons

Figure 218. Pdf Styles view



Display Name	Image	Title	To Display Path String
General	module://icons/x16/blank.png	bold italic 20.0pt Arial	/Services/EnterpriseSecurityService/pdfStyles/Genera

This view opens when you click the Pdf Styles menu item, under the **Controller (System) Setup > Miscellaneous** menu.

The view displays standard controls across the top and a table of all existing styles in the lower part. Below the control buttons the view lists all the existing Pdf styles that are available.

Columns



Column	Description
Display Name	Shows the style display name.
Image	Shows the location and name of the graphic used with the style.
Title	Displays the style title.
To Display Path String	Displays the path to the style definition location.

Add New (or edit) PDF Styles view

This view configures, names, and saves a new Pdf Styles template.

## Links


**Figure 219.** Add Pdf Style view

 Save
  PDF Styles

Display Name

PDF Style

Image
 





Arial ▼ 20 ▼
 

**B** ☒ ☐ U ☐

Title
 

AaBbYyZz



Foreground 
 Background 

Arial ▼ 12 ▼
 

**B** ☐ ☐ U ☐

Clock
 


AaBbYyZz

Foreground 
 Background 

Page Width  in

Page Height  in

To access this view you click **Controller (System) Setup > Miscellaneous > PDF Styles**, followed by clicking the

Add control button () at the top of the Pdf Styles view or you double-click an existing Pdf style record in the Pdf Styles view (to edit the record).

A **Save** link and a **Pdf Styles** link are located directly above the **Display Name** property at the top of the view. Type a name for your PDF style in this property and configure the properties in the PDF style tab, as desired.

## Properties

Property	Value	Description
Image	File Chooser	Use this property to browse to and assign a graphic to display across the top of the exported Pdf. The image must be located in the station database.
Title	multiple properties	Sets up the display colors and font style for the exported report title.
Clock	multiple properties	Sets up display colors and font style for the creation time of the exported report.

Property	Value	Description
Page Width	inches	Specifies the width of the PDF page.
Page Height	inches	Specifies the height of the PDF page.

License Manager view

This view manages the licenses required to use the system.

License view sections

Figure 220. License Manger view

Current License and Certificate Files

☐

[ConserveIt.license \(ConserveIt 4.6 - expires 2022-01-01\)](#)

☐

[Honeywell.license \(Honeywell 4.6 - expires 2022-01-01\)](#)

☐

[Niagara.license \(Tridium 4.6 - expires 2022-01-01\)](#)

☐

[ConserveIt.certificate \(ConserveIt - never expires\)](#)

☐

[Honeywell.certificate \(Honeywell - never expires\)](#)

☐

[Tridium.certificate \(Tridium - never expires\)](#)

Delete

Upload New license, certificate or lar File

File

Browse...

Restart station after upload

true

▼

Upload

This view opens when you select **Controller (System) Setup > Miscellaneous > License Manager** from the main menu.

Section	Description
Current License and Certificate files	Lists your current licenses and certificate files. Click on the hyperlinked file name to open and view the license file in the browser.
Upload New license, certificate or lar File	Displays a property for browsing to and uploading a new license or certificate file.

### Upload New license, certificate or lar File properties

Property	Value	Description
File	Browse... file chooser	Selects a file in the local station.
Restart station after upload	true (default) or false	Controls station restart.

### Network TCP/IP Settings view

In a Supervisor station you configure the TCP/IP properties using your PC's operating system. For a Supervisor station, this view defines station and system names. In a controller station, this is where you configure all of the controller's network properties including names.

**Figure 221.** Display Names and Network Settings (Supervisor view)

Display Names

Station Display Name

System Display Name

Update Display Names

Station Name Settings (Changes to these settings require a restart the station to take effect)

Station Name

entSecurity801

Apply Changes and Restart Station

Network Settings (Changes to these settings require a reboot to take effect)

Host Name

EntSec-J8-10

Use IPv6

No

Domain

IPv4 Gateway

172.31.64.1

DNSv4 Servers(comma separated)

IPv6 Gateway

DNSv6 Servers(comma separated)

ID

en0

Description

Onboard Ethernet Adapter en0

Physical Address

EC:11:27:A8:0F:A0

Adapter Enabled

Enabled

DHCPv4

Disabled

IPv4 Address

172.31.66.10

IPv4 Subnet Mask

255.255.252.0

IPv6 Support

Yes

IPv6 Enabled

Enabled

Obtain IPv6 Settings Automatically

Yes

IPv6 Address

fe80::ee11:27ff:fea8:fa0

IPv6 Network Prefix Length

64

ID

en1

This view opens when you log in to a controller for the first time or when you select **Network TCP/IP Settings** from the **Controller (System) Setup > Miscellaneous** menu.

Display Names section

The Display Names and Network Settings views provide two sections for configuring the station and system display names.

Figure 222. Display Names view

Display Names

Station Display Name

System Display Name

Update Display Names

The Update Display Names button saves changes to the text properties and refreshes the browser view.

**NOTE:** During a reboot of the station, the station name (display or actual name) dims until the station is restarted. Station Name and Host Name Network Settings section.

Property	Value	Description
Station Display Name	text	Defines a name that appears in the top right corner of the system interface, to the left of the <b>System Display Name</b> . The <b>Station Display Name</b> is unique for each controller. <b>NOTE:</b> This name takes priority over the Station Name and displays in the interface when both names are defined. The station n displays if no <b>Station Display Name</b> value is defined.
System Display Name	text	Defines a name that appears in the top right corner of the system interface to the right of the <b>Station Display Name</b> . This name is unique for the system and provides a hyperlink to the supervisor station from a subordinate controller.

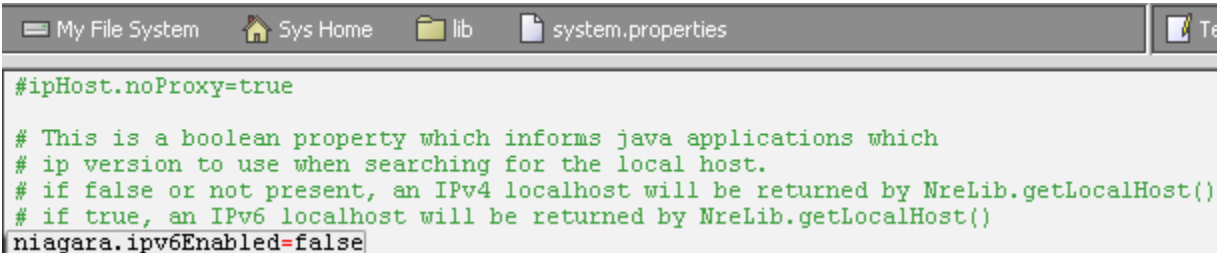
Station Name and Host Name Network Settings section

This section documents two of the properties, which configure the platform that is hosting the system. Two buttons at the bottom of the view apply or cancel changes.

**CAUTION:** Changes made in this view require you to reboot the controller. Clicking the **Apply Changes** and **Reboot** button immediately reboots the controller.

**NOTE:** To use IPv6, you must also enable it on your host by editing the `system.properties` file from Workbench. Using IPv6 may disable VPN communications when using some versions of Windows 7.

**Figure 223.** Use the system properties file to enable or disable IPv6



```
#ipHost.noProxy=true

# This is a boolean property which informs java applications which
# ip version to use when searching for the local host.
# if false or not present, an IPv4 localhost will be returned by NreLib.getLocalHost()
# if true, an IPv6 localhost will be returned by NreLib.getLocalHost()
niagara.ipv6Enabled=false
```

Property	Value	Description
Station Name	text	Creates a name for the station on the network. This name displays in the system interface if no Station Display Name is specified in the Display Names section.
Host Name	read-only	Identifies the name (Id) of the host platform. For a Supervisor PC this is localhost.
Use IPv6	Yes or No (default)	Yes configures the platform daemon to respond to IPv6 requests, that is to create IPv6 server sockets (daemon) and IPv6 Fox multicast sockets. This property applies only to certain hosts.
Domain	text	Defines a URL. If not applicable, leave it blank.
IPv4 Gateway	IP address	Defines the IP address of the Supervisor PC or remote controller.
DNSv4 Servers(comma separated)	IP address	Defines the IP addresses for any DNS servers separating each with a comma.
IPv6 Gateway	IP address	Defines the IP address for the device that forwards packets to other networks or subnets.
DNSv6 Servers(comma separated)	IP address	Defines the IP addresses for any DNS servers separating each with a comma.

Interface properties

This topic documents the Interface properties.

**Figure 224.** Interface properties

**Network Settings (changes to these settings require a reboot to take effect)**

Station Name

Host Name

Use IPv6  ▾

ID	Ethernet 2
Description	Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for Windows x64
Physical Address	00:05:9A:3C:7A:00
Adapter Enabled	<input type="button" value="Enabled"/> ▾
DHCPv4	<input type="button" value="Disabled"/> ▾
DNS Domain	<input type="text" value="honeywell.com"/>
IPv4 Address	<input type="text" value="172.19.113.53"/>
IPv4 Gateway	<input type="text" value="172.19.113.49"/>
IPv4 Subnet Mask	<input type="text" value="255.255.255.240"/>
DNSv4 Servers (comma separated)	<input type="text" value="10.192.2.45,10.216.2.51"/>
IPv6 Support	Yes
IPv6 Enabled	<input type="button" value="Enabled"/> ▾
Obtain IPv6 Settings Automatically	<input type="button" value="No"/> ▾
IPv6 Address	<input type="text" value="fe80::3a0e:26ec:d827:2249"/>
IPv6 Gateway	<input type="text" value="::"/>
IPv6 Network Prefix Length	<input type="text" value="0"/>
DNSv6 Servers (comma separated)	<input type="text"/>

Property	Value	Description
ID, Description, Physical Address	read-only	Report identifying information about the interface.
Adapter Enabled	Enabled (default) or Disabled	Brings the adapter on line and takes it offline.
DHCPv4	Enabled or Disabled (default)	Turns use of this protocol (Dynamic Host Configuration Protocol), version 4, on and off.



Property	Value	Description
DNS Domain	text	Provides domain identification, if necessary.
IPv4 Address	IP address	Defines the IP (Internet Protocol) v4 (version 4) address for the station.
IPv4 Gateway	IP address	Defines the node in the network that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet. (Wikipedia)
IPv4 Subnet Mask	number consisting of four 8-bit octets	Associated with each IP address, this number defines the range of valid IP addresses.
DNSv4 Servers (comma separated)	IP addresses	For IPv4, define the dns Host address, if necessary. Separate each entry with a comma (,).
IPv6 Support	Yes (default) or No	Indicates the network supports IPv6.
IPv6 Enabled	Enabled (default) or Disabled	Turns IPv6 support on and off.
Obtain IPv6 Settings Automatically	drop-down list, Yes or No (default)	Turns automatic downloading of IPv6 settings on and off.
IPv6 Address	IP address	Defines the IP address if using version 6.
IPv6 Gateway		Defines the gateway address for IPv6 usage.
IPv6Network Prefix Length	defaults to zero (0)	Defines the node in tan IPv6 network that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet. (Wikipedia)
DNSv6 Servers (comma separated)		For IPv6, define the dns Host address, if necessary. Separate each entry with a comma (,).

### Final properties

These properties appear at the bottom of the Network Settings view.

**Figure 225.** Final Network Settings properties



Property	Value	Description
Edit Hosts File	icon; when you click it opens a blank text file	<p>Opens the Hosts File editor. The operating system uses this plain text file to map host names to IP addresses. It is stored in the Windows folder This utility provides an easy way to edit it.</p> <p>You can type directly into this view to edit the hosts file and click the <b>Save</b> button at the bottom of the view to save changes.</p>
Apply Changes and Reboot button	button	Saves changes and reboots the controller.
Reload Without Changes button	button	Abandons changes and reloads the view.

Maintenance view (Server)

This view provides information about the Supervisor station (server). The Maintenance Info tab contains a list of read-only properties that indicate the version of individual software modules that are part of the system and several other station properties.

Links

Figure 226. Server Maintenance view



Open this view by selecting **Controller Setup > Miscellaneous > Server Maintenance**.

- **Save** updates the server maintenance record in the database.
- **Save Station** starts a job to save the current version of the station. A progress bar appears during the save process, followed by a **Success** or **Fail** window to report the results of the job.
- **Restart Station** opens the **Restart Station** confirmation window. If you confirm (click **Ok**), the station restarts immediately.

**NOTE:** During a station restart, the station name (located in the top right corner of the user interface) dims. When the station is available again, the name displays its normal color.

- **Update Reader Count** (Supervisor only) removes any readers left in the database after removing a controller

from the Supervisor network and updates the database with any added readers.

- **Get Invalid Pins** starts a job to check for any invalid (corrupted) PINs and opens a **Get Corrupt Pin Numbers** window, shown below.

### Properties

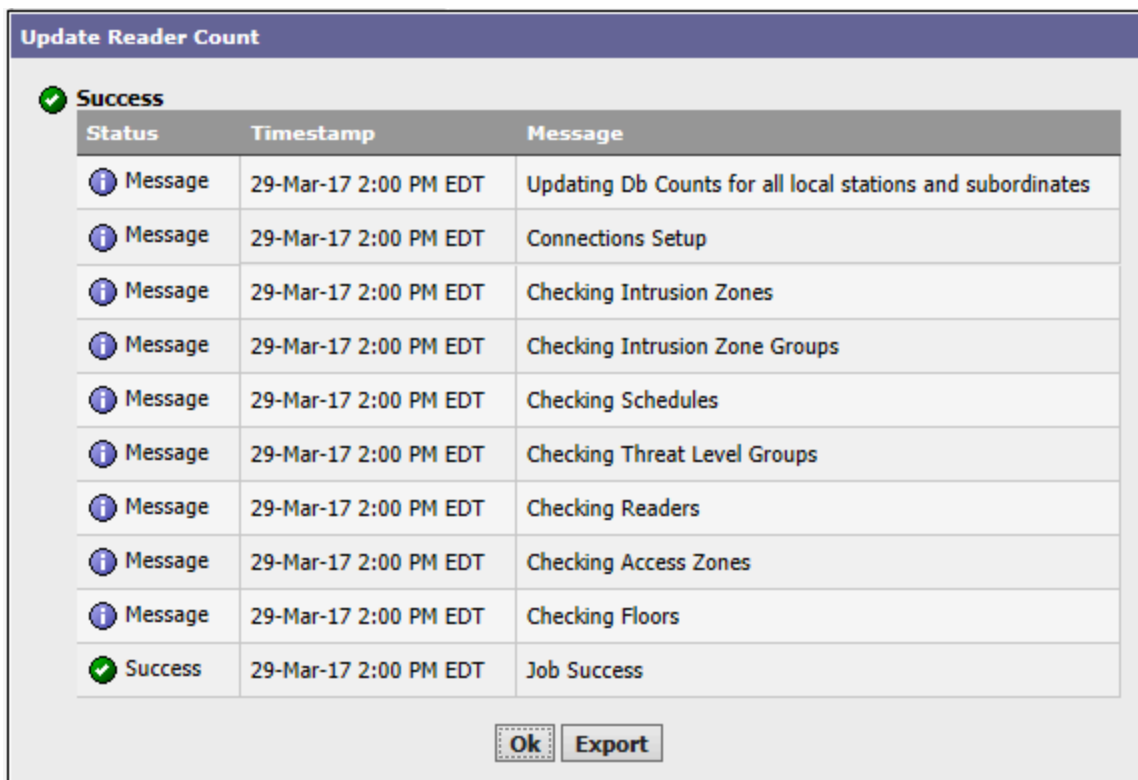
Property	Value	Description
Software Version	read-only	Displays the version of the station-level software that is running the system.
Entsec Version	read-only	Displays the version of the system.
Access Driver Version	read-only	Displays the version of the system's networking module (driver).
Last Station Restart	read-only	Displays the time, in days and hours, since the last station restart.
Last Station Save	read-only	Displays the time, in hours and minutes, since the last station save.
Intrusion Detection	read-only	Indicates if the Intrusion Detection feature is licensed for this application.
Threat Level Group Limit	read-only	Indicates the number of Threat Level Groups that currently exist.
Threat Level Count Limit	read-only	Indicates the maximum number of Threat Levels this application is licensed for.
Reader Limit	read-only	Displays the maximum number of readers that the controller or supervisor is licensed for.
Reader Count	read-only	Displays the number of readers that the controller or supervisor is currently using. A supervisor station counts all the readers in a joined system. A controller shows only its reader count. Reader count is based on the number of reader devices that are assigned to a module in the software representation. Reader count does not poll or connect to detect the presence of a physical reader. If you remove or disable reader hardware, but the device is still present in your system database, the system counts the device as being present.
Photo ID	read-only	Indicates if the system is licensed to use Photo ID.
Asure ID Device Limit	read-only number	
Asure ID Device Count	read-only number	Indicates the number of Asure IDs currently in use by the system.

Property	Value	Description
ADA	read-only	Indicates if the system is licensed for ADA.
Access Zone Limit	read-only	Indicates the maximum number of Access Zones this application is licensed for.
Access Zone Count	read-only	Indicates the number of Access Zones currently in use.
Credential Limit	read-only	<p>Displays a value indicating the number of total people and total badges that the system is licensed for. For example, if the number is 10,000 — the system is licensed for 10,000 people and 10,000 badges.</p> <p><b>NOTE:</b> If you happen to be over the license limit, the following error message displays:  <code>javax.baja.license.LicenseException: Credential License Limit Reached: &lt;limit&gt;</code> If replication or joining is trying to push information to a controller and a station is exceeding the limit of people or badges, the replication or join fails. To complete a replication or join correct the license limit.</p>
Badge Count	read-only	Indicates the total number of badges in the system.
Person Count	read-only	Indicates the number of people in the system.
Access Right Count	read-only	Indicates the number of distinct access rights that exist in the system.
Access Right Assignment Count	read-only	Indicates the total number of times access rights are assigned to one or more people. For example, if "Access Right A" is assigned to "Person1", "Person2", and "Person3", then that accounts for three Access Right Assignments. If "Access Right B" is assigned to "Person1", "Person2", and "Person4", then that accounts for an additional three Access Right Assignments. The total number of Access Right Assignments in this case is six.
FIPS Status	read-only	Indicates if the platform is setup to be compliant with FIPS standards.
Show Guided Tour	true or false	When <code>true</code> is selected and saved, this property causes the Guided Tour to

Property	Value	Description
		display at the top of the interface when a user logs on the system. When <code>false</code> is selected and saved, the Guided Tour does not display.
Coalesce Alarms	<code>true</code> or <code>false</code>	<p>When <code>true</code> is selected and saved, this property combines alarm notifications, which may improve system performance and lower network traffic. However, by combining alarm notifications, in some cases (when an alarm is initiated and quickly cleared), you may only see the "alarm cleared" notification and not the original alarm. To see all alarm notifications individually, select <code>false</code>. When <code>false</code> is selected and saved, the Coalesce Alarms does not combine the alarms, but sends individual alarm notifications.</p> <p><b>NOTE:</b> If sequences or notifications in the Supervisor station are triggered by alarms, you should not coalesce alarms. You do not coalesce alarms if you may need to document security incidents.</p>

Update Reader Count window

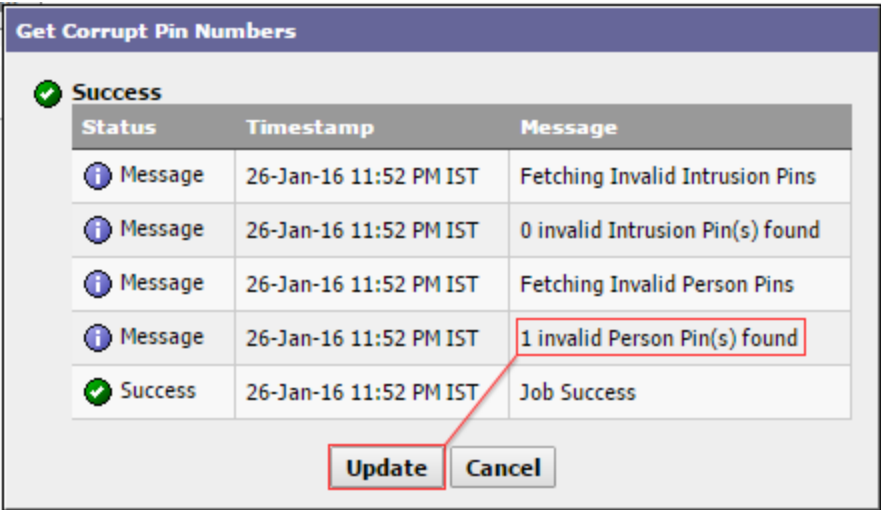
This window displays the received messages.

**Figure 227.** Update Reader Count window

### Get Corrupt Pin Numbers window

This window displays a list of corrupt PIN numbers.

Figure 228. Get Corrupt Pin Numbers window

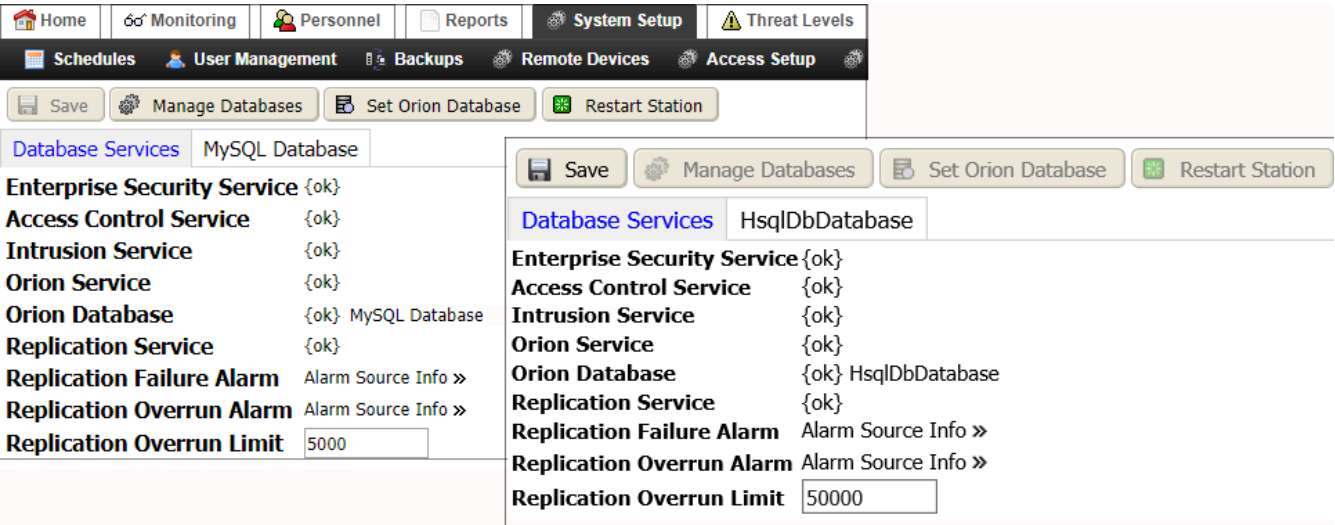


This window shows job status with time stamped messages that indicate if any invalid PINs are found. If one or more invalid PINs are found, then the window displays an **Update** button that you can click to launch a job that updates any PINs that are identified as invalid.

## Configure Database view, Database Services tab

This view displays the station's database and network configuration settings.

Figure 229. Configure Database view, Database Services tab in a remote station



You access this view by clicking **Controller (System) Setup > Miscellaneous > Configure Database**.

### Tabs

The Database Services tab shows the status of the currently-assigned Orion database. It contains read-only and



other properties that describe the status of Database Services or configure alarming properties related to the Database Services.

An additional tab identifies the associated database. Although a Supervisor station may have more than one database, each station can have only one Orion Database at a time. The HsqldbDatabase supports only remote controller stations. The database in a Supervisor station is usually a MySQL or MS SQL database.

#### NOTE:

The tabs appear in both Supervisor and remote (subordinate) stations but only the properties for the Supervisor database may be edited. HsqldbDatabase properties cannot be edited.

#### Links

In addition to a **Save**, these links are available along the top of the view:

- **Manage Databases** opens the Manage Databases window. You use this window to add, delete, rename or duplicate databases for use in your system. For each database that you add, an additional tab, representing that database configuration, displays on the view.
- **Set Orion Database** opens the Set Orion Database window. Use this window to designate which of the configured databases (if you have more than one configured) to use for the Orion Service. A reset of the Orion Database requires a station restart.  
**CAUTION:** Using the Set Orion Database window can result in unintentional loss of data. Be sure that you have backed up any data that you want to preserve before changing the Orion database.
- **Restart Station** starts the current stations. This is necessary after configuring or reassigning a station database.

Property	Value	Description
Enterprise Security Service	read-only	Indicates if the service is running. It should report {Ok}.
Access Control Service	read-only	Indicates if the service is running. It should report {Ok}.
Intrusion Service	read-only	Indicates if the service is running. It should report {Ok}.
Orion Service	read-only	Indicates if the service is running. It should report {Ok}.
Orion Database	read-only	Indicates that the connection from Orion to the selected rdbms database is {Ok}, and which database Orion is connected to.
Replication Service	read-only	Indicates if the service is running. It should report {Ok}.
Replication Failure Alarm (Alarm Source Info)	read-only	Links to a set of properties for configuring and routing alarms. These properties are documented in the <a href="#">Alarm Setup</a> topic of the PDF and in the help system (search for Alarm Source Info).

Property	Value	Description
Replication Overrun Alarm (This alarm occurs when the deletion table record count is greater than the <code>Replication Overrun Limit</code> property value.)	read-only	Indicates that there are too many non-replicating subordinates assigned to the Supervisor database. To get rid of this alarm, make all subordinates available for replication or delete them from the Station Manager - Database view. This stops the replication process from keeping track of the station's deleted records. You can always re-discover, add, and join the subordinate station at a later date.
Replication Overrun Limit	number; The default value is 5000.	Specifies the maximum number of records that are allowed in a deletion table. You will receive a replication overrun alarm when the deletion record count is greater than this number.

## Database Configuration tab (HsqlDbDatabase)

An HSQL database is a relational database management system written in Java. It has a JDBC driver and supports a large subset of SQL-92 and SQL:2008 standards. (Wikipedia). This tab is available in a controller station.

**Figure 230.** HsqlDbDatabase properties

The screenshot shows the 'Controller Setup' menu with 'Configure Database' selected. Below the menu, there are 'Save' and 'Restart Station' buttons. The 'Database Services' tab is active, showing the 'HsqlDbDatabase' configuration. The properties are listed as follows:

<b>Status</b>	{ok}
<b>Enabled</b>	true
<b>Fault Cause</b>	
<b>Health</b>	Ok [12-Mar-25 11:57 AM UTC]
<b>Alarm Source Info</b>	Alarm Source Info »
<b>User Name</b>	
<b>Base Directory</b>	file:^hsqldb
<b>Database Name</b>	orion
<b>Defrag On Save</b>	<input checked="" type="checkbox"/> true
<b>Defrag And Save Periodic Schedule</b>	30 days {Sun}

You access this view from the main menu by clicking **Controller Setup > Miscellaneous > Configure Database**, followed by clicking the HsqlDbDatabase tab.

In addition to the standard properties (Status, Enabled, Fault Cause, Health, and Alarm Source Info), these properties support an HSQL database.

Property	Value	Description
Privileged Username	text	<b>NOTE:</b> Starting in Niagara 4.14, the HsqlDbDatabase component properties <b>Use Encrypted Connection</b> , <b>User Name</b> , and <b>Password</b> are replaced with a single <b>Privileged Username</b> property. The HSQL database is automatically generated and not editable or visible. When using HSQL, if the station keyring is corrupted, you need to load a backup station, as this instance of the HSQL database is no longer operational.
Base Directory	read-only	Defines the path that points to the location of the database. A typical configuration uses a folder file space directly under the station. For example, if the folder is named <b>hsqldb</b> , the path would be: <b>file:^hsqldb</b> .
Database Name	read-only	Defines the name of the database to connect to. If the database does not already exist, the system creates it when you save the property sheet with a completed <b>Base Directory</b> and <b>Database Name</b> .
Defrag on Save	true or false (default)	Configures the system to remove blank records in the database when you save it. Removing blank records can take time. Based on your use of the system, you should establish a regular time to defragment the database. Other backups can be performed without defragmentation to save time.

### Database configuration tabs (MySQL and SqlServer databases)

MySQL is an open-source relational database management system (RDBMS) supported by Oracle Corporation. SqlServer is a relational database management system developed by Microsoft. The properties required to configure these databases are similar to one another.

Properties

**Figure 231.** MySQL database properties

Home

Monitoring

Personnel

Reports

System Setup

Photo I

Schedules

User Management

Backups

Remote Devices

Access Set

Save

Manage Databases

Set Orion Database

Restart Station

Database Services

MySQLDatabase

Status

Enabled

Fault Cause

Health

Alarm Source Info

Host Address

User Name

Password

Database Name

Port

Extra Connection Properties

Max Active Connections

Peak Active Connections

Active Connections

{down,alarm,unackedAl.

true

Fail [09-Oct-18 8:13 PM EDT]

Alarm Source Info >>

ip:localhost

admin

••••••••

entsec

3306

30

0

0

You access this tab from the main menu in a Supervisor station by clicking **System Setup > Miscellaneous > Configure Database**, followed by clicking the **MySQLDatabase** tab.

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support the MySQL database.

Property	Value	Description
Host Address	IP address	Defines the IP address of the computer platform where the database resides.
User Name	text	Defines the user name credential with which to log in to the database.  For MySQL databases, this should be a name other than the default, "root," which only connects to a database hosted

Property	Value	Description
		on localhost.
Password	two properties	The <code>Password</code> property defines a password that is used to log in to the database. The <code>confirm</code> property must be an exact match to the <code>Password</code> property.
Database Name	text	Defines the name of the database to connect to. If the database does not already exist, the system creates it when you save the property sheet with a completed <code>Base Directory</code> and <code>Database Name</code> .
Port	number	<p>Specifies the port to use when connecting to the database.</p> <p>Common default values are:</p> <p>HsqldbDatabase - no port is specified because this rdb is for local database use only.</p> <p>MySQLDatabase - Port 3306</p> <p>SqlServerDatabase - Port 1433</p>
Extra Connection Properties	semicolon list of property,value pairs in the form "property=value;..."	Properties, such as <code>charset</code> , define values to use when connecting to the database.
Max Active Connections	number	Defines the maximum number of active connections that can be allocated from this pool at the same time. Changing this property requires a station restart.
Peak Active Connections	number	Defines the peak number of active connections in the pool.
Active Connections	number	Defines the number of current active connections in the pool.

## Web Service view

This view displays a set of properties to configure web service settings.

Properties

Figure 232. Web Service view

HomeMonitoringPersonnelReportsSystem SetupThreat Levels

SchedulesUser ManagementBackupsRemote DevicesAccess Setup

Save

Web Service

Status

{ok}

Fault Cause

Public Server Port

80

[1 - 65535]

Http Enabled

true

Public Server Port

443

[1 - 65535]

Https Enabled

true

Https Only

false

Https Cert

tridium

X Frame Options

Sameorigin

Show Stack Trace

false

Web Launcher Module Caching Type

Host

Web Launcher Enabled

true

Min Threads

4

[4 - 30]

Max Threads

30

[6 - +inf]

Thread Idle Timeout

00000

h

05

m

00

s

[1 second - +inf]

<

>

You select this view by choosing **Controller (System) Setup > Miscellaneous > Web Service** from the main menu.

In addition to the standard properties (**Status** and **Fault Cause**), these properties support the Web Service.

Property	Value	Description
Public Server Port	number (defaults to 80)	Specifies the HTTP client's TCP port. The service listens on on this port for connections.
Http Enabled (general)	true or false	Turns the processing of HTTP requests on (true) and off (false).
Public Server Port	number (defaults to 443)	Specifies the HTTP client's TCP port. The service listens on on

Property	Value	Description
		this port for connections.
Https Enabled (general)	true (default) or false	Turns the processing of HTTPS requests on (true) and off (false).
Https Only (general)	true or false (default)	<p>Configures the security of the connection.</p> <p>true redirects any attempt to connect using a connection that is not secure (Http alone) to a secure Https connection.</p> <p>false permits an Http connection.</p>
Https Cert (general)	drop-down list of server certificates; defaults to tridium	Specifies the alias of the host platform's server certificate, which the client uses to validate server authenticity. The default identifies a self-signed certificate that is automatically created when you initially log on to the server. It cannot be deleted and should be used for recovery purposes. The default certificate is protected by the global certificate password. If other certificates are in the host platform's key store, you can select them from the drop-down list.
X Frame Options	drop-down list	<p>Prevents Cross-Frame Scripting (XFS) attacks. You choose whether or not a browser should be allowed to render a page in a &lt;frame&gt; or &lt;iframe&gt;, thus possibly allowing your content to be embedded into other sites.</p> <p>Deny prevents any attempt to load the page in a frame. This option may negatively impact the display of information.</p> <p>Sameorigin (default) loads the page in a frame as long as the site including it in a frame is the same as the one serving the page (same server).</p> <p>If a page specifies Sameorigin, browsers will prevent framing</p>

Property	Value	Description
		<p>only if the top-level origin FQDN (fully-qualified-domain-name) does not exactly match FQDN of the subframe page that demanded the <code>Sameorigin</code> restriction. This is considered a safe practice.</p> <p><code>Any</code> allows XFS and Cross-Site Scripting (XSS). This is the least safe choice.</p>
Show Stack Trace (general)	<code>true</code> or <code>false</code>	<p>Controls if exception stack traces, when available, appear in error responses.</p> <p><code>true</code> shows exception stack traces in error responses when they are available.</p> <p><code>false</code> disables exception stack traces in error responses.</p>
Web Launcher Module Caching Type (general)	drop-down list; defaults to <code>Host</code>	<p>Determines how a client using the Web Launcher caches modules.</p> <p><code>Host</code> results in a folder and the downloading of installation modules to the <code>module</code> folder (<code>n4applet</code> for N4, and <code>wbapplet</code> for AX). This results in the creation of multiple folders of downloaded modules, which negatively affects platform memory usage.</p> <p><code>User</code> results in the creation of a <code>.sharedModuleCache</code> folder (one cache per host visited; one shared cache per user). The system then downloads to a sub-folder at this location (<code>n4applet</code> for N4, and <code>wbapplet</code> for AX). This option minimizes the memory required when running in a controller.</p>
Web Launcher Enabled	<code>true</code> (default) or <code>false</code>	Enables ( <code>true</code> ) and disables ( <code>false</code> ) the use of the Web Launcher.
Min Threads	number (defaults to 4)	Ensures that at least four threads

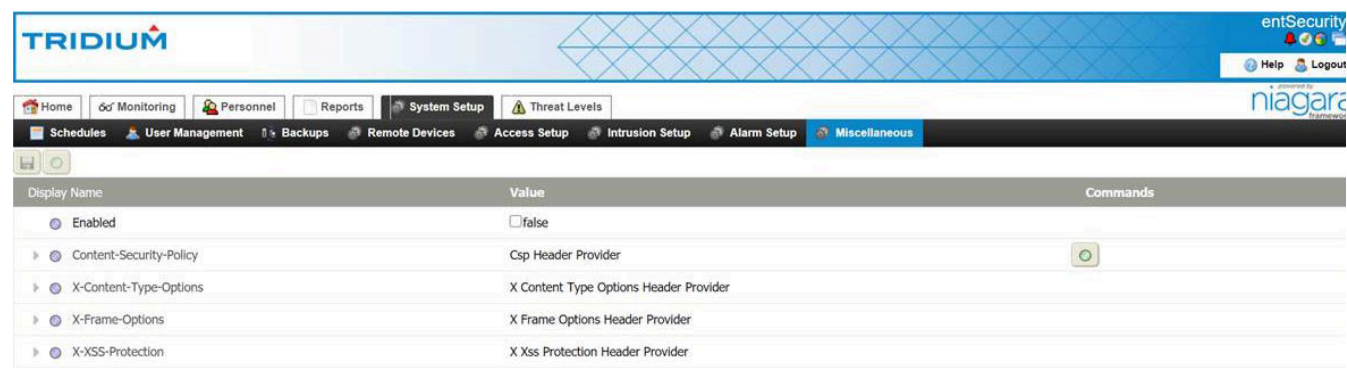


Property	Value	Description
		process at a time.
Max Threads	number	<p>Tunes large networks (those with many station components) to process more than a single thread at a time. It is the only visible part of a shared thread-pool scheme for scaling large-jobs and allows the local station's thread pool to grow uncapped.</p> <p>Each thread uses one JDBC Connection to communicate with the database, so there are as many connections created as there are threads.</p> <p>Normally you increase this value to between 20 and 50 to improve performance when handling large volumes of data.</p>
Thread Idle Timeout	hours minutes seconds (defaults to five hours)	Configures the amount of idle time to elapse before a thread times out.

HTTP Header Providers view

These headers pass additional information with an HTTP request or response between the client and server. This information ensures the authenticity of the messages providing security against click-jacking and other threats. This component contains four headers that you may customize as needed. To ensure the most robust security, leave all headers enabled. To turn off a header, if necessary, set its **Enabled** property to `false`.

Figure 233. Http Header Providers view



To access these properties navigate to **System SetupMiscellaneous > Http Header Providers**.



















Property	Value	Description
Enabled	check box (defaults to <code>false</code> )	<p>Turns on (<code>true</code>) and off (<code>false</code>) the use of Http Header Providers.</p> <p>Disable the check box (<code>false</code>) if your cameras do not support secure communication or your cameras are not loading on the browser.</p>
Content-Security-Policy	additional properties	<p>Notifies the browser what restrictions should be put on images, JavaScript, or CSS, in response to a request for resources.</p> <p>Refer to <a href="#">Content-Security-Policy</a>.</p>
X-Content-Type-Options	drop-down list (defaults to <code>nosniff</code> )	<p>Indicates to browsers that they should apply additional restrictions to auto-detect content types in downloaded files.</p> <p>For best security, <code>nosniff</code> is the recommended value.</p>
X Frame Options	drop-down list (defaults to <code>Sameorigin</code> )	<p>Indicates if a browser should be allowed to render pages served by your station in a <code>&lt;frame&gt;</code> or <code>&lt;iframe&gt;</code> of another site. Use it to avoid click-jacking attacks.</p> <p><code>Sameorigin</code> allows the browser to embed other pages from within the same station. This is considered a safe practice and is necessary for the correct functioning of the HTML5 Hx Profile.</p> <p><code>Deny</code> prevents the browser from loading the page in a frame.</p> <p><b>NOTE:</b> <code>Deny</code> inhibits the display of some typical HTML5 Hx Profile views.</p> <p><code>Any</code> may cause a Cross-Frame Scripting (XFS) or click-jacking vulnerability and is not recommended. If an external site needs to embed your station's web interface, configure a</p>

Property	Value	Description
		"frame-ancestors" directive under Content-Security-Policy.
X-XSS-Protection	text (defaults to 1; mode=block)	Ensures that, if an XSS attack is detected, the browser prevents the page from loading. 1; mode=block is the recommended value.

### Content-Security-Policy

The default values for this header have been customized for typical usage with HTML5 Hx Profiles. Additional sources may be added to these directives, but removing any of the default sources may cause your views to stop working.

**Figure 234.** Content-Security-Policy properties

Property Sheet	
 <b>Content-Security-Policy (Csp Header Provider)</b>	
 Enabled	<input checked="" type="radio"/> true 
 Status	<input data-bbox="649 451 998 493" type="text" value="{ok}"/>
 Violation Text	<input data-bbox="649 514 1331 556" type="text"/>
 child-src	<input data-bbox="649 577 1331 619" type="text"/>
 connect-src	<input data-bbox="649 640 1331 682" type="text" value="'self' workbench ws://%hostname%:%port%"/>
 default-src	<input data-bbox="649 703 1331 745" type="text" value="'self' workbench"/>
 frame-src	<input data-bbox="649 766 1331 808" type="text"/>
 font-src	<input data-bbox="649 829 1331 871" type="text"/>
 img-src	<input data-bbox="649 892 1331 934" type="text" value="'self' workbench data:"/>
 manifest-src	<input data-bbox="649 955 1331 997" type="text"/>
 media-src	<input data-bbox="649 1018 1331 1060" type="text"/>
 object-src	<input data-bbox="649 1081 1331 1123" type="text"/>
 report-uri	<input data-bbox="649 1144 1331 1186" type="text" value="/csp-reports"/>
 script-src	<input data-bbox="649 1207 1331 1249" type="text" value="'self' workbench 'unsafe-inline' 'unsafe-"/>
 style-src	<input data-bbox="649 1270 1331 1312" type="text" value="'self' workbench 'unsafe-inline'"/>
 Additional Directives	<div data-bbox="649 1333 1331 1438"></div>
<div data-bbox="1063 1449 1274 1501">Refresh</div> <div data-bbox="1339 1449 1469 1501">Save</div>	

The screen capture shows a Workbench Property Sheet. To view this Property Sheet, connect to the station using Workbench, expand **Station > Config > Services > WebService > Http Header Providers > Content-Security-Policy**.

To view the same properties in the web UI, navigate to **System SetupMiscellaneous > Http Header Providers** and expand **Content-Security-Policy**.

**NOTE:** The host `workbench` in the properties above allows HTML views, such as Web Chart to correctly function in Workbench and should not be removed under normal circumstances.

In addition to the standard properties (Enabled and Status), these properties are unique to this component.

Property	Value	Description
Violation Text	text	<p>Creates the text to display when a browser reports a Content-Security-Policy violation to a station, which logs it in the web.reporting.csp log.</p> <p>The station logs the first violation with SEVERE priority, and subsequent violations as FINE.</p> <p><b>NOTE:</b> A Content-Security-Policy violation should not typically occur during normal usage of the system. If you receive one, consider whether your Content-Security-Policy configuration should be changed to match browser behavior or if the violation represents an attempted XSS attack.</p>
child-src	text	Defines the valid sources for web workers and nested browsing contexts loaded using elements, such as <frame> or <iframe>.
connect-src	text (defaults to 'self' workbench ws://%hostname%:%port% wss://%hostname%:%port%)	<p>Restricts the URLs that can be loaded using script interfaces.</p> <p>You can set up a template so that all Content-Security-Policy directives reference the %scheme%, %hostname%, and %port% from the originating HTTP request.</p> <p><b>NOTE:</b> When viewing HTML views in Workbench, this request is made to Workbench. Content-Security-Policy headers include this by default. Removing it may cause HTML views to stop working in Workbench.</p>
default-src	text (defaults to 'self' workbench )	Serves as a fallback for the other fetch directives.
frame-src	text	Specifies valid sources for nested browsing contexts loading using elements such as <frame> or <iframe>.
font-src	text	Specifies valid sources for fonts loaded using @font face.
img-src	text (defaults to 'self' workbench data: )	Specifies valid sources of images and favicons.

Property	Value	Description
manifest-src	text	Specifies valid sources of application manifest files.
media-src	text	Specifies valid sources for loading media using the <audio>, <video> and <track> elements.
object-src	text	Specifies valid sources for the <object>, <embed>, and <applet> elements.
report-uri	text (defaults to /csp-reports )	Instructs the user agent to report attempts to violate the Content Security Policy. These violation reports consist of JSON documents sent via an HTTP POST request to the specified URI.
script-src	text (defaults to 'self' workbench 'unsafe-inline' 'unsafe-eval' )	<p>Specifies valid sources for JavaScript.</p> <p>To perform various functions with Asure ID, such as template discovery, template data discovery and badge printing, you must add the Asure ID port number in this property. The syntax for the port number is:</p> <p>http://localhost:&lt;number&gt;  where &lt;number&gt; is the Asure ID port number. For example: 'self' workbench 'unsafe-inline' http://localhost:3001</p>
style-src	text (defaults to 'self' workbench 'unsafe-inline' )	Specifies valid sources for stylesheets.
Additional Directives	text	Provides a location to enter any Content-Security-Policy directives not covered by the other properties on this component.

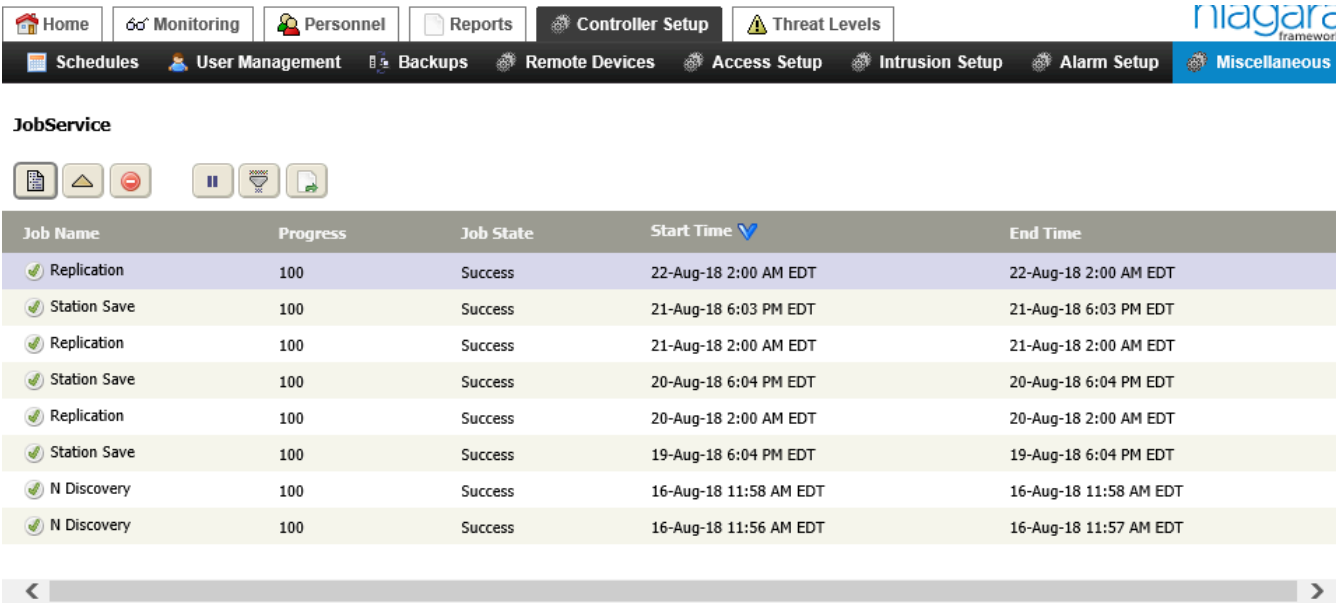
**NOTE:** The Security Dashboard provides information about the HTTP Header configuration and whether there is any performance degradation. It provides notification for any non-secure headers and explains why the settings are not secure. To secure the header's settings, set the values as described in the [Web Service view](#).

## Job Service view

This view shows a table listing of all the jobs that have run on the local station.



Buttons

Figure 235. view



This view opens when you select **Controller Setup (System) Setup > Miscellaneous > Jobs** from the main menu. The view shows a table listing of all the jobs that have run on the local station.

You can use the standard control buttons across the top of this view to filter, delete, auto-refresh or export a report of this table. In addition to the standard control buttons, the following controls are also available in this view.

-  Summary button opens the Success window or Error window, which provides summary and detailed results views of the selected job.
-  Job Log button opens the Job Log window, which provides a log of the job actions for the selected job.

Columns

Column	Description
Job Name	The name of the job.
Progress	A percentage that provides general information about how long the job has taken and is likely to take.
Job State	Reports success or failure.
Start Time	Reports when the job started.
End time	Reports when the job finished.

System Date Time Editor view

This view displays a set of properties for setting the associated controller’s date and time.

**Figure 236.** System Data Time Editor view

The screenshot shows the 'System Data Time Editor' interface. It contains two main sections: 'System Time' and 'Time Zone'. The 'System Time' section has six dropdown menus for day, month, year, hour, minute, and AM/PM, followed by the text 'EDT'. The 'Time Zone' section has a single dropdown menu showing 'America/New\_York (-5/-4)'. At the bottom right, there are two buttons labeled 'Refresh' and 'Save'.

This view opens from the main menu when you click **Controller (System) Setup > Miscellaneous > System Date Time**

The properties are dimmed until you check the **Change System Time** check box. Changes to these properties must be saved before leaving the view or they are not effective.

**NOTE:** A station restart is required when you choose a new option even if the time zone differential does not change. For example, changing from America/New York to America/Toronto requires a restart, even though the current time differential may be the same for both options.

## End User Licenses Agreement view

This view displays a single page listing End User License Agreement for this application. Select this view by clicking on the following menu items from the main menu: **Controller (System) Setup > Miscellaneous > End User License Agreement**.

## Third Party Licenses view

This view displays a single page listing of all the third party software licenses that are associated with this application. Select this view by clicking on the following menu items from the main menu: **Controller (System) Setup > Miscellaneous > Third Party Licenses**.

## Controller TimeServers Settings

This view configures NTP (Network Time Protocol) properties in a controller platform.



Settings properties

Figure 237. NTP view in a controller station

HomeMonitoringPersonnelReportsController SetupThreat Levels

SchedulesUser ManagementBackupsRemote DevicesAccess SetupInt

Settings

Enabledfalse

Sync Local Clock to NTPtrue

Sync Time At Bootfalse

Use Local Clock as Backupfalse

Generate NTP Statisticsfalse

Time Servers

☐

Address

Peer Mode

Server

Burst

false

Preferred

false

Min. Poll Interval

6log2 s

Max. Poll Interval

10log2 s

Refresh

Save

To access this view, click **Controller Setup > Miscellaneous > TimeServers Settings**

Property	Value	Description
Enabled	true (default) or false	If true, the host will use NTP to sync its clock with time values retrieved from other servers.
Sync Local Clock to NTP	true (default) or false	If true, this enables the host to adjust its local clock by means of NTP. If disabled (false), the local clock free-runs at its intrinsic time and frequency offset. This flag is useful in case the local clock is controlled by some other device or protocol and NTP is used only to provide synchronization (as server) to other clients. In this case, the local clock driver can be used to provide this function and also certain time variables for error estimates and leap-indicators.
Sync Time At Boot	true or false (default)	Default is false. If true, when the

Property	Value	Description
		controller boots, before the stations starts or the ntpd starts, it executes the ntpdate command. This updates the system local time.
Use Local Clock as Backup	true or false (default)	<p>If <code>true</code>, should the specified NTP server(s) become unavailable at the time of a poll, the time used is provided by the system clock. This prevents the timing of the polling algorithm in the ntpd (which is executed at specified/ changing intervals) from being reset.</p> <p>A <code>true</code> value does not result in any change to the NTP daemon's polling interval (frequency). In fact, by using the local system clock the NTP-calculated polling time would remain the same, and thus not result in more polling.</p>
Generate NTP Statistics	true or false (default)	<p>If <code>true</code>, the NtpPlatformService reports whatever information it can about its operation. To access these statistics with the station opened in Workbench, right-click the NtpPlatformServiceQnx and select <b>ViewsSpyRemote</b>. Keep in mind that the ntpd is a QNX process; thus Niagara has no control over what it reports.</p>

### Time Servers properties

These properties become available when you click the Add button.

Property	Value	Description
Address	server domain name	Fully qualified domain name, IP address, or host files alias for the NTP time server.
Peer Mode	drop-down list	<p>Defines the type of server:</p> <p><code>Server</code> indicates that the controller platform is in a subordinate role to the server with regard to time synchronization.</p> <p><code>Peer</code> indicates that the platform functions as an equal with the</p>

Property	Value	Description
		server with regard to time synchronization.
Burst	Drop-down list, true or false (default)	false by default. If true, when server is reachable, upon each poll a burst of eight packets are sent, instead of the usual one packet. Spacing between the first and second packets is about 16 seconds to allow a modem call to complete, while spacing between remaining packets is about 2 seconds.
Preferred	Drop-down list, true or false (default)	If true, designates a server as preferred over others for synchronization. Note also that priority order (top highest, bottom lowest) is also evaluated if multiple servers are entered.
Min. Poll Interval	seconds (defaults to 6)	Minimum poll interval for NTP messages, from 4 to 16. Note that units are in "log-base-two seconds," or 2 to the power of n seconds (NTP convention), meaning from 2 to the 4th (16 seconds) to 2 to the 16th (65,536 seconds).
Max. Poll Interval	seconds (defaults to 10)	Maximum poll interval for NTP messages, from 10 to 17. Note that units are in "log-base-two seconds," or 2 to the power of n seconds (NTP convention), meaning from 2 to the 10th (1,024 seconds) to 2 to the 17th (131,072 seconds).



## Chapter 12. Controller (System)–Miscellaneous Graphics

Graphics views are custom displays you create using the Graphic Editor view. Graphic views contain controls, links, and indicators related to building access and automation system controls. Graphic views support two **Target Media**: `HxPxMedia` (for viewing in a browser) or `WorkbenchPxMedia` (for viewing in Workbench).

**Figure 238.** Graphics menu



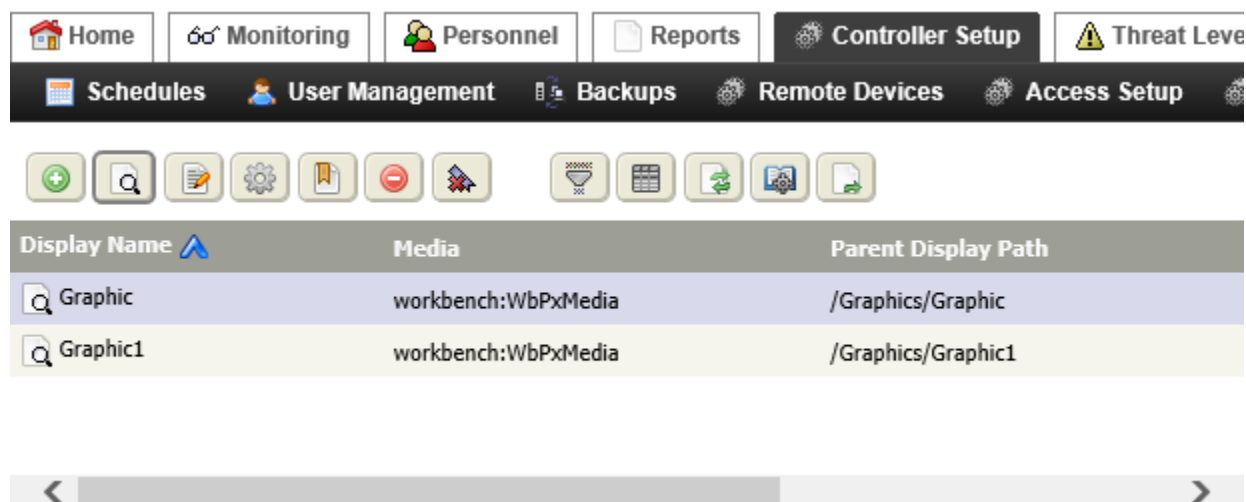
You access this menu by clicking the **Controller (System) Setup > Miscellaneous > Graphics** menu item.

In Niagara 4.9, three of the widgets run in a browser using HTML5: `LiveVideoPlayer`, `Control Panel` and `CameraWidget`. The remaining widgets: `PanTiltJoystick`, `ZoomSlider`, `MouseDownButton` and `VideoMultistreamPane` require Web Launcher and run outside of the browser. `WorkbenchPxMedia` run without additional requirements in Workbench. Running in the web UI they require the Java Web Launcher applet, which displays them outside of the browser.

### Graphics view (Graphics Management)







This view lists all the existing graphic views, including their Display Name, Media, and Parent Display Path. This view is also where you add new and edit existing graphic views.

## Buttons

**Figure 239.** Graphics view

This view opens when you select **Controller (System) Setup > Miscellaneous > Graphics > Graphics Management** from the main menu.

In addition to the standard buttons (Delete, Filter, Column Chooser, Refresh, Manage Reports and Export), this view provides these control buttons:

-  Add opens a view or window for creating a new record in the database.
-  View Graphic displays the selected graphic in the browser using the designated media type.
-  Graphic Editor opens the selected graphic in the Graphic Editor view for editing.
-  Modify Settings opens the **Modify Settings** window with which to edit existing graphic view properties. You can change the view name, associated icon, or **Target Media** type using this window.
-  Edit Nav opens the Edit Nav window with which to configure where the graphic appears in the system's menu structure.
-  Remove Nav deletes the custom nav file associated with the selected graphic view. The system prompts you to confirm the deletion. When you confirm, the view no longer appears in the system's menu structure.

Columns

Column	Description
Display Name	Reports the name assigned to the graphic when it was created.
Media	Reports the type of graphic. The graphic type determines where it can be viewed, in Workbench, browser or Web Launcher.
Parent Display Path	Reports the URL where the graphic record is located in the database.

Add a graphic window

This window provides the properties to add a new graphic.

Figure 240. Add a new graphic window

The 'Add' window is a dialog box with a title bar. It contains three labeled text fields: 'View Name' with the value 'Graphic', 'View Icon' with the value 'module://icons/x16/views/view.png', and 'Target Media' with a dropdown menu currently showing 'HxPxMedia'. A mouse cursor is hovering over the dropdown menu, which is open to show two options: 'WorkbenchPxMedia' and 'HxPxMedia'. At the bottom of the window are two buttons: 'Ok' and 'Cancel'.

Property	Value	Description
View Name	text	Identifies the name of the graphic.
View Icon	file path	Defines the location of an icon to represent the graphic.
Target Media	drop-down list	Identifies where the graphic will be used: Workbench or the web (HxPxMedia).

Modify Settings window

This window configures graphics properties.

Figure 241. Modify Settings window properties

The 'Modify Settings' window is a dialog box with a title bar. It contains three labeled text fields: 'View Name' with the value 'Graphic', 'View Icon' with the value 'module://icons/x16/views/view.png', and 'Target Media' with a dropdown menu currently showing 'WorkbenchPxMedia'. At the bottom of the window are two buttons: 'Ok' and 'Cancel'.

You access these properties by selecting a row in the Graphics view table followed by clicking the Modify

Settings button ().

The graphics properties you can edit are documented in the “Add a graphic window” topic.

Edit Nav window

This window configures where the graphic appears in the Nav tree.

Figure 242. Edit Nav window properties

Edit Nav

Nav Name

3rdFloor

Display Name

3rd Floor

Parent Path

Graphics

Index

2

Is Default Child

false

Ok

Cancel

You access these properties by selecting a row in the Graphics view table followed by clicking the Edit Nav

button ().

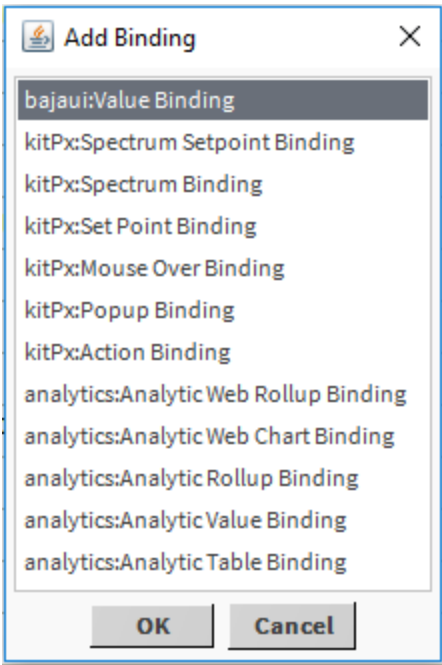
Property	Value	Description
Nav Name	text	Specifies a name for the navigation tree.
Display Name	text	Specifies the name of the graphic file as it appears in the navigation tree.
Parent Path	drop-down list	Specifies where, in the existing system navigation hierarchy, to place a new menu item.
Index	number	Specifies where, in the parent this menu item is located. The first position (from left to right, or top to bottom) is 0, then 1, 2, and so on.
Is Default Child	true or false	Sets the current graphic as the default view more than one graphic is assigned to the parent view.

Types of bindings

Some bindings work with only a certain type of widget (for example, a bound label binding) and other bindings may be used with several types of widgets including some that are not available in the system.



Figure 243. Types of bindings

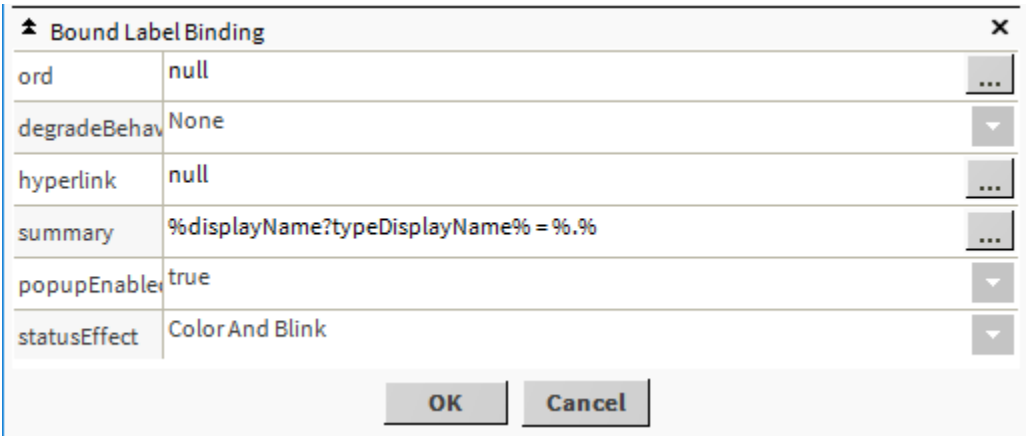


To access this menu in the Graphic Editor, open the Widget Tree side bar, double-click the object in the Widget Tree or on the canvas.

About bound label bindings

Bound label bindings exclusively connect a value to a bound label widget. Bound labels, which you can add from the Graphics Editor popup menu, have properties that are available from the properties side bar.

Figure 244. Bound label binding properties

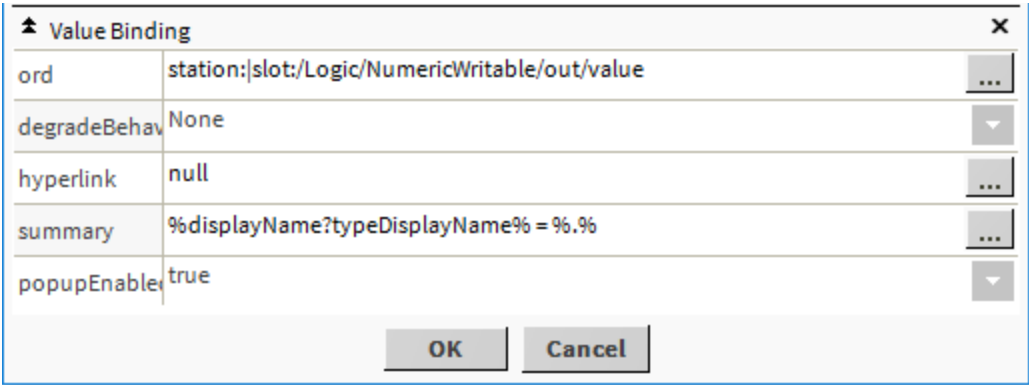


To access these properties after dragging a **BoundLabel** from the kitPx palette to the Px Editor, double-click the bound label. These properties are toward the bottom of the list.

Property	Value	Description
Ord	Defaults to <code>null</code>	<p>Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.</p> <p>In a Popup binding this path that designates the component view to display in the popup window.</p>
Degrade Behavior	Defaults to <code>None</code>	Specifies what the user sees when binding communications are not available. If a binding cannot be used, this property determines how the UI degrades gracefully. For example, if a user does not have permission to invoke a specific action, a button bound to the action can be grayed out or hidden entirely.
Hyperlink	Defaults to <code>null</code>	Links to another object. When used, the link is active in the browser or in the graphic view.
Summary	Bql Query statement; defaults to <code>%displayName%=%.%</code>	Specifies a display name for the widget as text or by means of a script.
Popup Enabled	<code>true (default)</code> or <code>false</code>	Specifies if a secondary window is to open when a user clicks this label in a browser or the graphic view.
Status Effect	three options	<p>Configures what happens when the status of a bound value changes:</p> <p><code>Color</code> changes the background color.</p> <p><code>Color</code> and <code>blink</code> changes the background color and causes the value to blink.</p> <p><code>None</code> disables any effects when the status of a bound value changes.</p>

## About value bindings

These bindings bind to values that are typically under a component. Value bindings support features such as real-time graphics, mouse-over, and right-click actions.



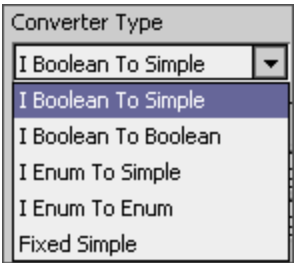
This pop-up opens when you right-click an object on a PX grid.

Property	Value	Description
Ord	Chooser; defaults to <code>null</code>	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Degrade Behavior	drop-down list; defaults to <code>None</code>	Specifies how the interface displays invalid options. For example, if a user does not have permission to invoke a specific action, a button bound to that action can be grayed out or hidden entirely.
Hyperlink	Chooser; defaults to <code>null</code>	Links to another object. When used, the link is active in the browser or in the graphic view.
Summary	Chooser; defaults to <code>%displayName%=%.%</code>	Specifies a display name for the widget as text or by means of a script.
Popup Enabled	<code>true</code> (default) or <code>false</code>	Specifies if a secondary window is to open when a user clicks this label in a browser or the graphic view.

Types of Converters

Converters are part of the system’s logic features. They change data from one type to another; for example, a `statusBoolean` to a `statusNumeric` so that a process, which outputs an inactive value, becomes a numeric value (1) in the next process. In most cases, when you animate a property, the correct data converter appears, by default, at the top of the list.

Figure 245. Types of converters



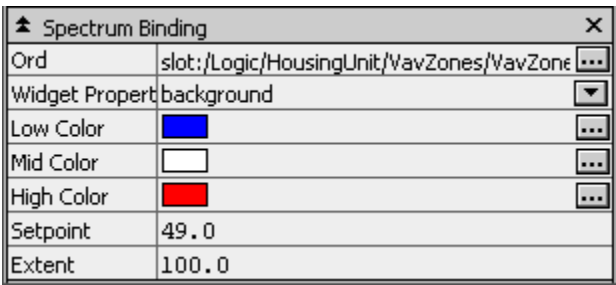
The following types of converters are available when using a value binding:

- I Boolean To Simple converts a number data type link (to-double, to-float, to-long, to-integer) resulting in a 0 value for a Boolean false, or 1 if a Boolean true.
- I Boolean To Boolean has a **False Value** converter property with a default value of 0. The default 0 keeps the statusBoolean value in synch with the source Boolean value. If **False Value** is set to 1, the linked statusBoolean value is opposite (NOT) the source.
- I Enum to Simple converts an enumerated value to a simple value.
- I Enum to Enum converts one enumerated value to the same type of value.
- Fixed Simple

About spectrum bindings

This binding animated a widget's brush (color) property by mapping a numeric value into a color range defined by lowColor, midColor, and highColor properties

Figure 246. Spectrum Binding properties



Property	Value	Description
Ord	Chooser; defaults to null	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Degrade Behavior	Chooser; defaults to null	Specifies how the interface displays invalid options. For example, if a user does not have permission to invoke a specific action, a button

Property	Value	Description
		bound to that action can be grayed out or hidden entirely.
Widget Property	drop-down list	Specifies the target property in the binding's parent widget. For example, if the spectrum binding has a bound label parent, this property can change the background or foreground property of the parent label. You can target only one property in the parent widget per binding. To target more than one, add additional bindings.
Low Color	chooser	Specifies the color for the lowest-value assignment. When the bound target value is less than the setpoint minus extent divided by two (2), it displays in this color. As the value bound to this property increases above the minimum value specified, the color changes, approaching the color set by the <code>Mid Color</code> property.
Mid Color	chooser	Specifies the color for the mid-range value. When the bound value is exactly at the setpoint, it displays in this color. As it increases above this point, the color changes, approaching the color set by the <code>High Color</code> property. As the value decreases below the setpoint, the color changes, approaching the color set by the <code>Low Color</code> property.
High Color	chooser	Specifies the color for the highest value assignment. When the bound target is greater than the setpoint plus extent divided by two (2), it displays in this color. As the bound value decreases below the maximum value specified, the color changes, approaching the color set by the <code>Mid Color</code> property.
Setpoint	number to one decimal	Specifies the mid-color value. For example, when set to 70, the value displays using the color you defined for <code>Mid Color</code> when it reaches 70.
Extent	number to one decimal	Represents the total range of the bound value, which maps from low to high.

About set point bindings

This binding displays the current value of a set point and also to provide the ability to modify it. A set point is typically a status value property such as fallback. The set point binding ORD must resolve down to the specific property that is being manipulated. If it is bound to a component or to a read-only property, then the binding attempts to use a set action to save.

Figure 247. Set Point Binding properties

Set Point Binding	
Ord	station:/slot:/Logic/HousingUnit/AirHandler/SetpointTei
Hyperlink	null
Summary	%displayName% = %.%
Popup Enabled	true
Widget Event	actionPerformed
Widget Property	value

Property	Value	Description
Ord	Chooser; defaults to null	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Hyperlink	Chooser; defaults to null	Links to another object. When used, the link is active in the browser or in the graphic view.
Summary	Chooser; defaults to %displayName%=%.%	Specifies a display name for the widget as text or by means of a script.
Popup Enabled	true (default) or false	Specifies if a secondary window is to open when a user clicks this label in a browser or the graphic view.
Widget Event	drop-down list	Defines the action to perform on the binding of the target component when an event is fired by the parent widget.
Widget Property	drop-down list	Specifies the target property in the binding's parent widget. For example, if the spectrum binding has a bound label parent, this property can change the background or foreground property of the parent label. You can target only one property in the parent widget per binding. To target more than one, add additional bindings.

About Increment Set point bindings

This type of set point binding is used increment or decrement a numeric value.

**Figure 248.** Increment set point binding properties

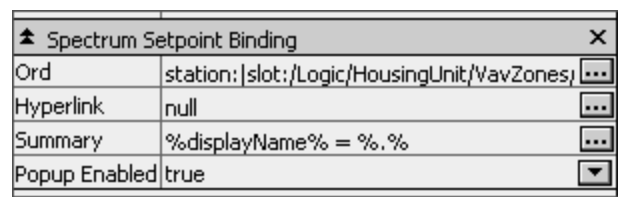
Increment Set Point Binding		X
Ord	null	...
Hyperlink	null	...
Summary	%displayName% = %.%	...
Popup Enabled	true	▼
Widget Event	actionPerformed	▼
Increment	1.0	

Property	Value	Description
Ord	Chooser; defaults to null	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Hyperlink	Chooser; defaults to null	Links to another object. When used, the link is active in the browser or in the graphic view.
Summary	Chooser; defaults to %displayName%=%.%	Specifies a display name for the widget as text or by means of a script.
Popup Enabled	true (default) or false	Specifies if a secondary window is to open when a user clicks this label in a browser or the graphic view.
Widget Event	drop-down list	Defines the action to perform on the binding of the target component when an event is fired by the parent widget.
Increment	positive or negative number to a single decimal point	Defines a value by which to increase or decrease the current value. A positive number increments the value. A negative number decrements it.

About spectrum set point bindings

This binding animates a widget's brush (color) property. You use it in conjunction with a spectrum binding to animate the Mid Color properties.

Figure 249. Spectrum set point binding properties

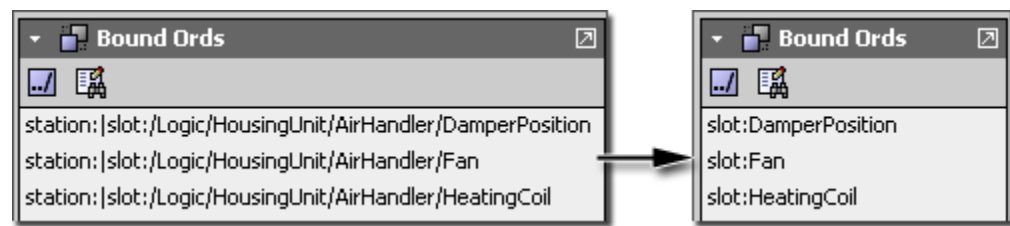


Property	Value	Description
Ord	Chooser; defaults to null	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Hyperlink	Chooser; defaults to null	Links to another object. When used, the link is active in the browser or in the graphic view.
Summary	Chooser; defaults to %displayName%=%.%	Specifies a display name for the widget as text or by means of a script.
Popup Enabled	true (default) or false	Specifies if a secondary window is to open when a user clicks this label in a browser or the graphic view.

Relative and absolute bindings

ORDs can define an absolute path to a specific device point or a relative path that identifies the same point in multiple stations.

Figure 250. Absolutely bound ORDs and relatively bound ORDs



An absolute `Ord`, such as: `station:/slot:/Logic/HousingUnit/AirHandler/DamperPosition` defines the absolute path to a single unique `DamperPosition` regardless of where the Graphic file or the parent component is located. If the same Graphic file is attached to a view that belongs to a different component, this absolute path ensures that the value always resolves to the original component.

A relative `Ord`, such as `station:/slot:DamperPosition` resolves relative to its current parent. This relative path makes the Graphic file resolve data bindings correctly to identically named components that reside in different locations, thus making one Graphic file usable in many views.



About action bindings

This binding invokes an action on the binding target component when an event is fired by the parent widget. The ORD of an action binding must resolve down to a specific action within a component. Examples of actions include: active, inactive, override, and other commands.

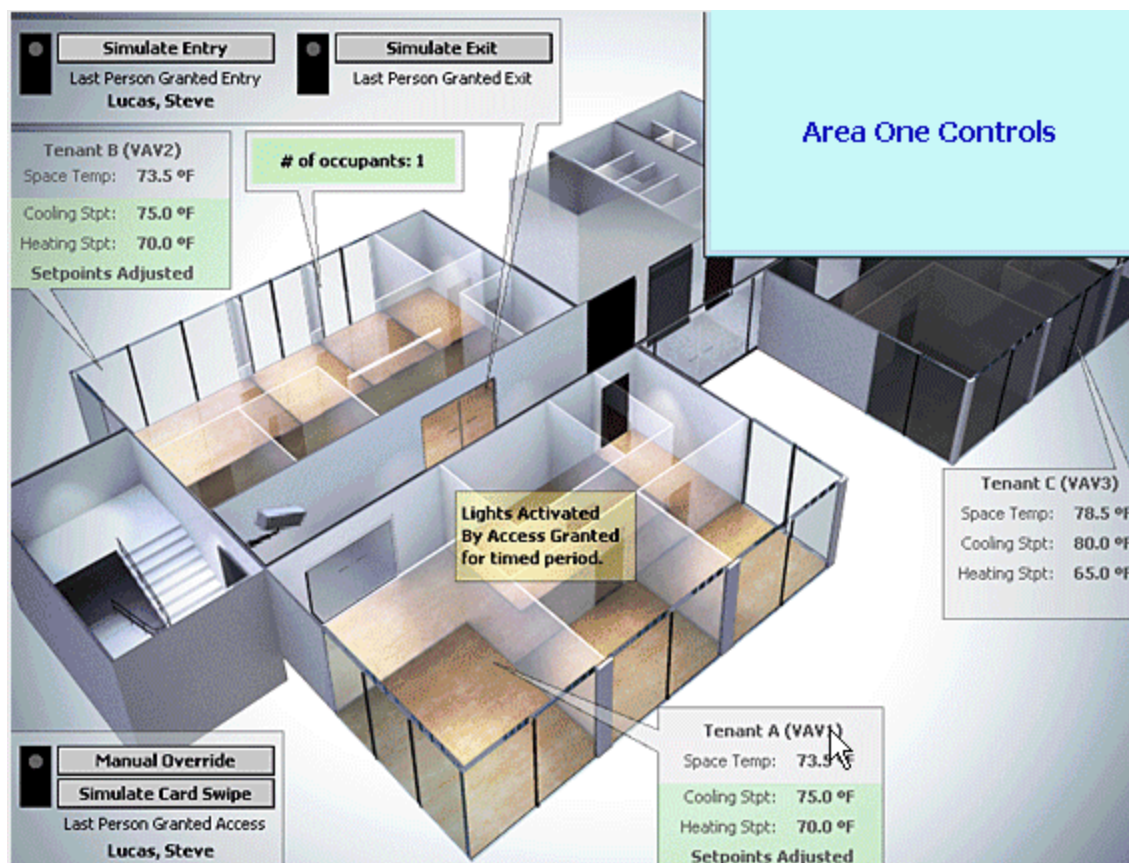
Figure 251. Action Binding properties

⬆ Action Binding X		
Ord	station:/slot:/Logic/HousingUnit/Air	
Widget Event	actionPerformed	▼
Action Arg		

Property	Value	Description
Ord	Chooser; defaults to null	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Widget Event	drop-down list	Defines the action to perform on the binding of the target component when an event is fired by the parent widget.
Action Arg	read-only	Displays an action argument.

View Graphic

This view represents the inside of a building.

**Figure 252.** Example graphic view

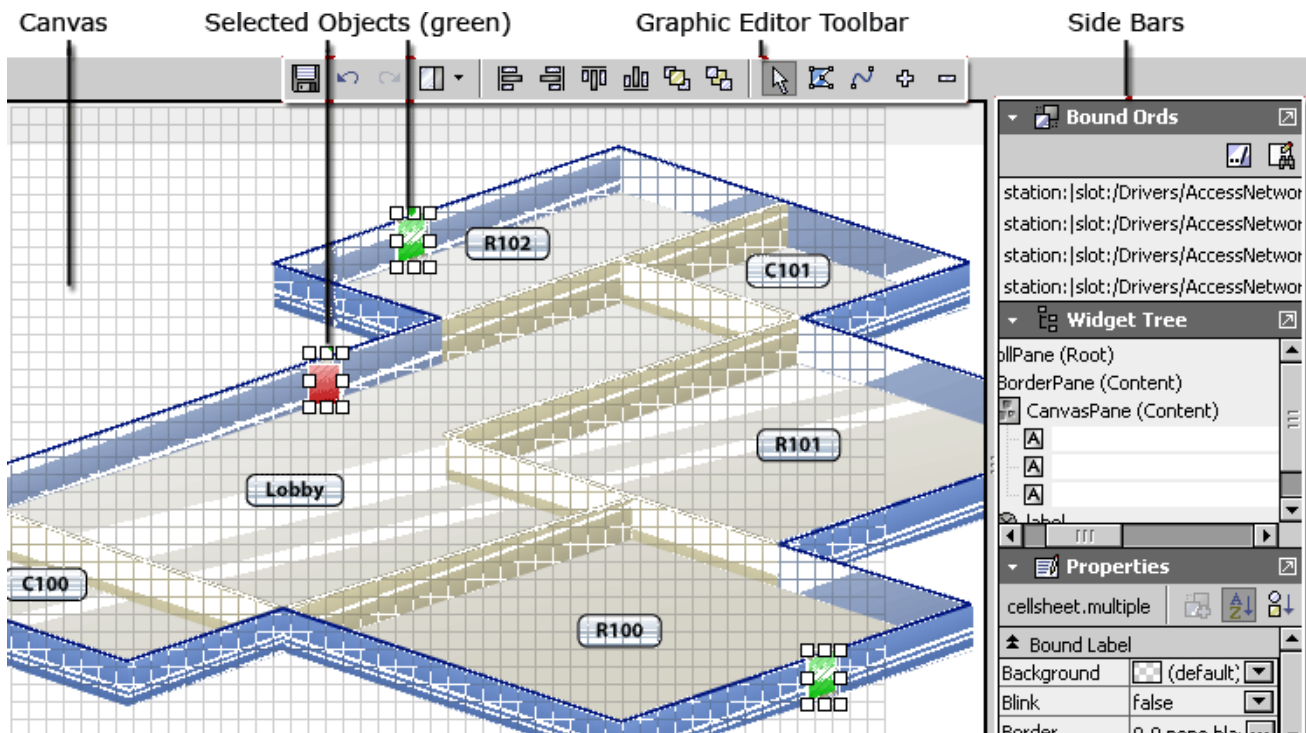
You access this view from the Graphics view by double-clicking the Display Name record in the Graphics view

or by selecting the record and clicking the View Graphic button (  ).

You create custom graphics using the Graphics Editor view. Graphics can contain controls, links, and indicators related to building access and automation system controls. Graphics may be designed specifically for one of two **Target Media**: HxPxMedia or WorkbenchPxMedia.

## Graphic Editor view

The Graphic Editor view provides a three-dimensional canvas and properties, which you use to set up the graphic.

**Figure 253.** Graphic Editor view

You access this view from the main menu by clicking **Controller (System) Setup > Miscellaneous > Graphics >**

**Graphics Management** followed by clicking the New button (  ) or selecting an existing graphic and clicking

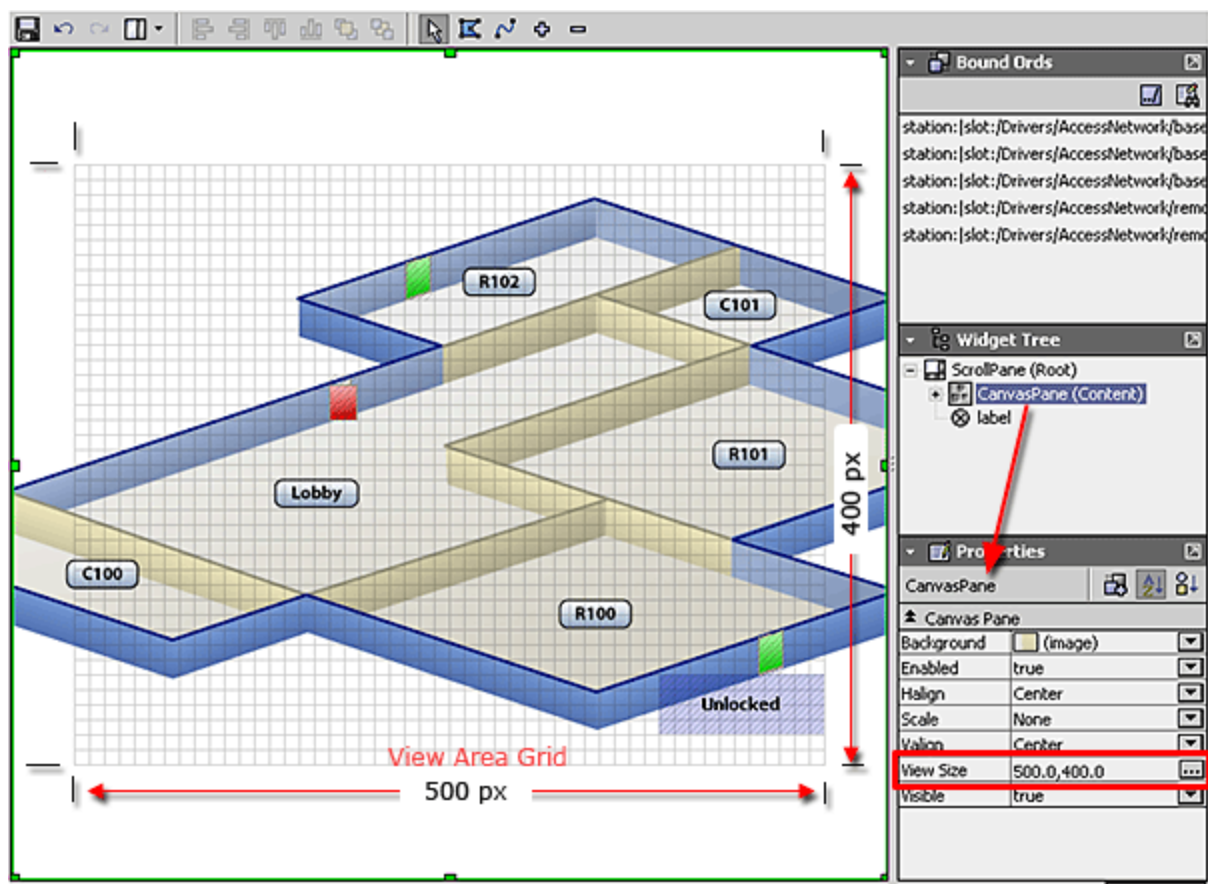
the Graphic Editor button (  )

### About the Graphic Editor canvas

The canvas is the largest area of the editor. It defines the visual boundaries of the graphic page and serves as your work area for previewing the graphic file as you develop it using the tools in the Graphic Editor.

You place widgets on the canvas and edit them and bind data to them using one or more of the side bars and additional windows, which are documented elsewhere. Most of the time, the canvas provides a live view of any widgets you add—without having to return to the Graphic Viewer. However, some graphic features may only appear in the Graphics Viewer.

**Figure 254.** Graphic Editor canvas



The Canvas has the following optional work aids:

- The grid provides a visual aid for graphical alignment. The grid lines display vertical and horizontal lines as well as define the visible area of the page.
- Hatching is an area of light-gray diagonal lines that define the boundaries of items that are placed on the canvas.
- View area

The view area is defined by the **View Size** property in the Canvas pane property pane. Visually, the view area is defined by the grid that displays in the editor only. The Graphic viewer clips off any part of the graphic that appears outside of the view area (when you select the view under the **Console** node of the navigation tree).

Property	Value	Description
Background	drop-down list for .png file	Selects the image of your facility to use as the background.
Enabled	drop-down list, defaults to <code>true</code>	Starts the functioning of components that make up the graphic.
Halign	drop-down list, defaults to <code>Center</code>	Aligns the background image horizontally.

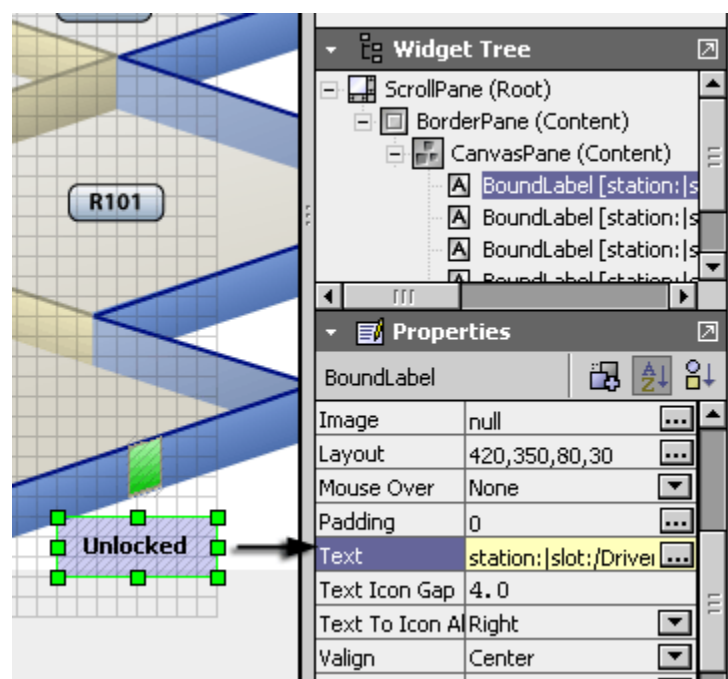
Property	Value	Description
Scale	drop-down list, defaults to <code>None</code>	Increases and decreases the background image proportionally.
Valign	drop-down list, defaults to <code>Center</code>	Aligns the background image vertically.
View Size	Chooser	Defines the dimensions of the background graphic.
Visible	drop-down list, defaults to <code>true</code>	Turns the graphic view on and off.

About Graphic Editor objects (widgets)

These objects, called widgets, represent the information to visualize in the graphic. Configuring widget properties defines the features, behaviors and appearance characteristics of widgets.

You view these properties when you right-click the canvas and select a bound label.

Figure 255. Widget properties



Property	Value	Description
Image	chooser (defaults to null)	Selects an image to include in the graphic.
Layout	chooser (pixels)	Defines the size of the graphic in pixels (picture elements).
Mouse Over	drop-down list (defaults to <code>None</code> )	Selects what to do when passing the


Property	Value	Description
		cursor over the graphic.
Padding	chooser (defaults to zero (0))	Defines space around the graphic.
Text	ORD	Identifies the location in the station of a text file.
Text Icon Gap	number (defaults to 4.0)	Defines the distance between the selected icon and the text box that describes it.
Text to Icon Alignment	drop-down list	Defines horizontal alignment: Right, Left, Center
Valign	drop-down list	Defines vertical alignment: Top, Bottom, Center

## About the Graphic Editor toolbar

This collection of buttons at the top of the view includes the **Save** and **Undo** buttons, as well as several other context-sensitive graphic alignment and drawing tools. Toolbar functions vary depending on the context. When you first open the Graphic Editor view to create a new graphic the following tools are available.

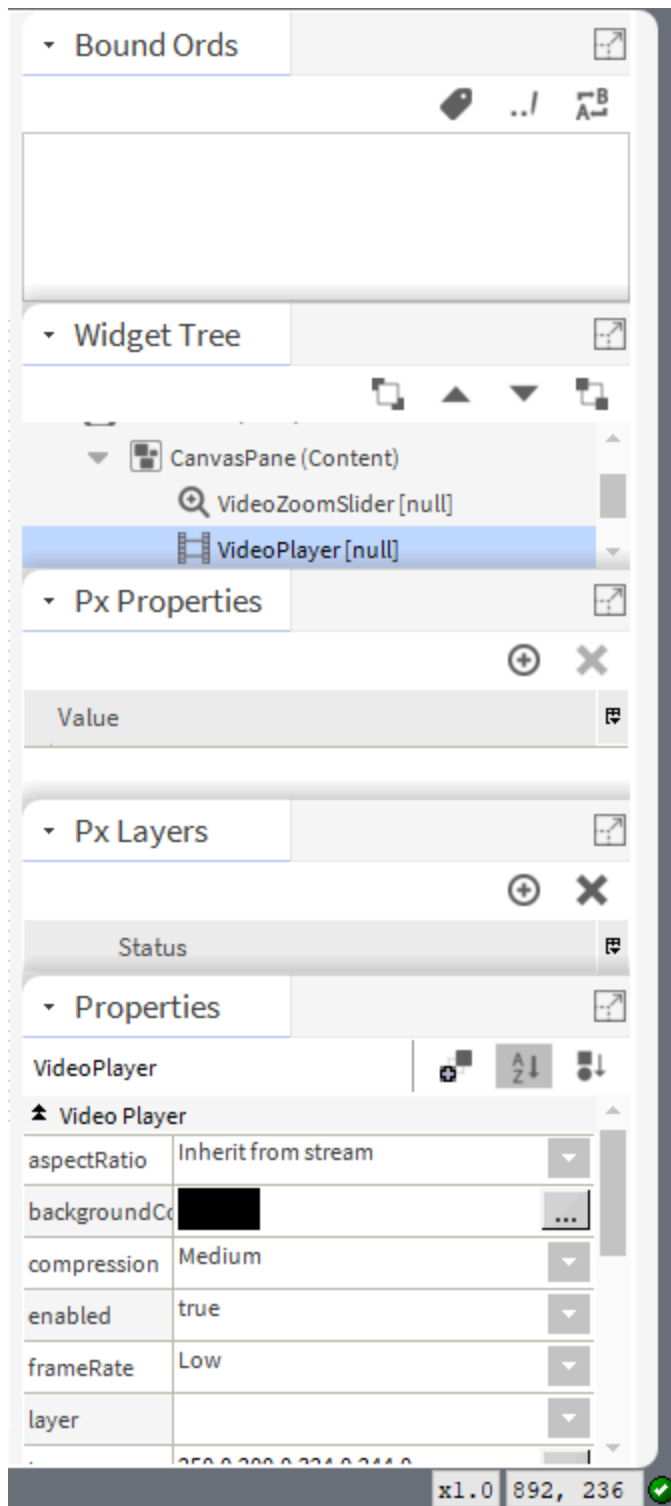
**Figure 256.** Default Graphic Editor Toolbar buttons



-  Save saves the graphic in the station database.
- Undo and Redo perform the tasks their names imply.
- Right side bar menu opens a drop-down menu of side bar options for the Graphic Editor.
- Alignment options align the selected widgets and objects at their left, right, top and bottom edges.
- The To Top and To Bottom icons adjust the position of object in relationship to each other.
- Select activates the pointer tool for selecting objects.
- Add Polygon adds a square, rectangle, etc.
- Add Path allows you to draw free-form lines.
- Add Point adds a point on a line or to a polygon.
- Delete Point removes the selected point from a path or polygon.

## About the side bar pane

This pane appears on the right side of the view pane when **Show Side Bar** is selected from the **Pane** menu on the Graphic Editor Toolbar. Use this menu to hide or display individual side bars and to show or hide the Graphic Editor side bar pane. The side bars provide the properties for creating graphics.

**Figure 257.** Graphics side bar

- The Bound ORD side bar lists all the bound ords in the current graphic. An ORD is the path to the data, which the graphic displays.
- The Widget Tree displays the hierarchy of widgets (panes, labels, graphic elements, and so on) in the



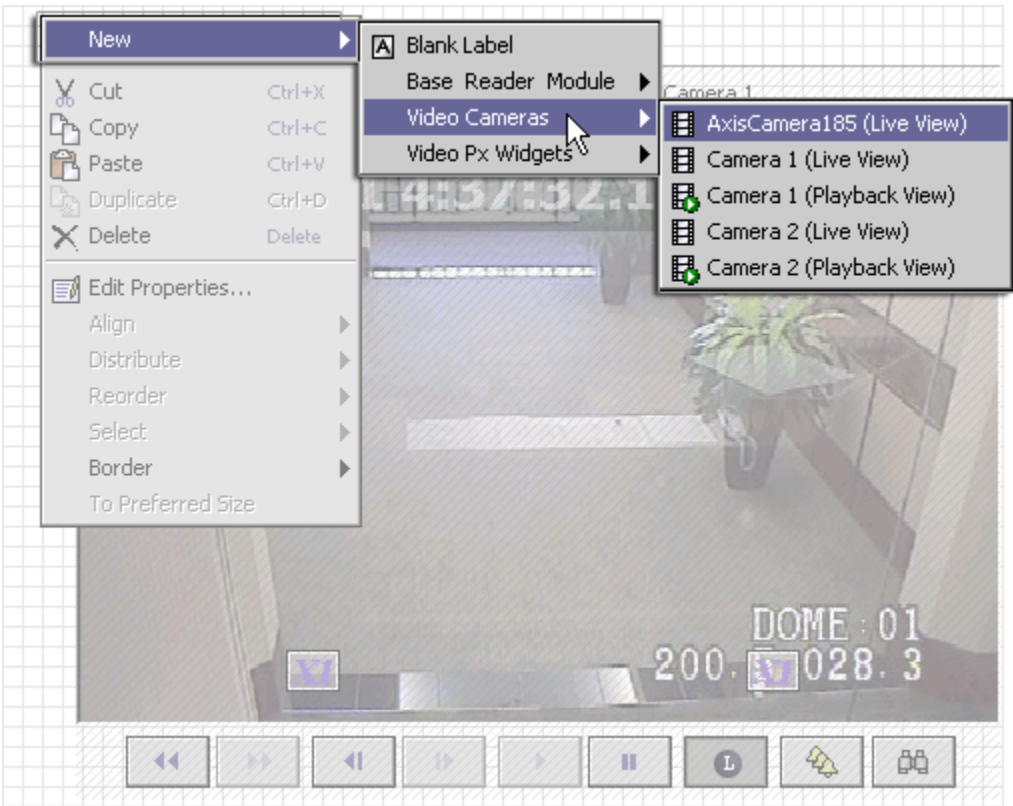
current Px view.

- Px Properties relate to the specific widget.
- Px Layers group objects in the Px Editor.
- Properties populate based on the type of widget.

Graphic Editor pop-up menu - available video cameras

This popup (right-click) menu includes context-sensitive menu items.

**Figure 258.** Graphic Editor popup menu - available video cameras



**Figure 259.** New menu items

Menu item	Description
Blank Labels	Selects a standard Px label widget, which you use to annotate the graphic.
Base Reader Module, Remote Reader Module	These menus are context sensitive and list widgets that represent the devices available under each module. Adding one to the graphic adds a representation of the device to the graphic.
Video Cameras	This list of widgets represents the camera(s) connected to your



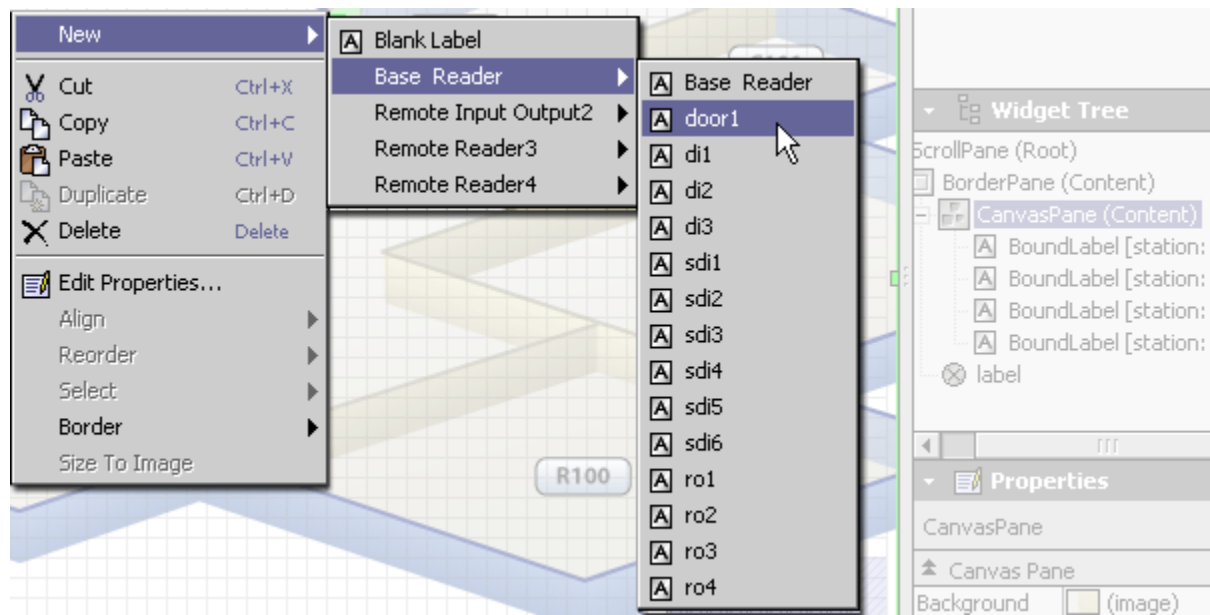
Menu item	Description
	Supervisor PC or subordinate controller. Each widget is labeled in the menu to indicate that the device it represents is either used to play back prerecorded video or to display live video. The playback icon also identifies playback widgets in the menu.
Video Px Widgets	A Supervisor station can support local or remote video graphics (using Px) and have them served by cameras that are attached to remote stations under the Supervisor's NiagaraNetwork. The following Px widgets support remote video:Live Video PlayerControl PanelPan Tilt JoystickZoom SliderCamera WidgetMouse Down WidgetVideo Multistream Pane

Refer to the “Video installation” chapter in the *Niagara Enterprise Security Installation and Maintenance Guide* for more about video devices and video.

Example: new Base Reader

The following is an example of the popup menu, Base Reader menu items.

Figure 260. Graphics Editor popup menus



The popup menu also provides many other context-sensitive commands, including the ability to add a border pane to a selected object.

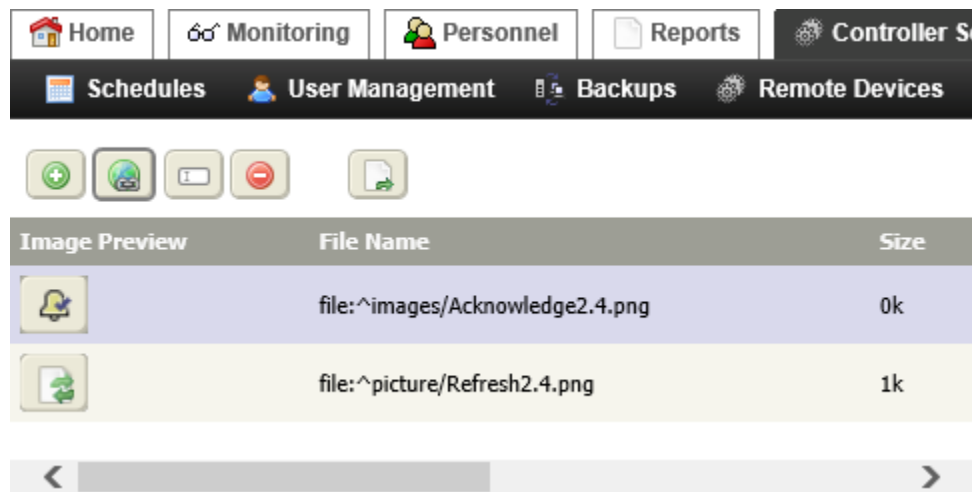
**NOTE:** If you add a door that is in an alarm condition, by default, the door blinks until the door is out of alarm and the alarm is acknowledged.

### Images view

This view lists all the images available on the local station. These images are the artifacts to make the graphic look like your building. You can have a graphics artist draw these artifacts.

#### Buttons

**Figure 261.** Images view



This view displays when you select **Images** from the **Controller (System) Setup > Miscellaneous > Graphics** from the main menu.

The control buttons at the top of the view provide standard controls, including an Add control button (  ) at the top of the view for adding a new image.


#### Columns


Column	Description
Image Preview	Provides a thumb-nail view of the image.
File Name	Identifies the name of the image file.
Size	Indicates the size of the image file.

### Add New Image view

The properties in this view provide a way for you to add image files to a designated location on the controller (an `images` folder, by default). Images that are loaded on the controller are available for use in graphic views.

Figure 262. Add New Image view

 Save

 Images

File Path

File to Upload

Browse...

Property	Value	Description
File Path	file_path (defaults to ^images)	Defines the folder under the station for storing uploaded image files. The ^ character specifies the station root directory. If you change the file path, the station creates the directory on the controller at the designated location.
File to Upload	File chooser	Provides a way to browse to and select the desired image for transferring to the controller.

### Display Image view


This view displays when you click the Hyperlink control button (  ) in the Images view. The view displays the file path as the view title directly above a link to the Images view. The single, selected image displays in the view.

Figure 263. Display Image view

file:^graphics/edit.png

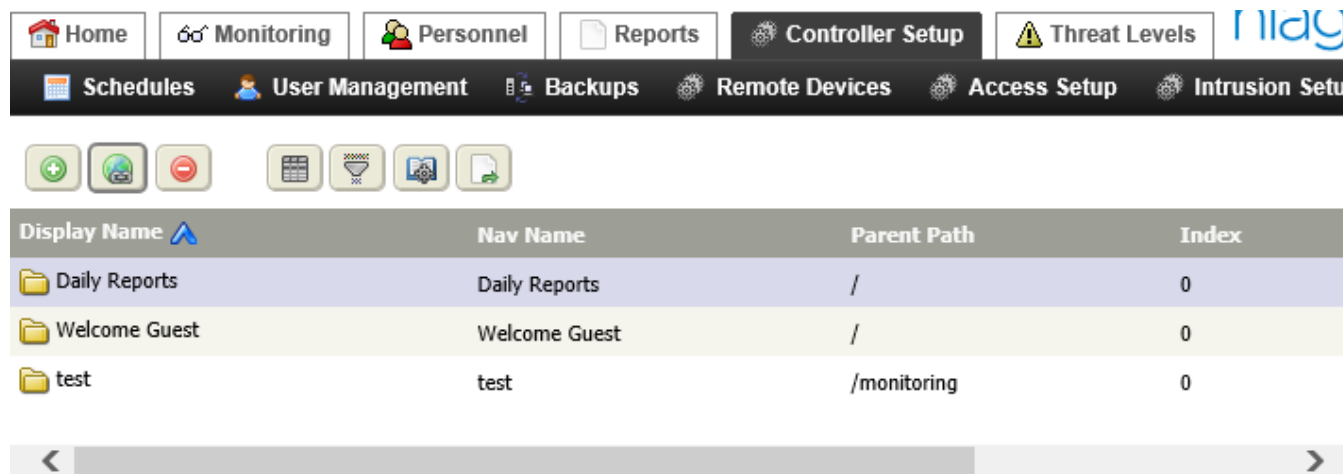
 Images



### Navigation Groups view

Nav Groups are custom menu items used to collect and organize graphic views. Once a nav group is created, you may assign child views to the group.

Figure 264. Navigation Groups view



You access this view by expanding **Controller (System) Setup > Miscellaneous > Graphics** and clicking **Navigation Groups**.

A nav group displays in the menu under its assigned parent. This view displays a table of all the navigation groups that are available on the local station. This view is also where you initiate the process of adding a new navigation group using the Add control button at the top of the view.

### Add New (or edit) Nav Group view

This view configures Nav group properties.

Figure 265. Add New Nav Group view

Save

Nav Groups

Nav Group

Nav Name

Display Name

Parent Path

Home

Icon

module://icons/x16/folder.png

Index

0

You access this view from the main menu click **Controller (System) Setup > Miscellaneous**, expand the **Graphics** menu and click **Navigation Groups**.

Property	Value	Description
Nav Name	text	Defines an identifier for the nav group. This name appears in the menu if no <code>Display Name</code> is specified. You may want to use this property for a design-logical name and use the <code>Display Name as</code> a more user-friendly name.
Display Name (BFormat general)	text	<p>Defines a BFormat string used to format text by using values obtained from objects.</p> <p>You specify this string as normal text with embedded scripts identified by the percent (%) character. The driver maps calls within the script to an object's methods. Use the dot operator (.) to chain calls. To insert a percent symbol itself, use two percent symbols (%%).</p> <p>For examples, click the question mark icon next to this property.</p>
Parent Path	drop-down list	<p>Defines where in the hierarchy to place a new menu item. A hierarchy of options matches the current navigation structure. You can choose the menu or submenu here to specify where, in the overall system navigation hierarchy, to place your new menu item.</p> <p>For example, to place a menu item under the Remote Devices submenu, choose the Remote Devices option in this property.</p>
Icon	path	Defines where the icon used for this column is located.
Index (Snmpp)	number	Displays the value that corresponds to the column index of the object created for it in the Input or Output Table.



# Chapter 13. Threat Levels

A threat level defines a range of operational values (threat levels) related to overall building security. Threat level groups define facility spaces for the purpose of managing perceived threats.

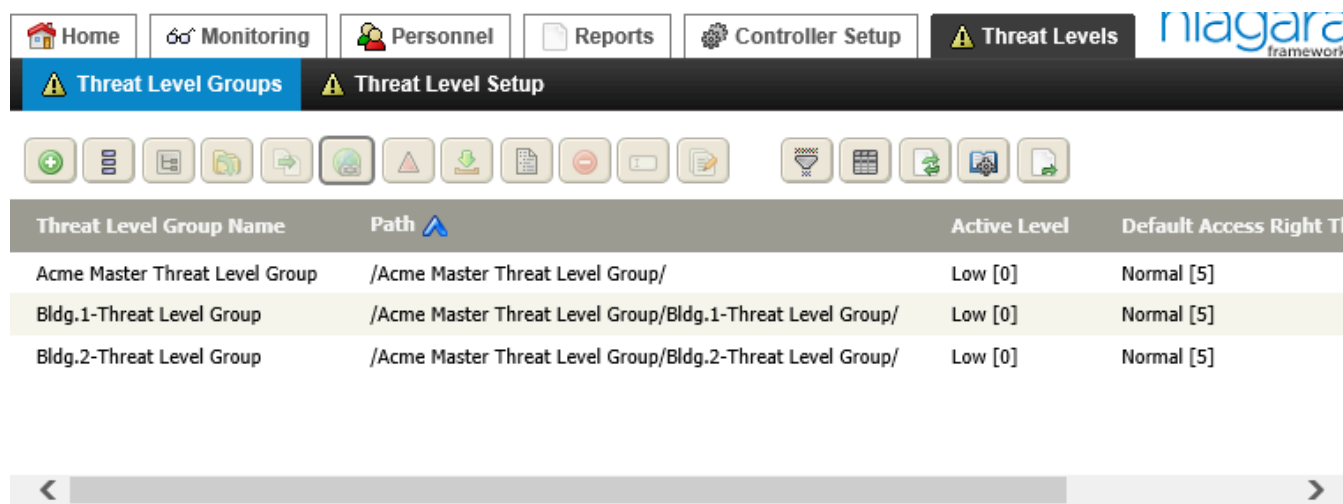
## Threat level groups view

This view displays a table that contains the currently-configured Threat Level Groups. Using this view you assign access rights and activation badges to a specific Threat Level Group.

### Buttons






Using this view you assign access rights and activation badges to a specific Threat Level Group. On the Threat Level Group tab, you set up the **Default Access Right Threat Level**.




Figure 266. Threat Level Groups view



To open this view, expand the **Threat Levels** node in the menu and click **Threat Level Groups**.

You edit threat level hierarchy relationships using the following control buttons:

-  Add opens the Add New Threat Level Groups view.
-  Show Top Level filters the table to display only parent Threat Level Groups.
-  Go into shows just the selected Threat Level Group and its children in the Threat Level Groups view.
-  Create child opens the Add New Threat Level Group window for the purpose of creating a Threat Level Group that is automatically assigned as a child to the selected group.
-  Move transfers the selected child Threat Level Group to a different parent. The Move window has one property: **New Parent**. You use this Ref chooser to locate the new parent.

-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row.
-  Activate Threat Level turns on the state of emergency.
-  Retrieve Active Status confirms that the threat level has been activated.

Columns

Column	Description
Threat Level Group Name	Identifies the purpose of the group.
Path	Shows where the Threat Level Group is located in the .overall parent-child hierarchy of Threat Level Groups.
Active Level	Indicates the current threat level.
Default Access Right Threat Level	Each Threat Level Group has a default access right. This column shows the current assigned access right for each displayed group.
Tenant Name	Identifies the Tenant(s) associated with the displayed Threat Level Group.

Threat Level Group filter

This filter sets up criteria to search the system database for specific threat level groups.

Figure 267. Threat Level Groups filter

Filter

☐ Threat Level Group Name

☐ Path

☐ Active Level

☐ Default Access Right Threat Level

☐ Tenant Name

%

%

%

Must Include

Must Include

Must Include

☒ Case Sensitive

☒ Case Sensitive

☒ Case Sensitive

Ok

Cancel

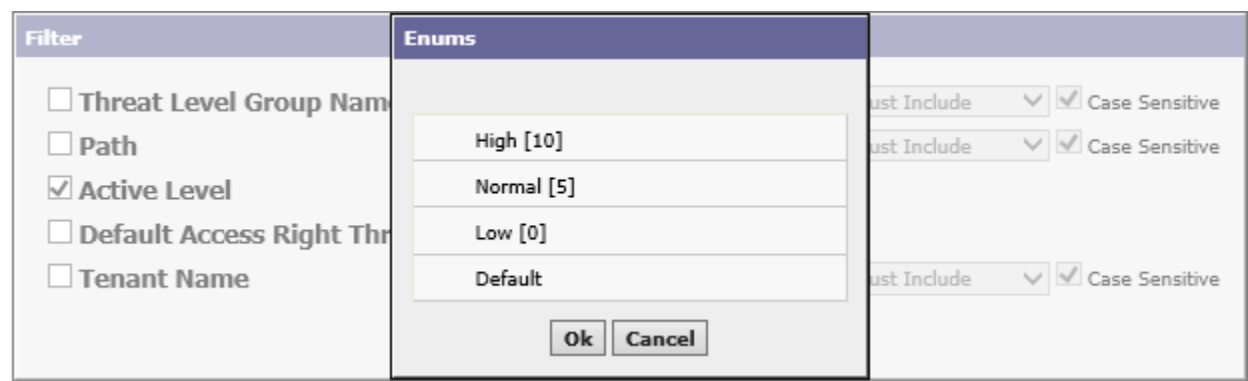
Criterion	Value	Description
Threat Level Group Name	wildcard	Defines the name(s) to search for.
Path	wildcard	Defines the URL to search.
Active Level	Enums chooser (default to: High, Normal, Low or Default)	Opens a window for selecting the threat level.
Default Access Right Threat Level	Enums chooser (default to: High, Normal, Low or Default)	Opens a window for selecting the default threat level to associate with the access right.
Tenant Name	wildcard	Defines the tenant name.



Activate Threat Level window

You activate a pre-configured threat level when an action is required to isolate or otherwise control an active threat.

Figure 268. Activate Threat Level window



The drop-down list levels default to:

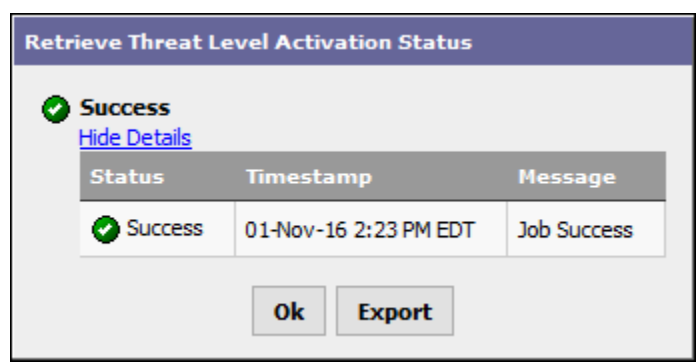
- Low [0]
- Normal [5]
- High [10]

To customize your configuration, you can add your own levels.


Retrieve Active Level Activation Status window

This feature refreshes the status of the threat level that is mapped to the remote station.

Figure 269. Retrieve Threat Level Activation Status window



To access this window you select a threat level group in the Threat Level Groups view and click the Retrieve

Active Status button (  ).

**Table 61.** Retrieve Threat Level Activation Status table columns

Column	Description
Status	Indicates the result of the action.
Timestamp	Indicates when the action occurred.
Message	Provides a short description of the action.

## Add New (or edit) Threat Level Group view

This view manages threat level groups.

### Links

**Figure 270.** Add New Threat Level Group view

HomeMonitoringPersonnelReportsController SetupThreat Levels

Threat Level GroupsThreat Level Setup

SaveThreat Level Groups

Display Name

Threat Level Group2

Parent

None

Summary

Threat Level Group

Activation Badges

Access Rights

Active Level

Low [0]

Default Access Right Threat Level

Low [0]

Active Ordinal

0

Tenant




None

To open this view, click the **Add** button on the Threat Level Groups view.

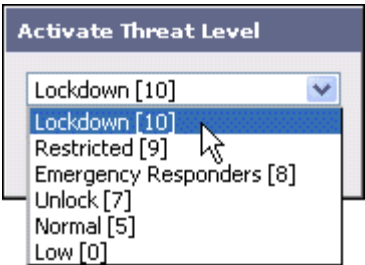
- **Save** updates the station database with any changes made to threat level properties.
- **Threat Level Groups** returns to the Threat Level Groups view.




### Buttons

These buttons support threat level group configuration:

-  Save updates the database with the current information.
-  Threat Level Groups returns to the Threat Level Groups view.
-  Activate Threat Level opens a drop-down list of threat level group options. Choosing one of these options, followed by clicking **Ok** turns the threat level on.

**Figure 271.** Activate Threat Level window



-  Retrieve Active Status initiates a system-wide job to determine what the active level is on all threat level groups across all controllers. The job returns a “Threat Level Mismatch” message if it finds a mismatched threat level group on a subordinate or peer station in the enterprise.  
**NOTE:** If any station was down at the time of a threat level change activation, that station has a mismatch. This process identifies any station that is currently down or has a mismatched threat level group.
-  Manage Devices/Drivers opens the Manage Drivers or Manage Devices window, which is used to Add, Delete, Rename, Duplicate, Copy, and Cut system drivers or devices.
-  Add Child initiates creation of a new threat level group that you can assign as a child to the group you are editing.  
**NOTE:** You cannot cancel threat level jobs, such as Activate Threat Level and Retrieve Active Status, from the browser once they are started.

Properties

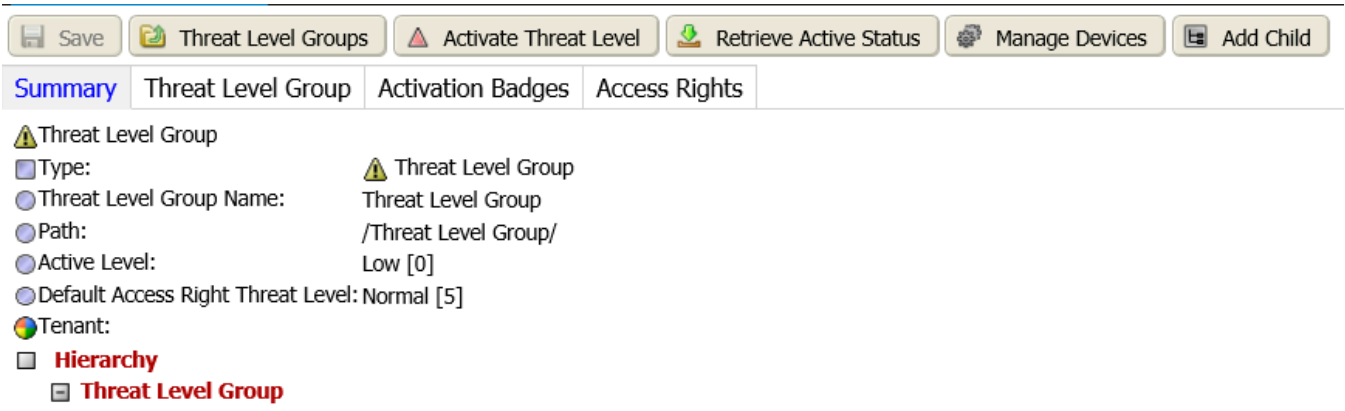
Property	Value	Description
Display Name	text	Creates an object name for display purposes, which may differ from the actual object name.
Parent	Ref Chooser	Provides a read-only display of any threat level group that is assigned as a parent group to the group that you are creating. The navigation arrows at the right side of the property open a <b>Ref Chooser</b> window for browsing, choosing and assigning a parent from existing groups.
Active Level	read-only	Displays the active (current) threat level setting for the threat level group. There can be only one active threat level per group, however, different groups may have different active threat levels.

Property	Value	Description
Default Access Right Threat Level	drop-down list	Selects the threat level to associate with a card holder by default when an access right using this threat level group is assigned to a card holder. With the threat level group assigned to an access right, you can edit this default level value without having to change the assignment on the access right.
Active Ordinal	read-only	Displays the active (current) threat level as an integer. Ordinals are the characteristic identifiers that are paired with string identifiers that can be edited. These are called tags in enumerated data types where there is a discrete range of values. This ordinal is displayed [in brackets] next to the threat level display text (tag) in other properties.
Tenant	Ref chooser	Defines the company name of the associated tenant.

Summary Tab

This tab displays information about the selected threat level group and indicates current active level and default access right level.

Figure 272. Threat level group summary



Some properties are not populated until you save the group. In the edit threat level group view, these properties display current information, including links to the appropriate edit view for a specific piece of information. For example, **Hierarchy**, **Remote Stations**, and **Activation Badges** properties display as links.

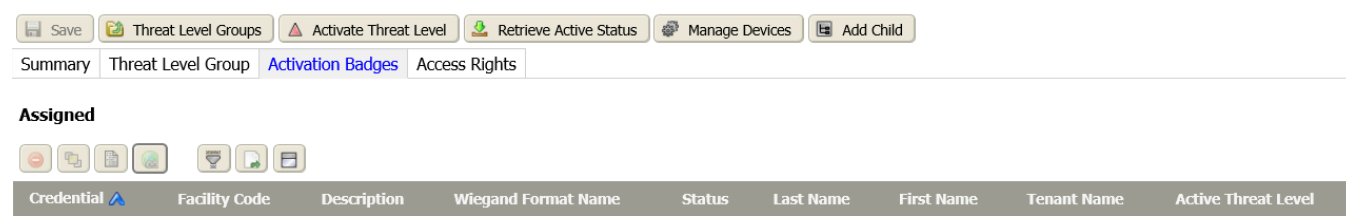
Property	Description
Type	Identifies the record type. In this case it is a threat level group.
Threat Level Group Name	Displays the name of the group.
Path	Identifies the location of the group in the station.
Active Level	Reports the current group level.

Property	Description
Default Access Right Threat Level	Reports the normal level for the group when it is activated.
Tenant	Identifies the tenant for whose location uses this threat level group.

Activation Badges tab

This tab provides standard assign-mode controls for adding existing activation badges to the new threat level group. An activation badge is the badge assigned a person who is responsible for activating the threat level group.

Figure 273. Activation Badges tab



To access this tab in a Supervisor station click **System Setup > Threat Level Groups**, double-click a group row in the table, and click the Activation Badges tab.

You access this tab on remote controllers only when you use the **Manage Devices** button to add an activation level input device.

Table 62. Activation Badges table columns

Column	Description
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description (badge)	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Last Name	Reports the family name of the person.
First Name	Reports the given name of the person.
Tenant Name	Reports the name of the associated tenant.
Active Threat Level	Displays the currently-active threat level.

Access Rights tab

This tab provides standard assign-mode controls for adding access rights to the new threat level group.

Figure 274. Access Rights tab



To access this tab in a Supervisor station click **System Setup > Threat Level Groups**, double-click a group row in the table, and click the Access Rights tab.

This tab is available on remote controllers only when you use the **Manage Devices** button to add an activation level output device.

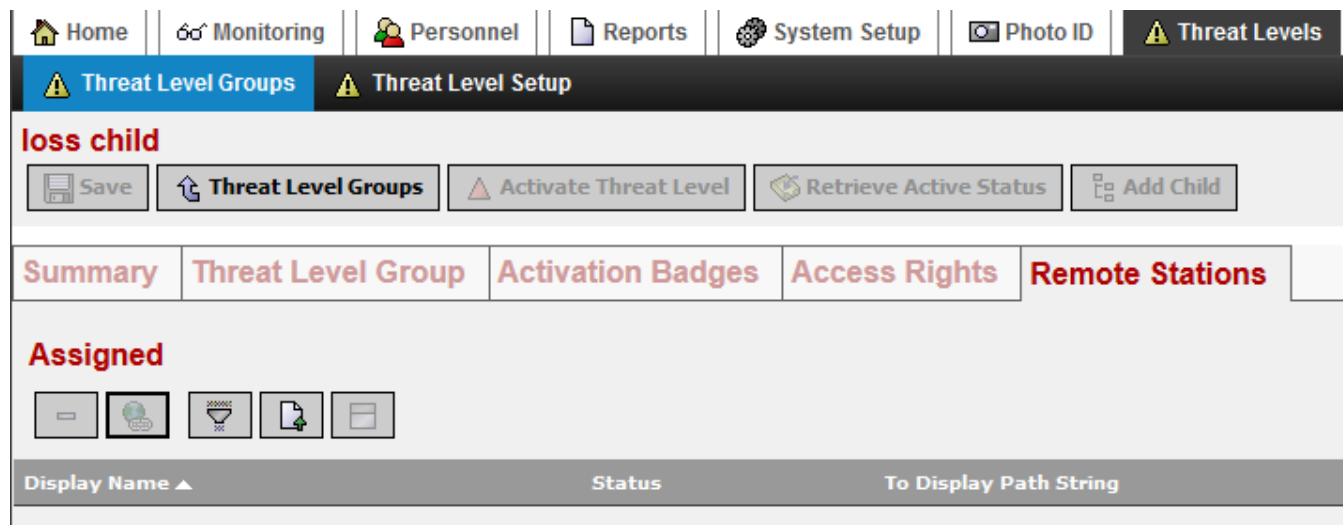
Table 63. Access rights tab table columns

Column	Description
Access Right Name	Identifies the title of the access right associated with the entity.
Schedule Name	Reports the name of the associated schedule (if any).
Integration Name, Niagara Integration ID	Reports the name of the associated integration ID. The system performs building automation actions, such as turning the lights on, associated with this type of ID.
Tenant Name Tenant	Reports the name of the associated tenant.
Threat Level Group Name	Reports the name of the associated threat level group.

Remote Stations tab

This tab provides standard assign-mode controls for adding remote stations to a threat level group.

Figure 275. Remote Station tab



To access this tab in a Supervisor station click **Threat Levels > Threat Level Groups**, double-click a group row in the table, and click the Remote Stations tab.

Table 64. Remote Stations table columns

Column	Description
Display Name	Reports the name that describes the event or function.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
To Display Path String	Defines the station path for this zone.

### Threat Level Setup view

This view and tab (Threat Level Setup) creates, edits, or deletes threat levels. Using this view you create your own customized threat level system.

Activation alert and alarm links

Figure 276. Threat Level Setup tab

Home

Monitoring

Personnel

Reports

Controller Setup

Threat Levels

Threat Level Groups

Threat Level Setup

Save

Threat Level Setup

Activation Initiated Alert

Alarm Source Info »

Activation Failure Alert

Alarm Source Info »

Activation Complete Alert

Alarm Source Info »

Activation Mismatch Alarm

Alarm Source Info »

Threat Level Range

Level	Name
10	High
5	Normal
0	Low

activationFailureAlarm

Alarm Source Info »

To access this view/tab, click **Threat Levels > Threat Level Setup**.

The view has a **Save** control button at the top of the view area and a **Threat Level Setup** tab with two main areas that contain properties to configure.

The chevrons to the right of these properties access alarm properties to configure for each type of threat level situation.

- An **Activation Initiated Alert** configures the alarm to generate when your an authorized person swipes a threat level group activation badge.
- An **Activation Failure Alert** configures the alarm to generate when an authorized person swiped a threat level group activation badge, but the system was unable to activate the group.
- An **Activation Complete Alert** configures the alarm to generate when an active threat level group is no longer needed.
- An **Activation Mismatch Alarm** relates to a database replication scenario where the current activeLevel of a Threat Level group does not match the activeLevel of the Threat Level group in the database that is being replicated.
- An **activationFailureAlarm** generates when an activating a threat level fails to activate or has a problem activating.



Each activation alert and activation failure alarm provides a set of identical properties, which are documented in a separate topic.



Threat Level Range table

This table sets up building access based on the current threat level. For example, in a range from zero (0) to five (5), a person assigned to level three (3) would have access to a specific location when threat levels 0 through 3 are active, but would not have access to the same location when levels 4 and 5 are active. This range defines the meaning of each level from least significant (0) to most severe (10).

Two buttons support the configuration of threat level ranges:

-  Add opens the **Add** window for creating a new threat level.
-  Edit opens an edit window for changing a selected threat level’s properties.

The table summarizes the configured thread levels.

Column	Description
Level	Assigns an arbitrary number to create a threat level.
Name	Provides a description of the level.

Activation alerts

These alerts configure alert properties for the following threat level activation states: Activation Initiated, Activation Failure, Activation Complete, Activation Mismatch. Each **Alarm Source Info** property expands by clicking the icon to the right of the property to display a list of additional properties as follows. Alerts monitor data sources which, when true, indicate there is an issue that requires attention. For Alerts, there is no "toNormal" transition.

Figure 277. Alarm Source Info adapted to threat levels

HomeMonitoringPersonnelReportsSystem SetupThreat Levels

Threat Level GroupsThreat Level Setup

Save

Threat Level Setup

Activation Initiated Alert

Alarm Source Info >>

Activation Failure Alert

Alarm Source Info >>

Alarm Source Info >>

Alarm Class

High

Source Name

%parent.displayName%

To Fault Text

To Offnormal Text

To Normal Text

Activation Complete Alert

Hyperlink Ord

null

Sound File

null

Alarm Icon

null

Alarm Instructions

Edit

Meta Data

Edit

[No configured facets]

Activation Mismatch Alert

Alarm Source Info >>

To open this tab from the main menu, click expand **Threat Levels**, click **Threat Level Setup** and click a chevron ( >> ) to expand a set of Alarm Source Info properties.

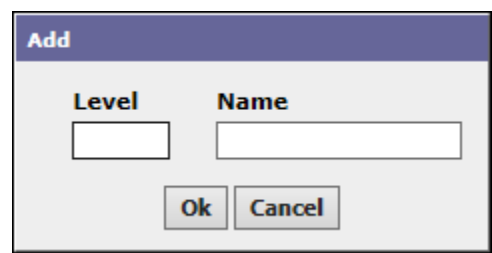
Property	Value	Description
Alarm Class	drop-down list	Specifies the alarm routing options and priority when this threat level is activated.
Source Name	text	Displays the name of the entity that generated this alarm. For threat level management, this text can identify the threat level that was activated.
To Fault Text	text	Defines the text string that appears on the Alarm Console when this threat level is activated.

Property	Value	Description
To Offnormal Text	text	Defines the text to display when the threat level transitions to an alarm state.
To Normal Text	text	Defines what to display on the Alarm Console when the threat has passed and is no longer active.
Hyperlink Ord	Ord, BQL query or file path	Defines the Ord, BQL Query or path to another location. A threat level alarm sent to the console activates the Hyperlink button. Clicking this button can transfer an operator to additional information at this location.
Sound File	file path	Defines the path to a sound file that executes when the threat level is activated. In Wb Web Profile mode (non Hx mode) you can browse to the file to use, and click an arrow icon to the right of the folder icon to test the path that you entered.
Alarm Icon	file path	Defines the location of a graphic file to add to the timestamp column of the alarm table in the Console Recipient view.
Alarm Instructions	Edit button	Provides end-user instructions when this threat level is activated. Click the Edit button to open the Edit window for working with alarm instructions.
Meta Data	text	Provides additional information about the source of the threat.


Add (or edit) threat level window

This window adds new threat levels and edits existing threat levels.

**Figure 278.** Add threat level window



You access this window from the main menu by clicking **System setup > Threat Levels > Threat Level Setup**,

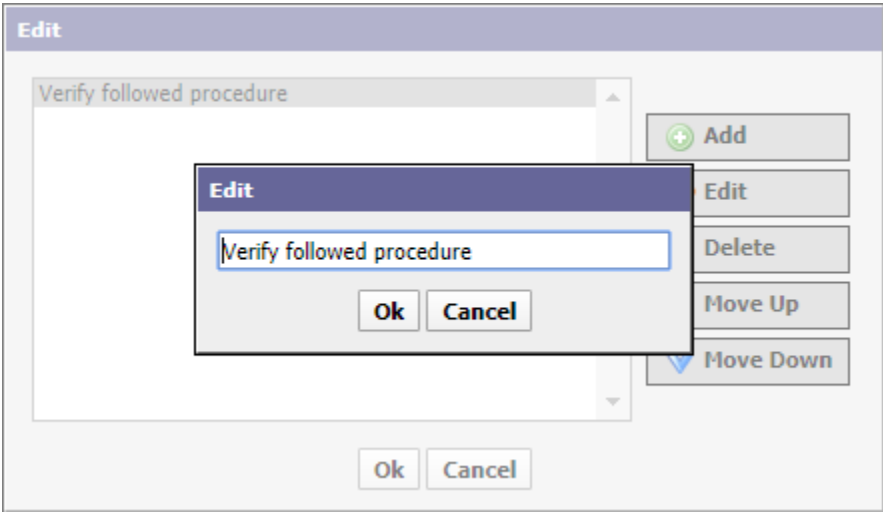
and clicking the add button ().

Property	Value	Description
Level	number (0-255) (defaults to 0 = Low, 5 = Normal, and 10 = High)	Defines a number to indicate the seriousness of the threat condition. You decide
Name	text	Assigns a descriptive name to the level.

Edit instructions window

This window edits threat level instructions.

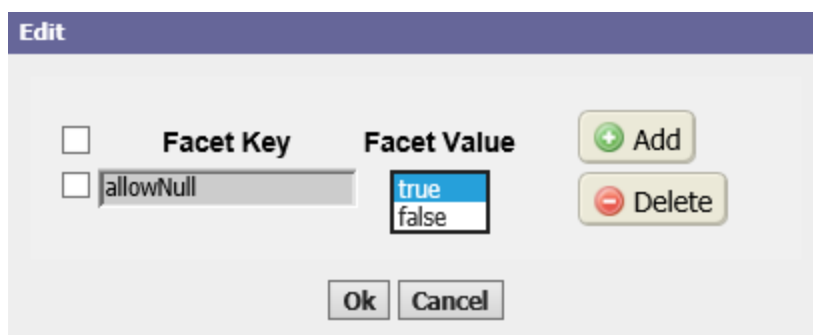
Figure 279. Edit alarm instructions windows



To access this window from the main menu, click **Threat Levels > Threat Level Setup**, expand an activation alert and click the **Edit** button next to **Alarm Instructions**.

Edit metadata windows

These windows add a **Facet Key**, which is another name for metadata associated with the threat level. Metadata provide additional information associated with the threat level alert.

**Figure 280.** Edit alarm metadata window

The image shows a software window titled "Edit" with a purple header bar. Inside the window, there is a table with two columns: "Facet Key" and "Facet Value". The "Facet Key" column has a checkbox and a text input field containing "allowNull". The "Facet Value" column has a dropdown menu with "true" selected and "false" as an option. To the right of the table are two buttons: "Add" (with a green plus icon) and "Delete" (with a red minus icon). At the bottom of the window are "Ok" and "Cancel" buttons.

<input type="checkbox"/>	Facet Key	Facet Value
<input type="checkbox"/>	allowNull	true false

Buttons: Add, Delete, Ok, Cancel

You access these windows from the main menu by clicking **System Setup > Threat Levels > Threat Level Setup**, expanding an activation alert or alarm and clicking the **Edit** button to the right of the **Meta Data** property.



# Chapter 14. LDAP network driver views, tabs and windows

The tabs, views and windows that manage the interface between your system and an LDAP server function like the device management tabs, views and windows.

Included are these features:

- Attribute discovery
- Attribute mapping to system properties
- The ability to ping the LDAP server
- Import from the LDAP server

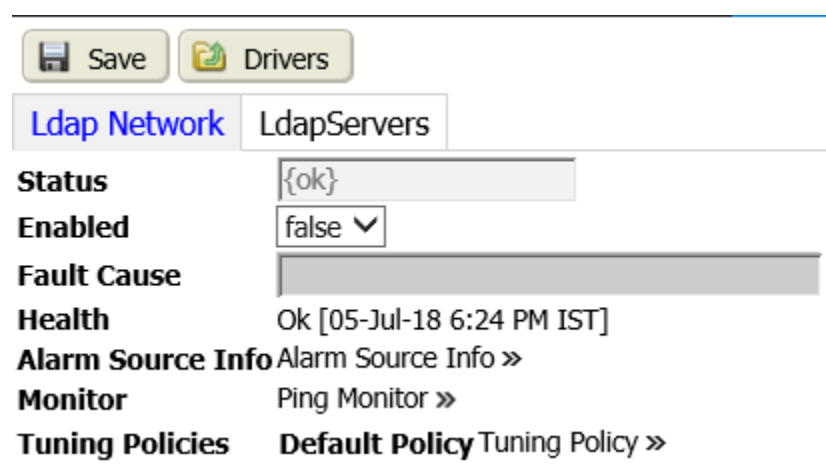
A standard network driver added to the Remote Drivers view provides these LDAP functions.

## LDAP Network view

This tab shows standard properties for the LDAP Network driver.

### LDAP Network tab

**Figure 281.** Ldap Network view with Ldap Network tab



To access this tab, navigate to **Controller (System) Setup > Remote Devices > Remote Drivers** and double-click your LDAP network device driver row in the Remote Drivers view.

The view title, Ldap Network in this example (this name may be different in your system), displays in the top left corner above the **Save** and **Drivers** links.

This tab turns the LDAP network on and off and reports network status. In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support the Ldap Network.

Property	Value	Description
Ping Monitor	additional properties	Links to a set of properties for configuring the ping monitor (the mechanism for confirming the health of devices on the network).  Refer to <a href="#">Ping Monitor</a> .
Tuning Policies	additional properties	Links to a set of properties for configuring network tuning policies (rules for write and read requests from polling).  Refer to <a href="#">Tuning Policy</a> .

Ping Monitor

Figure 282. Ping Monitor properties

Monitor

Ping Monitor

Ping Enabled

true

Ping Frequency

+ 00000 h 05 m 00 s

Alarm On Failure

true

Startup Alarm Delay

+ 00000 h 05 m 00 s

Num Retries Until Ping Fail

0 [0 - 2147483648]

Property	Value	Description
Ping Enabled	true (default) or false	Turns the use of the ping monitor on and off.
Ping Frequency	hours minutes seconds	Defines how frequently the system pings the server.
Alarm On Failure	true (default) or false	Controls whether or not the system issues an alarm when a ping fails.
Startup Alarm Delay	hours minutes seconds	Defines a waiting period before the system issues an alarm when the ping fails.
Num Retries Until Ping Fail	number	Defines the number of retries until ping is successful.

Tuning Policy

A network’s tuning policy defines rules for when to write to a writeable proxy point, and how to determine the freshness of a read request from polling.



Figure 283. LDAP Network Tuning Policy properties

Tuning Policies

Default Policy

Tuning Policy ⌵

Min Write Time

00000

h

00

m

00

s

[0 ms - +inf]

Max Write Time

00000

h

00

m

00

s

[0 ms - +inf]

Write On Start

true ▾

Write On Up

true ▾

Write On Enabled

true ▾

Stale Time

00000

h

00

m

00

s

[0 ms - +inf]

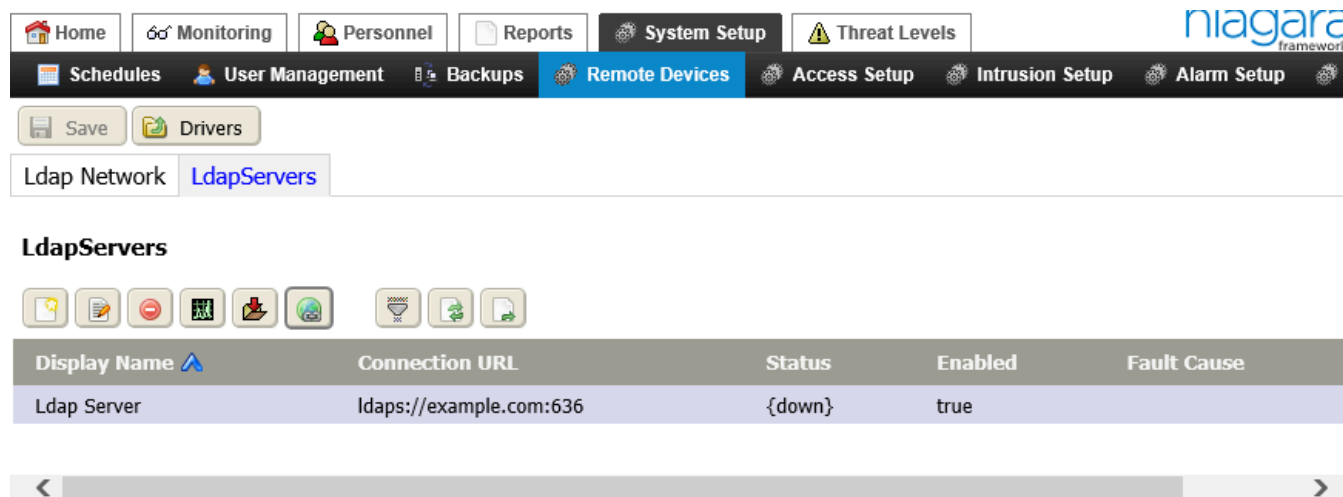
Property	Value	Description
Min Write Time	hours minutes seconds, zero (default) to infinity	<p>Specifies the minimum amount of time allowed between writes to writable proxy points, especially ones that have one or more linked inputs. This provides a way to throttle rapidly changing values so that only the last value is written.</p> <p>The default value (0) disables this rule causing all value changes to attempt to write.</p>
Max Write Time	hours minutes seconds, zero (default) to infinity	<p>Specifies the maximum amount of time to wait before rewriting the value, in case nothing else has triggered a write, to writable proxy points. Any write action resets this timer.</p> <p>The default (0) disables this rule resulting in no timed rewrites.</p>
Write On Enabled	true (default) or false	<p>When its status transitions from disabled to enabled, defines a writeable proxy point's behavior.</p> <p>true initiates a write when the transition occurs.</p> <p>false prevents a write when the transition occurs.</p>
Write On Start	true (default) or false	At station startup, defines a

Property	Value	Description
		<p>writeable proxy point's behavior.</p> <p><code>true</code> initiates a write when the station first reaches a steady state.</p> <p><code>false</code> prevents a write when the station first reaches a steady state.</p>
Write On Up	<code>true (default) or false</code>	<p>When the point and its parent device transition from down to up, defines a writeable proxy point's behavior.</p> <p><code>true</code> initiates a write when the transition occurs.</p> <p><code>false</code> prevents a write when the transition occurs.</p>
Stale Time	hours minutes seconds; defaults to 0 (zero)	<p>Defines the period of time without a successful read (indicated by a read status of {ok}) after which a point's value is considered to be too old to be meaningful (stale).</p> <p>A non-zero value causes the point to become stale (status stale) if the configured time elapses without a successful read, indicated by Read Status {ok}.</p> <p>The default value (zero) disables the stale timer causing points to become stale immediately when unsubscribed.</p>

Ldap Servers tab

This tab lists one or more Ldap server.




Figure 284. LdapServers tab



To access this tab, click **System Setup** > **Remote Devices** > **Remote Drivers**, double-click your LDAP network device driver row in the Remote Drivers view, and click the LdapServers tab.

Control buttons

In addition to standard control buttons (Edit, Delete, Hyperlink, Filter, Refresh and Export), these buttons specifically apply to LDAP:

-  New opens a window with properties to configure the connection between your system and an LDAP server.
-  Ping sends a command to the LDAP server to verify the connection.
-  Force Import from LDAP server opens the Import Preferences window. You use this window to create a new database of personnel records or to completely replace an existing personnel database. A forced import deletes all existing records in the database.

**WARNING:** Do not click this button unless you intend to start from scratch.

Columns

Table 65. LDAP server view columns

Column	Description
Display Name	Reports the name that describes the event or function.
Connection URL	Reports the LDAP server's domain address.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Enabled	Reports if the function is turned on ( <code>true</code> ) or off ( <code>false</code> ).
Fault Cause	Indicates the reason for a fault.

New (and Edit) LDAP server window

This window contains the properties associated with each LDAP server. You use this window when you are setting up your system personnel database for the first time.

Figure 285. New LDAP server window

New

Display Name

LdapServer

Status

{ok}

Connection Host

localhost

Connection Port

10389

Enable TLS

false

Connection User

uid=admin,ou=system

Connection Password

.....

Enable Connection Pooling

true

Initial Size

0

Max Size

10

Pref Size

0

Connection Timeout (in milli seconds)

0

Search Scope

Object Scope

Polling Interval

+ 00000

h 05


m 00


.000

s

Ok

Cancel

You access this window when you click the New button () on the LdapServers tab. You access this view by clicking **System Setup > Remote Devices > Remote Drivers**, followed by double-clicking the LdapNetwork driver row in the table and clicking the LdapServers tab.

To edit the properties for an existing server, you select the server row on the LdapServers tab and click the Edit button ()

Property	Value	Description
Display Name	text	Creates an object name for display purposes, which may differ from the actual object name.
Status	read-only	Reports the condition of the entity or process at last polling.

Property	Value	Description
		<p>{ok} indicates that the component is licensed and polling successfully.</p> <p>{down} indicates that the last check was unsuccessful, perhaps because of an incorrect property, or possibly loss of network connection.</p> <p>{disabled} indicates that the <b>Enable</b> property is set to <code>false</code>.</p> <p>{fault} indicates another problem. Refer to <b>Fault Cause</b> for more information.</p>
Connection Host (LDAP)	URL or IP Address	Defines the URL or IP address of the platform on which the Ldap Server is running. The location may be on the same computer or elsewhere available on an intranet or the Internet.
Connection Port (LDAP)	number	Defines the port over which the computer communicates with the server.
Enable Connection TLS (LDAP)	<code>true</code> or <code>false</code> (default)	Selects secure transmission and identity verification using the TLS protocol. Do not change this value unless you are confident of what you are doing. Changing this value could open the system to hackers.
Connection User (LDAP)	name	<p>Defines the LDAP server attributes for the system administrator.</p> <p>uid=admin is an example of the distinguished name for this user.</p> <p>dc=com is the user parent class.</p>
Connection Password (LDAP)	password	Defines the password for the user specified in property <b>Connection User</b> . When used, requires a valid password in the LDAP server. The system uses

Property	Value	Description
		this password to connect to the server for authentication.
Enable Connection Pooling (LDAP)	true (default) or false	Enables (true) and disables (false) the use of a connection pool. To speed processing, LDAP servers maintain a pool of connections. A request from the system that uses an existing connection saves valuable processing time, which improves system performance. Do not change the default (true = enabled) setting unless you know what you are doing.
Initial Size (LDAP)	number (defaults to 0)	Defines the number of pooling connections.
Max Size	number (defaults to 10)	Defines the maximum number of connections to the LDAP server that the system supports concurrently.
Pref Size	number (defaults to 0)	Defines the preferred number of connections to the LDAP server that the system supports concurrently.
Connection Timeout (general)	number of milliseconds	Determines how long a station attempts to connect to a server before the attempt fails. This time should not be too short to cause false connection failures, and not so long as to cause excessive delays when a server is down.
Search Scope	drop-down list	Defines how much of the User Search Base to actually search.
Polling Interval	plus or minus hours minutes and seconds	Defines how frequently to poll the LDAP server.

### Import Preferences window

This window configures how to import data from the LDAP server. You use this window when you are setting up your system personnel database for the first time, or, if you would like to discard the records in the database and start again from scratch. This window initiates a "forced import." By its nature, a forced import deletes all existing personnel records that correspond to the particular LDAP server and retrieves the entire data set again.

**Figure 286.** Import Preferences window

Import Preferences

The following configurations are used for Ldap Import..

User SearchBase

User SearchFilter

(objectclass=\*)

Search Scope

Object Scope

Group Attribute

Allow New InactiveUsers

true


Status Attribute

Active Status Values (Comma Seperated)

Ok

Cancel

This window opens when you click **System Setup > Remote Devices > Remote Drivers**, followed by double-clicking the LdapNetwork driver row in the table.

Another way to open this window is to click the **Import** button on the Ldap Server view. You access this view by clicking **System Setup > Remote Devices > Remote Drivers**, followed by double-clicking the LdapNetwork driver row in the table, clicking the Ldap Servers tab, selecting the server, and clicking the Force Import from LDAP Server button (  ).

Property	Value	Description
User SearchBase	text	Defines where to start searching for personnel in the LDAP server hierarchy.  ou stands for organizational unit.  dc stands for domain controller.  dn stands for distinguished name. This name both uniquely identifies an entry in the LDAP database and describes its position in the hierarchy.
User SearchFilters	text	For personnel, defines the objectClass (metadata) associated with each record that identifies it as a personnel record versus a system or other record type in the server database.

Property	Value	Description
Search Scope	drop-down list	Defines how much of the User Search Base to actually search.
Group Attribute	text	Defines the LDAP server group attribute that provides the LDAP group Distinguished Name. Each LDAP user belongs to a group. Specify the group attribute. Specify the attribute that holds the group and associated with an access right in the ldap server.
Allow New Inactive Users	true (default) or false	Indicates that users may be added before they are activated in the system.
Status Attribute	read-only	Reports LDAP user status: active or inactive. Inactive status could possibly be marked for deletion from the database. For example, it could be a person that no longer works at the owning company.
Active Status Values (Comma Separated)	text values, comma separated	Defines a list of values, which indicate a valid user status. This list is specific to your organization's personnel policies.

## Ldap Server view

This view and tab configures LDAP server properties.



Properties

Figure 287. Ldap Server view and tab

HomeMonitoringPersonnelReportsSystem Setup

SchedulesUser ManagementBackupsRemote DevicesAcc

SavePingImportLdap Network

Ldap ServerAttributesGroups

Status

{down}

Enabled

true

Fault Cause

Health

Fail [25-Jul-18 1:11 PM EDT] example.com:636

Alarm Source Info

Alarm Source Info »

Ldap Connection

Ldap Connection »

Vendor Name

Vendor Version

Supported L D A P Version

3

User Search Base

»

User Search Filter

(objectclass=\*)»

Search Scope

Object Scope

Polling Interval

00 d 00 h 05 m 00 s [5mins - +inf]


Periodic purge schedule

2:00 AM {Sun Mon Tue Wed Thu Fri Sat}

LdapImportConfig

Ldap Import Config »

To access this view, click **System Setup > Remote Devices > Remote Drivers**, double-click your LDAP network device driver row row in the Remote Drivers view, click the LdapServers tab, and double-click the server row in

the table or select the server row and click the Hyperlink button (  ).

The view title, LdapServer in this example (this name may be different in your system), displays in the top left corner above the buttons and link.

- **Save** updates the server record in the database.
- **Ping** initiates communication with the server to verify the connection.
- **Import** opens the Import Preferences window.
- **LdapNetwork** returns the focus to the LdapNetwork view.

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support the Ldap server.

Property	Value	Description
Ldap Connection	additional properties	Refer to <a href="#">LDAP Connection</a>

Property	Value	Description
		<a href="#">properties</a> .
Vendor Name	read-only	Identifies the name of the LDAP server vendor.
Vendor Version	read-only	Reports the software version of the LDAP server.
Supported L D A P Version	read-only	Reports the supported version number.
User SearchBase	text	<p>Defines where to start searching for personnel in the LDAP server hierarchy.</p> <p>ou stands for organizational unit.</p> <p>dc stands for domain controller.</p> <p>dn stands for distinguished name. This name both uniquely identifies an entry in the LDAP database and describes its position in the hierarchy.</p>
User SearchFilter	text	<p>Defines where to start searching for personnel in the LDAP server hierarchy.</p> <p>ou stands for organizational unit.</p> <p>dc stands for domain controller.</p> <p>dn stands for distinguished name. This name both uniquely identifies an entry in the LDAP database and describes its position in the hierarchy.</p>
Search Scope	drop-down list	Defines how much of the User Search Base to actually search.
Polling Interval	plus or minus hours minutes and seconds	Defines how frequently to poll the LDAP server.
Periodic purge schedule	read-only	<p>When a personnel record is deleted from the system database, it needs to be deleted from the LDAP server. The system removes deleted records from the LDAP server on a regular schedule, which is documented here. This schedule can be changed using</p>

Property	Value	Description
		Workbench.
Ldap Import Config	additional properties	Refer to <a href="#">Ldap Import Config</a> .

LDAP Connection properties

These properties configure the physical connection between the Supervisor PC and the LDAP server.

Figure 288. Ldap Connection properties

Ldap Connection

Ldap Connection

Connection Host

Connection Port

Enable TLS

Authentication Mechanism

Connection User

Connection Password

Enable Connection Pooling

Initial Size

Max Size

Pref Size

Connection Timeout (in milli seconds)

localhost

10389

false

Simple

uid=admin,ou=system

••••••••

true

0

10

0

0

You access these properties by navigating to **System Setup > Remote Devices > Remote Drivers**. Then you double-click the LDAP network driver row in the table, click the LdapServers tab, double-click the LDAP server name in the table, and expand the **Ldap Connection** property group.

Property	Value	Description
Connection Host	URL or IP Address	Defines the URL or IP address of the platform on which the Ldap Server is running. The location may be on the same computer or elsewhere available on an intranet or the Internet.
Connection Port	number	Defines the port over which the computer communicates with the server.
Enable TLS	true or false (default)	Configures secure communication between the station and network devices. By default, the system uses TLS secure communication. You

Property	Value	Description
		<p>would change this network property to <code>false</code> only if a legacy device (camera) cannot support TLS.</p> <p>If some devices on your network support TLS and others do not, you may add two networks of the same type: one for the secure devices, and the other for those that do not support security.</p>
Authentication Mechanism	drop-down list; defaults to <code>None</code>	<p>Identifies the method used to verify the identity of the LDAP server to its client, the system database.:</p> <p><code>Simple</code></p> <p><code>Cram Md5</code></p> <p><code>Digest Md5</code></p> <p>For information about these options, refer go the <i>Niagara Station Security Guide</i></p>
Connection User	<code>name</code>	<p>Defines the LDAP server attributes for the system administrator.</p> <p><code>uid=admin</code> is an example of the distinguished name for this user.</p> <p><code>dc=com</code> is the user parent class.</p>
Connection Password	<code>password</code>	<p>Defines the password for the user specified in property <code>Connection User</code>. When used, requires a valid password in the LDAP server. The system uses this password to connect to the server for authentication.</p>
Enable Connection Pooling	<code>true (default) or false</code>	<p>Enables (<code>true</code>) and disables (<code>false</code>) the use of a connection pool. To speed processing, LDAP servers maintain a pool of connections. A request from the system that uses an existing connection saves valuable processing time, which improves system performance.</p>

Property	Value	Description
		Do not change the default (true = enabled) setting unless you know what you are doing.
Initial Size	number (defaults to 0)	Defines the number of pooling connections.
Max Size	number (defaults to 10)	Defines the maximum number of connections to the LDAP server that the system supports concurrently.
Pref Size	number (defaults to 0)	Defines the preferred number of connections to the LDAP server that the system supports concurrently.

### User Search Base string chooser

#### **WARNING:**

WARNING: If, after importing records from the LDAP server, you change the search criteria (**User Search Base**, **User Search Filter** or **Search Scope**), and then purge records from the system, the purge deletes all existing personnel records in the database. If this happens, personnel will not have access to your facility.

Defines where to start searching for personnel in the LDAP server hierarchy.

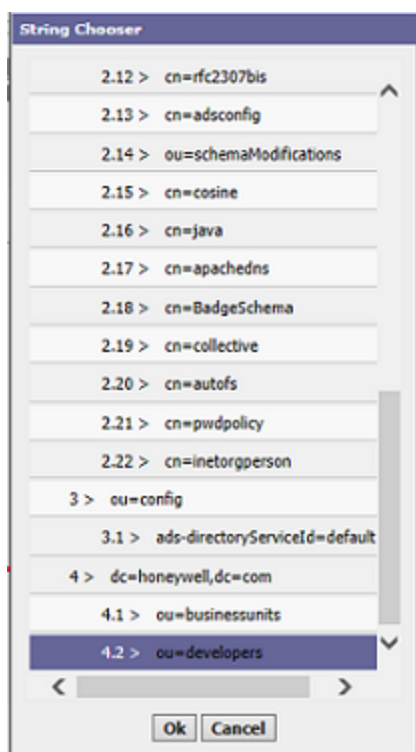
`ou` stands for organizational unit.

`dc` stands for domain controller.

`dn` stands for distinguished name. this name both uniquely identifies an entry in the LDAP database and describes its position in the hierarchy.

You would change this property to access the personnel records for a specific tenant or other group.

Rather than requiring you to type the LDAP server attribute equivalents, this window provides a list from which to choose.

**Figure 289.** User Search Base string chooser

You access this window by clicking the chevron to the right of **User Search Base** on the Ldap Server tab.

#### User Search Filter string chooser

>

**WARNING:** If, after importing records from the LDAP server, you change the search criteria (**User Search Base**, **User Search Filter** or **Search Scope**), and then purge records from the system, the purge deletes all existing personnel records in the database. If this happens, personnel will not have access to your facility.

Defines the objectClass (metadata) associated with each personnel record. This objectClass identifies the record as a personnel record versus a system or other record type in the server database.

This chooser adds metadata (text strings), which the system uses to search the LDAP server.

**Figure 290.** User Search Filter string chooser

You access these properties by clicking the chevron next to **User Search Filter** property on the Ldap Server tab.

The three control buttons (Add, Edit and Delete) perform standard functions.

#### Ldap Import Config

These properties configure the import action from the LDAP server to the station database. By default, the system imports data from the LDAP server once every hour. The maximum number of personnel records the system can import at one time is 5000. This number is not likely to be reached within the space of one hour.

Figure 291. Ldap Import properties

Ldap Import Config ⌵

LdapImportConfig

Import Frequency

Daily ⌵

Last Import Time

01 ⌵ - Jan ⌵ - 1970 05 ⌵ : 30 ⌵ AM ⌵ IST

Group Attribute

Allow New Inactive Users

true ⌵

Status Attribute

Active Status Values

Account Expiry Date Time Attribute

Property	Value	Description
Import Frequency	drop-down menu	Selects how frequently to import users: Hourly, Daily, Weekly or Instant (instantly).
Last Import Time	read-only	Displays the date and time of last successful import.
Group Attribute	text	Defines the LDAP server group attribute that provides the LDAP group Distinguished Name. Each LDAP user belongs to a group. Specify the group attribute. Specify the attribute that holds the group and associated with an access right in the ldap server.
Allow New Inactive Users	true (default) or false	Indicates that users may be added before they are activated in the system.
Status Attribute	read-only	Reports LDAP user status: active or inactive. Inactive status could possibly be marked for deletion from the database. For example, it could be a person that no longer works at the owning company.
Active Status Values (Comma Separated)	text values, comma separated	Defines a list of values, which indicate a valid user status. This list is specific to your organization's personnel policies.
Account Expiry Date Time Attribute	text	Specifies the name of the account expiry attribute in the LDAP server. Some LDAP servers configure user accounts to expire on a specific date,

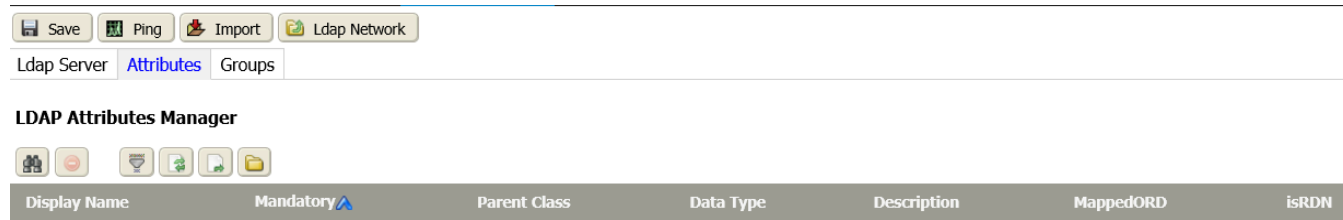


Property	Value	Description
		at a specific time. This name identifies the attribute that contains this information.
		The security system's import job ignores data from any user account that has expired.

Attributes tab

LDAP attributes map to system properties.

Figure 292. Attributes tab



You access this tab by navigating to **Controller (System) Setup > Remote Devices > Remote Drivers**, double-clicking the LdapNetwork driver row in the table, clicking the Ldap Servers tab, double-clicking the Ldap Server row, and clicking the Attributes tab.

Table 66. Database columns

Column	Description
Display Name	Reports the name that describes the event or function.
Mandatory	Indicates if this attribute is required or not.
Parent Class	Identifies the owner of this attribute.
Data Type	Identifies the type of data: Boolean, numeric, enum or string.
Description	Provides additional information.
MappedORD	Reports the parent class and system property for the attribute.
isRDN	Indicates if this property is the relative distinguished name (RDN), that is, the primary piece of information used to identify a record in the database. This is usually the uid (user ID).

Table 67. Discovered columns

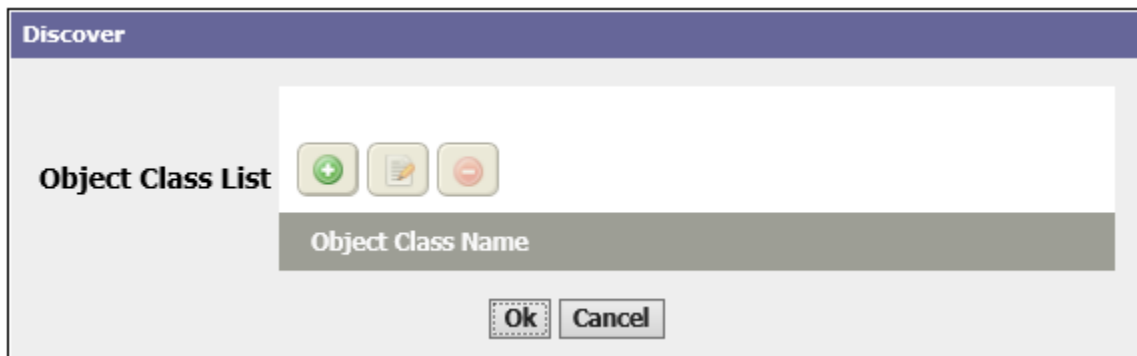
Column	Description
attrName	Reports the name of the attribute.
isMandatory	Indicates if this attribute is required or not.
parentClass	Identifies the owner of this attribute.
dataType	Identifies the type of data: Boolean, numeric, enum or string.
description	Provides additional information.

Discover attributes window

This window defines the object classes used to filter the search of LDAP database records.

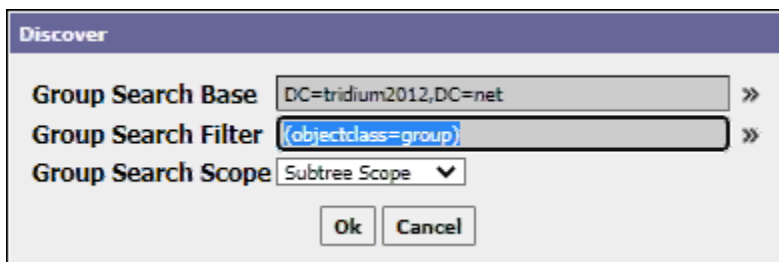
You access this window when you click the **Import** button on the Ldap Server or Attributes tabs.

**Figure 293.** Discover attributes window with two object classes



This window opens when you click the Discover button under LDAP Attributes Manager.




Discover window opens.



Fill in the Discover criteria and click OK:

- **Group Search Base:** Click >> to open **String Chooser** and select the group search base as `DC=tridium2012,DC=net`. This refers to the parent class.
- **Group Search Filter:** Click >> to open **String Chooser** and select group search filter as `group`. This will search all the groups in the parent class. can add, edit, or delete group search filter in the **String Chooser**.
- **Group Search Scope:** Select **Subtree Scope** as group search scope from the drop-down list. This will search up to all the child nodes for the selected **Group Search Base** and **Group Search Filter**.

Control buttons:



-  Add opens a view or window for creating a new record in the database.
-  Edit opens the Edit window.
-  Delete removes the selected record (row) from the database table. This button is available when you select an item.

The list may contain multiple object classes for discovery.

Property	Value	Description
Object Class List/Object Class Name	text	Defines the piece of information that identifies to which group each attribute record belongs. For example, an <code>Object Class Name</code> of "badge" identifies an attribute as a piece of badge information, such as facility code, Wiegand format, etc. An object class of "person" identifies attributes associated with employees, such as last name, first name, person ID, etc.

LDAP Attributes Manager pane

In addition to the standard control buttons (Delete, Filter, Refresh, and Learn Mode), these buttons in the Database pane apply specifically to LDAP configuration:


-  Discover identifies the LDAP attributes that are available to be assigned to system properties.
-  Back and forward arrow icons in the center of the view, equal with the Discovered title, page through multiple discovered results, go to a specific page, and control the number of items that appear on each page.

The


Table 68. LDAP Attributes Manager columns

Column	Description
Display Name	Identifies the attribute.
Mandatory	Indicates if the property is required by the LDAP server.
Parent Class	Identifies the parent class in the LDAP server hierarchy.
Data Type	Identifies the type of data: String, Boolean, etc.
Description	Reports the text entered for Description when the attribute was mapped.
MappedORD	Defines the parent class and property to which the attribute is mapped in the system.
isRDN	Indicates if this property is the relative distinguished name (RDN), that is, the primary piece of information used to identify a record in the database. This is usually the uid (user ID).

Discovered pane

To view the Discovered pane, click the Discover control button (.

In addition to the standard control buttons (Filter and Export), these buttons apply specifically to LDAP configuration:

-  Add moves the selected discovered attribute from the Discovered pane to the LDAP Attributes Manager pane.



- Match associates the selected attribute in the LDAP Attributes Manager pane with its discovered and selected LDAP equivalent in the Discovered pane.

Table 69. LDAP Discovered columns

Column	Description
attrName	Identifies the attribute in the LDAP server.
isMandatory	Indicates if the property is required by the LDAP server.
parentClass	Identifies the parent class in the LDAP server hierarchy.
dataType	Identifies the type of data: String, Boolean, etc.
description	Reports the text entered for Description when the attribute was mapped.
AttributeExists	Attribute exists defaults to false.

Add attribute window

This window adds a discovered LDAP attribute to the station database. Discovering the attribute requires an LDAP connection. Discovering the attribute and adding it into database will open this window.

Figure 294. Add Attribute window

Add

Device Type

Ldap Attribute

Display Name

cn

Data Type

String

Mapped O R D

Person

Last Modified



Is R D N

false

Ok

Cancel

This window opens when you expand **System Setup > Remote Devices** and click **Remote Drivers**; double-click the LdapNetwork driver row in the table; click the Ldap Server tab; double-click the Ldap Server row; click the

Attributes tab; click the Discover button (  ); and click the Add button (  ) in the Discovered pane.

Property	Value	Description
Device Type	read-only	Identifies the data as an LDAP attribute.
Display Name	read-only	Indicates the attribute name in the LDAP server.
Data Type	drop-down list	Defines the type of attribute data:


Property	Value	Description
		<div>String identifies the attribute as text.</div> <div>Binary identifies the attribute as a Boolean value.</div>
Mapped O R D first drop-down list	drop-down list	Identifies the parent class of the attribute name. This is a group to which the selected information belongs.
Mapped O R D second drop-down list	drop-down list	Identifies the system property to associate with the selected LDAP attribute.
Is R D N	true or false (default)	Indicates if this attribute/property combination serves as the relative distinguished name (RDN) for the person. Only one attribute/property combination can serve this function. It is usually a number, such as, employeeNumber.

Groups tab

This tab maps groups to system access rights.

Figure 295. Groups tab



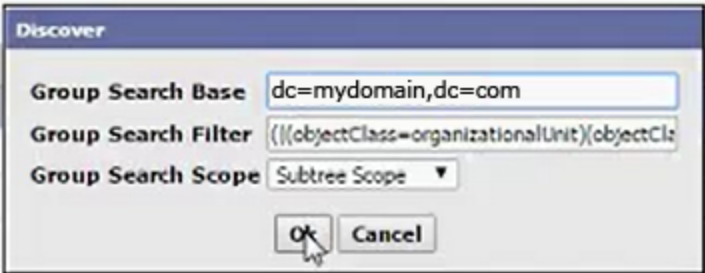
You access this tab by navigating to **Controller (System) Setup > Remote Devices > Remote Drivers**, double-clicking the LdapNetwork driver row in the table, clicking the Ldap Server tab, double-clicking the Ldap Server row, and clicking the Groups tab. To view the Discovered pane, click the discover control button (  ).


Discover groups window

Groups in the LDAP server equate to access rights in the system.

You access this view when you click the Groups tab in the Ldap Server view.

Figure 296. Discover groups window



This window opens when you click the Discover button () on the Ldap Server Groups tab.

Property	Value	Description
Group Search Base	text	Defines from which node in the LDAP server to begin searching for groups (access rights).
Group Search Filter	domain components	For group records, defines the objectClass (metadata) associated with each record that identifies it as a group record versus a system or other record type in the server database.
Group Search Scope	drop-down list	Defines how much of the LDAP server to search.  Object Scope  One Level Scope  Subtree Scope extends the scope to the child nodes of the node defined in the Group Search Base expression.

LDAP Group Manager pane

In addition to the standard control buttons (Delete, Filter, Refresh, and Learn Mode), these buttons serve LDAP functions.


-  Discover identifies the LDAP groups that are available for to be assigned to system access rights.

Table 70. LDAP Group Manager columns

Column	Description
GroupName	Identifies the system name for this group.

Column	Description
AccessRight	Identifies the system name for the assigned set of access rights.

Discovered Pane

In addition to the standard control buttons (Filter and Export), these buttons apply specifically to LDAP configuration:



-  Add moves the selected discovered group from the Discovered pane to the LDAP Group Manager pane.
-  Match associates the selected access right in the LDAP Group Manager pane with a discovered and selected LDAP group in the Discovered pane.


Table 71. LDAP group Discovered columns

Column	Description
distinguishedName	Identifies the attribute in the LDAP server.
cn	Indicates if the property is required by the LDAP server.
GroupExists	Group exists defaults to false.

LDAP Audit History view

This view provides an audit trail of actions taken to synchronize records from the LDAP server with their counterparts in the Supervisor station database.

Figure 297. LDAP Audit History view

access Access History Alarm History Intrusion History Attendance History Audit History Log History Hardware Reports LDAP Audit History Miscellaneous Reports							
							
Timestamp	Ldap Server Ord	Activity	Owner	Activity Id	Status	Details	
06-Jul-18 12:35 PM IST	slot:/Drivers/Ldap\$20Network/Ldap\$20Server	Import Personnel	admin	0	ERROR	Error during import process	
06-Jul-18 12:35 PM IST	slot:/Drivers/Ldap\$20Network/Ldap\$20Server	Import Personnel	admin	0	ERROR	No mapping details available.Import cannot proceed	
06-Jul-18 12:35 PM IST	slot:/Drivers/Ldap\$20Network/Ldap\$20Server	Import Personnel	admin	0	ERROR	Error during import process	
06-Jul-18 12:35 PM IST	slot:/Drivers/Ldap\$20Network/Ldap\$20Server	Import Personnel	admin	0	ERROR	No mapping details available.Import cannot proceed	
06-Jul-18 10:54 AM IST	slot:/Drivers/Ldap\$20Network/Ldap\$20Server	Cleanup Personnel	Personnel cleanup process	0	ERROR	0 users got deleted by cleanup process.	
06-Jul-18 10:54 AM IST	slot:/Drivers/Ldap\$20Network/Ldap\$20Server1	Cleanup Personnel	Personnel cleanup process	0	ERROR	0 users got deleted by cleanup process.	

You access this report by clicking **Reports > LDAP Audit History**.

In addition to the standard control buttons (Summary, Auto Refresh, Column Chooser, Filter, Refresh, Manager

Reports and Export, the Purge Config button () opens the Purge Config window.

Table 72. LDAP Audit History columns

Column	Description
Timestamp	Identifies when the activity occurred.
Ldap Server Ord	Identifies the location of the LDAP server.
Activity	Provides a quick summary of the task.
Owner	Identifies the person who performed the action.

Column	Description
Activity Id	Identifies the job.
Status	Indicates the success or lack thereof of the activity: SUCCESS, WARNING, ERROR.
Details	Provides an error message; indicates any action taken; identifies the LDAP mode, and provides additional data.

Periodic Purge Schedule

These properties are only available in Workbench.

Figure 298. Periodic Purge Schedule properties

▼

Periodic purge schedule

2:00 AM {Sun Mon Tue Wed Thu Fri Sat}

Trigger Mode

Daily

Time Of Day

02:00:00 AM EDT

Randomization

+000000h 00m 00s

Days Of Week

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Last Trigger

06-Sep-2018 02:00 AM EDT

Next Trigger

07-Sep-2018 02:00 AM EDT

You access these properties on the Ldap Server property sheet in Workbench by clicking **Config > Drivers > Ldap Network** in the Nav tree, double-clicking the **LdapServer** node, followed by expanding the **Periodic Purge Schedule** property.

Property	Value	Description
Trigger Mode	additional properties	Refer to <a href="#">Trigger Mode properties</a>
Last Trigger	date and time (defaults to null)	Indicates when the last job ran.
Next Trigger	date and time	Indicates the next time the job will run.

Trigger Mode properties

These properties configure the clean-up job.

Property	Value	Description
Time of Day	time	Defines when to run the job.
Randomization	hours minutes seconds	Defines an amount of time between jobs.
Days of the Week	check boxes	Configures when to run the job.

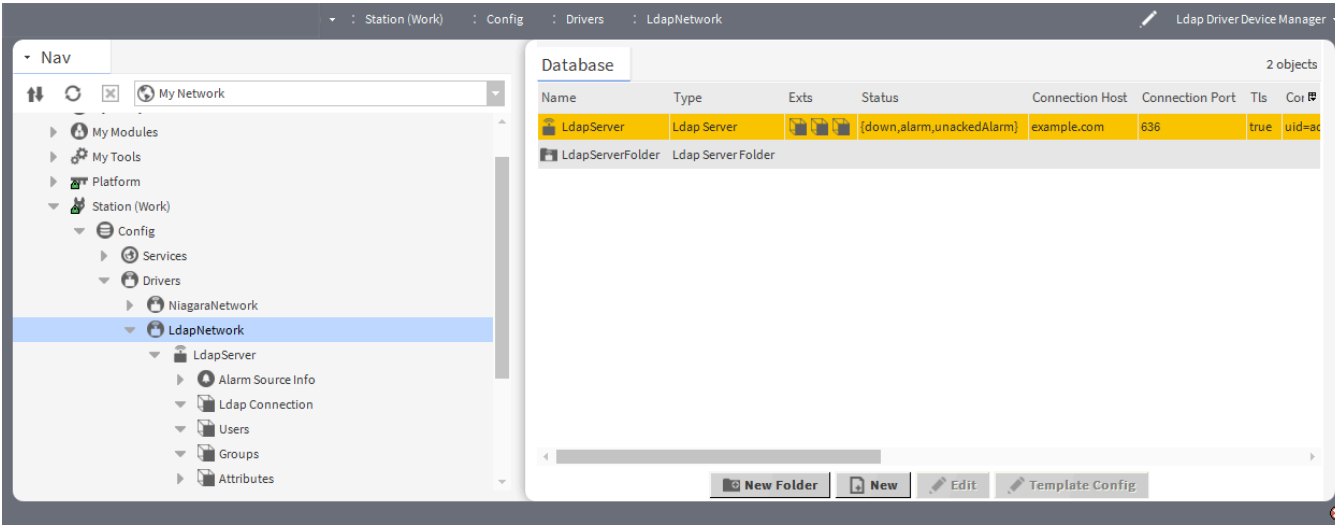
Ldap Driver Device Manager

This view adds and displays device records. It is available on the **Driver** container.



Columns

Figure 299. Ldap Driver Device Manager



To open this view, expand **Config > Drivers** and double-click the **LdapNetwork**.

Column	Description
Name	Reports the name of the station.
Type	Reports the type of station.
Status	Indicates the current state of the remote station.
Exts	Provides access to a single extension that opens the view.
Connection Host	Reports the URL to the LDAP server. The location may be on the same computer or elsewhere available on an intranet or the Internet.
Connection Port	Reports the port over which the computer communicates with the server.
Tls	Indicates if TLS secure communication is on (true) or off (false).
Connection User	Reports the LDAP server attributes for the system administrator.  uid=admin is an example of the distinguished name for this user.  dc=com is the user parent class.
Connection Password	Displays the LDAP password used to connect to the server.
Enable Connection Pooling	Enables and disables the use of a connection pool. To speed processing, LDAP servers maintain a pool of connections. A request from the system that uses an existing connection saves valuable processing time, which improves system performance. Do not change the default (true = enabled) setting unless you know what you are doing.
Initial Size	Reports the number of pooling connections.
Max Size	Reports the maximum number of connections to the LDAP server that the system supports concurrently.
Pref Size	Defines the preferred number of connections to the LDAP server that the system supports concurrently.
Connection Pool Timeout	Determines the length of time the station attempts to connect to the LDAP server before the connection fails.  The station will not fail over to the next LDAP server until the first connection attempt is unresponsive for the amount of time specified in the connection timeout. This time should be not

Column	Description
	too short to cause false connection failures, but not so long as to cause excessive delays when a server is down.
Search Scope	Reports the User Search Base to actually search.
Polling interval	Reports how frequently to poll the LDAP server.

## Buttons

- **New Folder** creates a new folder for devices. Each such folder provides its own set of manager views.
- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.
- **Template Config** accesses the station template that defines configuration options. You would select a template to set up the device with pre-configured properties.

# Chapter 15. Nrio Driver views, tabs and windows

This driver provides an interface between a remote controller station and the hardware modules connected to the station, as well as to other remote I/O modules. This driver is not available on a Supervisor PC. With this driver you can incorporate standard building automation features, such as temperature and energy management in your system.

























A low-level daemon communicates to the I/O processors on the hardware. An Nrio device uses RS-485 connections, which allow a single controller to run multiple NrioNetworks, each with its own COM port.

For more information about this driver and how to configure the devices it supports, refer to the *NRIO Driver Guide*. While this guide documents the Workbench interface, the same properties are available using the web UI.

## Nrio Device Manager view

The Nrio Network views tabs and windows manage creating updating and deleting remote module records. The Nrio Device Manager view lists device level NrioModule components.

**Figure 300.** Nrio Device Manager view










Display Name	Enabled	Status	Device Type	Uid	Installed Version	Available Version
Nrio16 Module	true	{fault}	Io16	000000000000		2.2

To access this view from the main menu, click **Controller Setup > Remote Devices > Remote Drivers**, and double-click the Nrio Network row in the Remote Drivers view.

### Control buttons

In addition to the standard control buttons, (Hyperlink, Delete, Rename, Delete, Filter, Refresh, and Exit), this view includes these control buttons:

-  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 point values as well as properties provided by the database.
-  Manage Devices/Drivers opens the Manage Drivers or Manage Devices window, which is used to Add, Delete, Rename, Duplicate, Copy, and Cut system drivers or devices.
-  Wink Device cycles the first digital output (relay output) for all selected devices on and off for a period of 10 seconds. This confirms that the device is responding before matching it to a specific component in the station database (typically, after you have added offline hardware are using the match function

-  Upgrade Firmware initiates an upgrade of a selected module.
-  Upload reads recursive, transient and persistent data from the device and writes it to the station database. After discovering and adding a new module, clicking this button populates current data in the device's components.
-  Download writes persistent data to the device from values in the station database. You use this button to restore known good values as previously saved in the station.
-  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.).

Database columns

Table 73. Nrio Device Manager database columns

Column	Description
Display Name, Name	Reports the name that describes the event or function.
Enabled	Reports if the function is turned on ( <code>true</code> ) or off ( <code>false</code> ).
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}.
Device Type	Reports the type of module.
Uid	Universal ID
Installed Version	Indicates which version of the driver is installed.
Available Version	Indicates an available version.

Discovered pane


This pane opens when you click the Discover control button ().

Table 74. Nrio Device Manager Discovered columns

Column	Description
Address	Identifies the location of the discovered module.
Device Type	Reports the type of module found.
Used By	After matching the discovered Access Network with the existing database Access Network, this column is updated with the existing access network display name.
Version	Indicates which version of the driver is installed on the found module.

Nrio Module view

This view updates Nrio properties and configures points.

Figure 301. Nrio module view

Save

Point Manager

Clear Totals

Go to Module

Nrio Network

Nrio16 Module

Status

{disabled,fault}

Enabled

false

Fault Cause

Invalid UID: Do Discover and Match.

Health

Fail [null]

Alarm Source Info

Alarm Source Info

Alarm Class

Medium

Source Name

%parent.parent.displayName% %parent.dis

To Fault Text

To Offnormal Text

%lexicon(driver:pingFail)%

To Normal Text

%lexicon(driver:pingSuccess)%

Alarm Source Info

Hyperlink Ord

Sound File

null

Alarm Icon

null

Alarm Instructions

Edit

Meta Data

Edit

[No configured facets]

Address

0

[0 - 16]

Nrio16 Status

Nrio16 Status

Io Status

Io Status

Active Ai Map

0

Value A I1

0

Value A I2

0

Value A I3

0

Value A I4

0

Value A I5

0

Value A I6

0

Value A I7

0

Value A I8

0

Active Di Map

0

Value High Speed D Is

0

Count High Speed D I1

0

Count High Speed D I2

0

Count High Speed D I3

0

Count High Speed D I4


0

To access this view from the main menu, click **Controller Setup > Remote Devices > Remote Drivers**, double-click the Nrio Network row in the Remote Drivers view, and double-click a module row or select the row and

click the Hyperlink button ().

Links

The row of buttons along the top of this view provide these functions:

- **Point Manager** opens the Nrio Point Manager view.
- **Clear Totals** resets the accumulated total value for all **CounterInputPoints** to zero (0), which is equivalent to invoking the `Reset` command on each point's proxy extension (ProxyExt).
- **Go To Module** opens the **Go to Module** window for navigating to another Nrio module under the controller's Nrio Network. The system populates this window only when there are two or more Nrio modules on the network.
- The **Nrio Network** button () returns up one level to the Nrio Network view.

Properties

In addition to the standard properties (**Status**, **Fault Cause**, and **Enabled**, **Health** and **Alarm Source Info**, these properties specifically support the Nrio Module view.

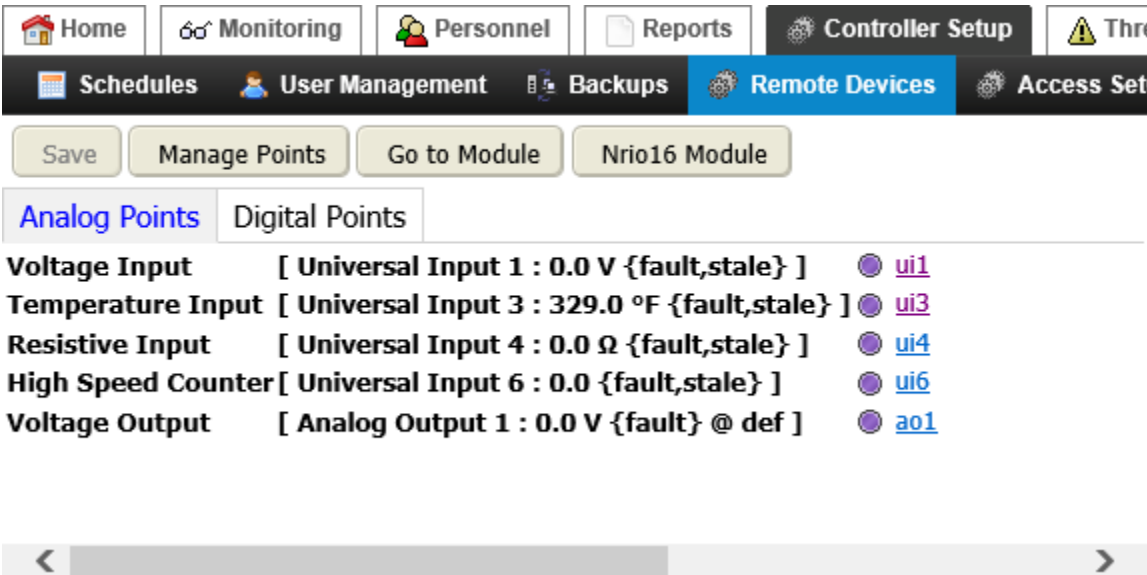
Property	Value	Description
Address	read-only	Displays an integer between 1 and 16, which is unique among all Nrio modules under the Nrio network. The system automatically derives this number and associates it with the physical I/O devices upon an online discover.
Io Status	read-only	Indicates the value (in hexadecimal) last received by the actrlid (access control daemon) process running on the controller.  These values are for advanced debug purposes only.

Nrio Point Manager, Analog Points tab

This view displays tabs that hold analog or digital points, which you can add using the **Manage Points** window.

Links

Figure 302. NRIO Point Manager view



To access this view from the main menu, click **Controller Setup > Remote Devices > Remote Drivers**, double-click the Nrio Network row in the Remote Drivers view, double-click a module row and click the **Point Manager** link.

In addition to **Save**, these links support the point manager:

- **Manage Points** opens the **Manage Nrio Points** windows, which add, rename, delete, cut, copy, and paste analog and digital point information.
- **Go To Module** opens the **Go to Module** window for navigating to another set of Nrio module points. The system populates this window only when there are two or more Nrio modules on the network.
- **Nrio 16 Module** (in the screen capture) opens the current module view. The name on this button changes depending on the name of the module.

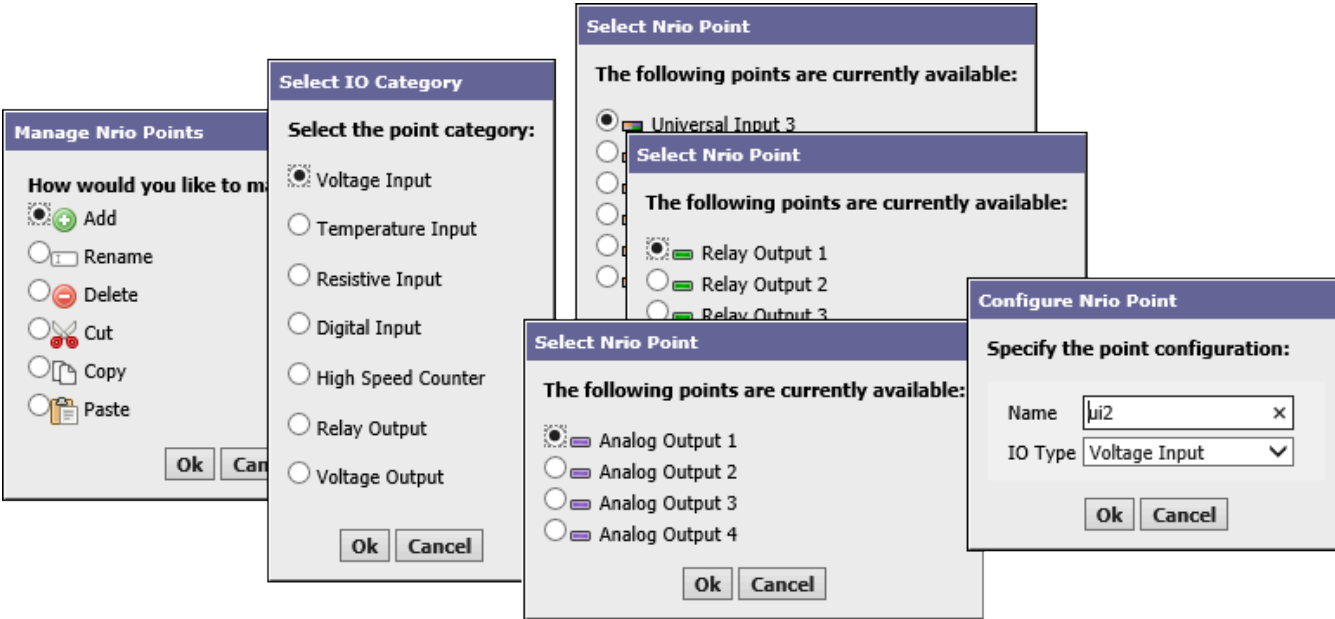
The system creates or adds to this tab when you add an analog point (voltage, temperature, resistive, or high speed counter) by clicking the **Manage Points** button and selecting **Add** in the Nrio Point Manager view.

Points display under the appropriate Analog or Digital tab with a hyperlink that takes you to the individual point view where you can configure each point.

Manage Nrio Points windows

These windows manage individual points.

Figure 303. Manage Nrio Points window



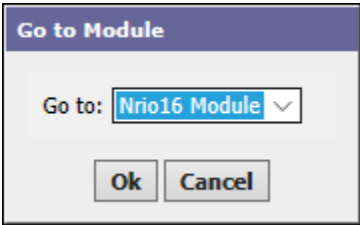
You open these windows from the main menu by clicking **Controller Setup > Remote Devices > Remote Drivers**, double-clicking the NrioNetwork row in the table, double-clicking the module name in the table, clicking the **Point Manager** link, followed by clicking the **Manage Points** link.

You can create two types of points: analog and digital, and those points may provide input or output functions. The sequence from left to right involves selecting the IO category (type of point), selecting the NRIO point to assign to this category, followed by naming the point and confirming its IO type.

Go to Module window

This window opens the module view for another module. The button that opens this window is only available if more than one module is present.

Figure 304. Go to Module window



This window opens in the module view when you click the **Go to Module** button.

Digital Points tab

This tab provides access to the system’s digital points.



Links



The system creates or adds to this tab when you add a digital point (digital input or relay output) by clicking the **Manage Points** button and selecting *Add* in the Nrio Point Manager view.

In addition to **Save**, these links support the point manager:

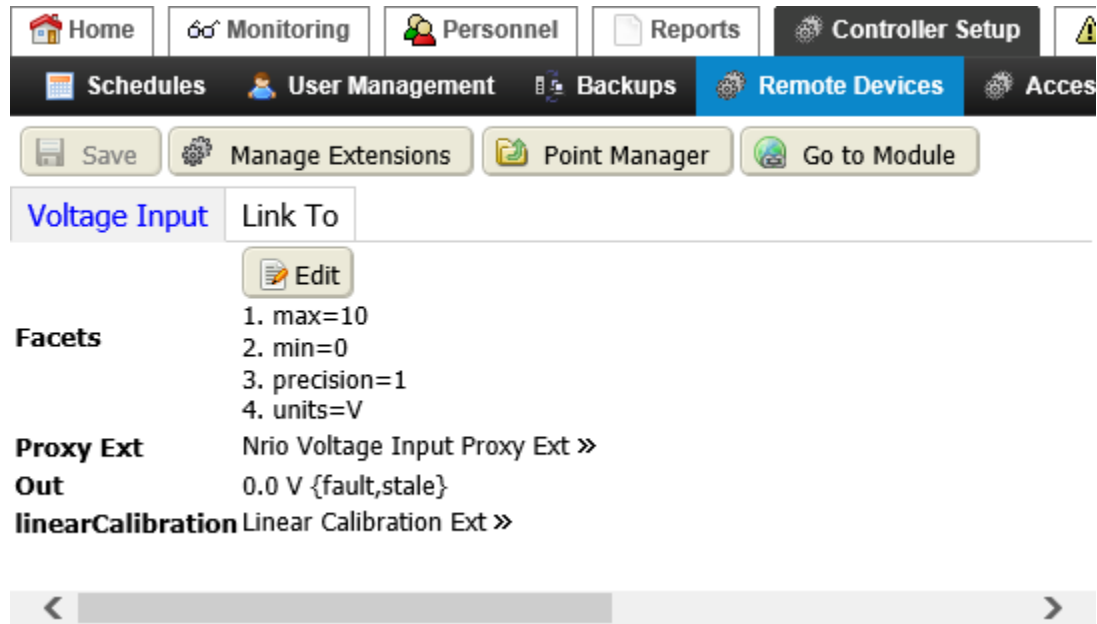
- **Manage Points** opens the **Manage Nrio Points** windows, which add, rename, delete, cut, copy, and paste analog and digital point information.
- **Go To Module** opens the **Go to Module** window for navigating to another set of Nrio module points. The system populates this window only when there are two or more Nrio modules on the network.
- **Nrio 16 Module** (in the screen capture) opens the current module view. The name on this button changes depending on the name of the module.

Nrio Point Edit view

This view edits point facets and provides links to point proxy extensions and other properties for each point.

Links

**Figure 305.** Example of a Point Edit view



You access this view from the main menu by clicking **Controller Setup > Remote Devices > Remote Drivers**, double-clicking the **NrioNetwork** row in the table, double-clicking a module, clicking the **Point Manager** button, followed by clicking the link to a specific point.

In addition to the **Save** link, these links support point management:

- **Manage Extensions** opens the windows for creating new point extensions.
- **Point Manager** returns to the Point Manager view.
- **Go To Module** opens a window for selecting the module to go to.

Button

Edit button opens the **Edit** window.

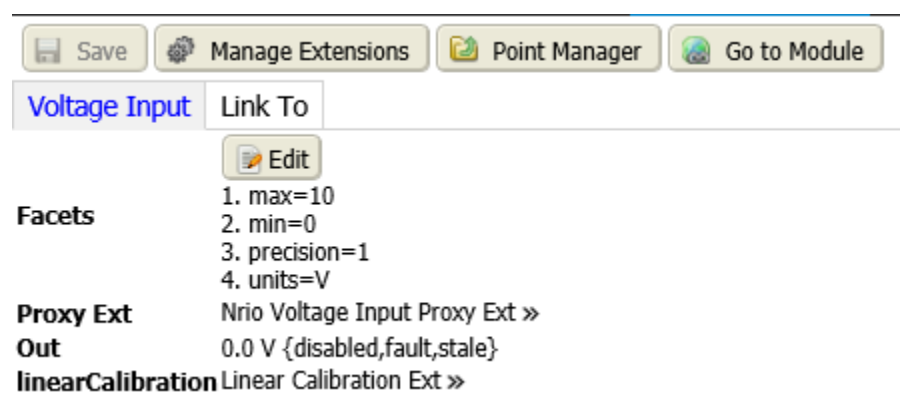
Properties

The properties for each point are described in the following topics.

Voltage Input points properties

This view provides tabs for editing and configuring Nrio proxy points under the points extension of a selected Nrio module.

**Figure 306.** Voltage Input tab



You access this view from the main menu by clicking **Controller Setup > Remote Devices > Remote Drivers**, double-clicking the **NrioNetwork** row in the table, double-clicking a module, clicking the **Point Manager** button, followed by clicking the link to a specific point.

Property	Value	Description
Facets	additional properties	Refer to <a href="#">Voltage Input points properties</a> .
Proxy Ext	additional properties	Refer to <a href="#">Voltage Input points properties</a> .
Out	read-only	Reports the current value of the proxy point and its status.
linearCalibration	additional properties	Refer to <a href="#">Voltage Input points properties</a> .

Voltage Input Facets

Facets determine how a point’s value displays in the station. Voltage Input facets include voltage numbers and decimal precision.

**Figure 307.** Voltage Input Facets and Edit facets window

Edit

Quantity

electric potential (m<sup>2</sup>·kg·s<sup>-3</sup>·A<sup>-1</sup>)

Unit

volt (V)

Min

0.0

Max

10.0

Precision

1

Ok

Cancel

This Edit window opens when you click the Edit button.

Property	Value	Description
Quantity	drop-down list	Defines input voltage.
max	number	Defines the maximum voltage value.
min	number	Defines the minimum voltage value.
precision	number	Defines the number of decimal places allowed.
units	defaults to Volts	Configures the default unit.

Voltage Proxy Ext properties

These properties configure the proxy point extension.

Figure 308. Voltage Proxy Ext properties

Nrio Voltage Input Proxy Ext ⌵

Proxy Ext

Status

{disabled,fault,stale}

Fault Cause

Enabled

true ⌵

Conversion

Default ⌵

Tuning Policy Name

Default Policy ⌵

Read Value

0.00 V {ok}

Write Value

0.00 V {ok}

Poll Frequency

Normal ⌵

Instance

1

Ui Type

Ai\_0to10\_vdc ⌵

In addition to the standard properties (**Status**, **Fault Cause**, and**Enabled**), these properties support the voltage proxy extension.

Property	Value	Description
Conversion	Drop-down list (defaults to Default)	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit</p>

Property	Value	Description
		<p>conversion should take place before or after the scale/offset conversion.</p> <p><code>Reverse Polarity</code> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list (defaults to <code>Default Policy</code> )	<p>Selects a network tuning policy by name. This policy defines stale time and minimum and maximum update times.</p> <p>During polling, the system uses the tuning policy to evaluate both write requests and the acceptability (freshness) of read</p>

Property	Value	Description
		requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only (applies to writable types only)	Displays the last value written using device facets.
Poll Frequency	drop-down list (defaults to <code>Normal</code> )	<p>Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its value. The network's Poll Service or Poll Scheduler defines these rates in hours, minutes and seconds. For example:</p> <p><code>Fast</code> may set polling frequency to every second.</p> <p><code>Normal</code> may set poll frequency to every five seconds.</p> <p><code>Slow</code> may set poll frequency to every 30 seconds.</p> <p>This property applies to all proxy points.</p>
Instance	number	<p>Defines the point's I/O terminal address based on its hardware type.</p> <p>If duplicated (same instance as same hardware type, same board), the point reports a fault status.</p> <p>If an edit attempt is made to an instance already in use by another proxy point, the system discards the edit, and retains the previous instance value.</p>
Ui Type	read-only	Identifies the Nrio Universal Input point type: Resistive Input, Boolean Output, etc.

Voltage Input, Linear Calibration Ext properties

These properties calibrate the calculated voltage value before it is applied to the Out slot, where  $[(\text{calculatedValue} \times \text{Scale}) + \text{Offset}] = \text{Out value}$ . Usage is optional, although `Offset` and `Units` are commonly configured.

**NOTE:** In most cases where the parent Nrio proxy point’s facets have been changed from defaults, you must edit the `Units` value in this extension to match the units in the point facets, otherwise the parent proxy point reports a fault for status!

Typically, you see this fault status immediately after you add a new input point, for example a `VoltageInputPoint` or `ResistanceInputPoint`, and configure it with a Linear conversion type (including a scale and offset), and then specify the point’s facets. It may not be immediately clear that the problem is in this Linear Calibration Ext, where you must match its `Units` value to the units in the point’s facets.

Figure 309. Linear Calibration properties

linearCalibration

Linear Calibration Ext

Scale

1.00000

Offset

0.00000

Units

Quantity

electric potential (m<sup>2</sup>·kg·s<sup>-3</sup>·A<sup>-1</sup>)

Unit

volt (V)

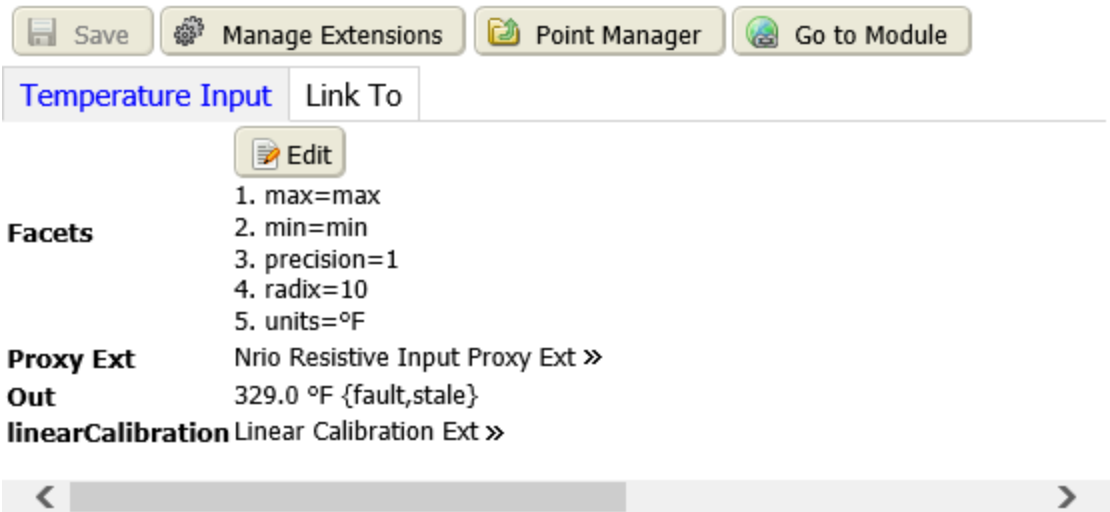
Fault Cause

Property	Value	Description
Scale	number, defaults to 1.0	Defines a scale value. Usually you leave this value set to the default. One exception is if you copied this extension under a <code>CounterInputPoint</code> for the purpose of returning a scaled total.
Offset	positive or negative number, defaults to 0.0	Can compensate for signal error introduced by sensor wiring resistance. If under a <code>CounterInputPoint</code> , leave it at zero (0).
Units	drop-down list	Defines the unit of measure. Should be the same as the parent proxy point’s facets.
Fault Cause	read-only	Indicates the reason why a system object (network, device, component, extension, etc.) is not working (in fault). This property is empty unless a fault exists.

Temperature Input points

Configures a temperature input point.

Figure 310. Temperature Input tab



You access this view from the main menu by clicking **Controller Setup > Remote Devices > Remote Drivers**, double-clicking the **NrioNetwork** driver, double-clicking a module, clicking the **Point Manager** link, followed by clicking the hyperlink to the right end of the `Temperature Input` point.

Property	Value	Description
Facets	additional properties	Refer to <a href="#">Temperature Input Facets</a> .
Proxy Ext	additional properties	Refer to <a href="#">Temperature Proxy Ext properties</a> .
Out	read-only	Reports the current temperature of the proxy point and its status.
linearCalibration	additional properties	Refer to <a href="#">Temperature Input, Linear Calibration Ext properties</a> .

Temperature Input Facets

Facets determine how a point’s value displays in the station. Temperature facets include a minimum, maximum, and decimal precision.



**Figure 311.** Temperature Input Facets and Edit facets window

Edit

Quantity

temperature (K) ▾

Unit

fahrenheit (°F) ▾

Min

-2.147483648E9

Max

2.147483647E9

Precision

1

Ok

Cancel

The Edit window opens when you click the **Edit** button.

Property	Value	Description
Quantity	drop-down list	Defines the units used to measure temperature.
max	number	Defines the maximum temperature value.
min	number	Defines the minimum temperature value.
precision	number	Defines the number of decimal places allowed.
radix	number, defaults to 10	Defines the number of unique digits, including zero, used to represent numbers in a positional numeral system.
units	defaults to degrees Fahrenheit	Configures the default unit.

Temperature Proxy Ext properties

These properties configure the proxy point extension.

Figure 312. Temperature Proxy Ext properties

SaveManage ExtensionsPoint ManagerGo to Module

Temperature InputLink To

Edit

Facets

1. max=max  
2. min=min  
3. precision=1  
4. radix=10  
5. units=°F  
Nrio Resistive Input Proxy Ext

Proxy Ext

Status

{disabled,fault,stale}

Fault Cause

Enabled

true

Conversion

Thermistor Type 3 (nrio)

Tuning Policy Name

Default Policy

Read Value

0.00 Ω {ok}

Write Value

0.00 Ω {ok}

Poll Frequency

Normal

Instance

3

Ui Type

Ai \_ Resistive

Out

329.0 °F {disabled,fault,stale}

Linear Calibration Ext

linearCalibration

Scale

1.00000

Offset

0.00000

Units

Quantitytemperature (K)Unitfahrenheit (°F)

Fault Cause

In addition to the standard properties (**Status**, **Fault Cause**, and **Enabled**), these properties support temperature proxy extensions.

Property	Value	Description
Conversion	Drop-down list (defaults to Default)	<div>Defines how the system converts proxy extension units to parent point units.</div> <div>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</div>

Property	Value	Description
		<p><b>NOTE:</b> In most cases, the standard <code>Default</code> conversion is best.</p> <p><code>Linear</code> applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the <code>Scale</code> and <code>Offset</code> properties to convert the output value to a unit other than that defined by device facets.</p> <p><code>Linear With Unit</code> is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on <code>"Device Value"</code> or <code>"Proxy Value"</code>. The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><code>Reverse Polarity</code> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the <code>Ui</code> input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p>

Property	Value	Description
		<p>Generic Tabular applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list (defaults to Default Policy)	<p>Selects a network tuning policy by name. This policy defines stale time and minimum and maximum update times.</p> <p>During polling, the system uses the tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.</p>
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only (applies to writable types only)	Displays the last value written using device facets.
Poll Frequency	drop-down list (defaults to Normal)	<p>Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its value. The network's Poll Service or Poll Scheduler defines these rates in hours, minutes and seconds. For example:</p> <p>Fast may set polling frequency to every second.</p> <p>Normal may set poll frequency to every five seconds.</p> <p>Slow may set poll frequency to every 30 seconds.</p> <p>This property applies to all proxy points.</p>

Property	Value	Description
Instance	number	Defines the point's I/O terminal address based on its hardware type.  If duplicated (same instance as same hardware type, same board), the point reports a fault status.  If an edit attempt is made to an instance already in use by another proxy point, the system discards the edit, and retains the previous instance value.
Ui Type	read-only	Identifies the Nrio Universal Input point type: Resistive Input, Boolean Output, etc.

Temperature Input, Linear Calibration Ext properties

These properties calibrate the calculated temperature value before it is applied to the Out slot, where [(calculatedValue x Scale) + Offset] = Out value. Usage is optional, although **Offset** and **Units** are commonly configured.

**NOTE:** In most cases where the parent Nrio proxy point's facets have been changed from defaults, you must edit the **Units** value in this extension to match the units in the point facets, otherwise the parent proxy point reports a fault for status!

Figure 313. Linear Calibration properties

linearCalibration

Scale

1.00000

Offset

0.00000

Units

Quantity

temperature (K)

▼

Unit

fahrenheit (°F)

▼

Fault Cause

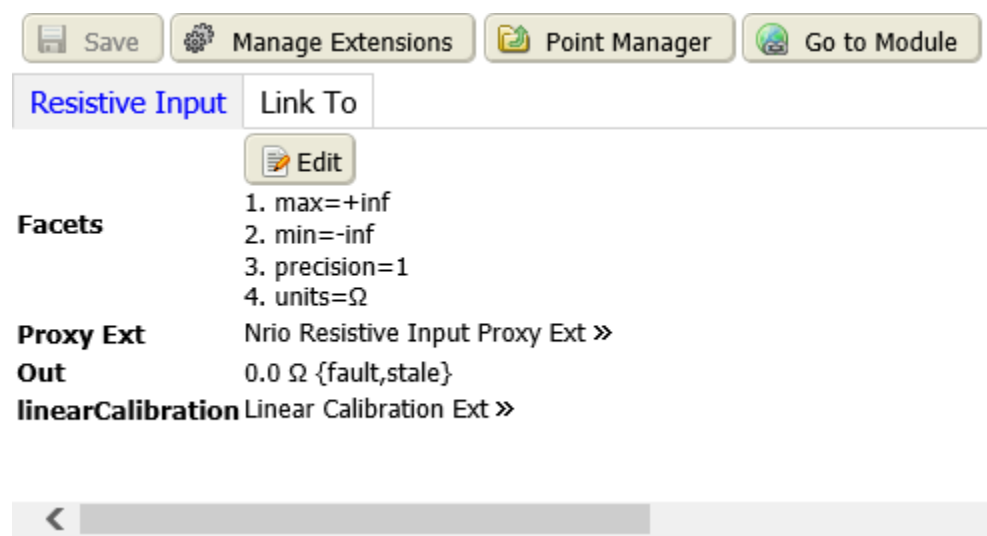
Property	Value	Description
Scale	number, defaults to 1.0	Defines a scale value. Usually you leave this value set to the default. One exception is if you copied this extension under a CounterInputPoint for the purpose of returning a scaled total.
Offset	positive or negative number, defaults to 0.0	Can compensate for signal error introduced by sensor wiring resistance. If under a CounterInputPoint, leave it at zero

Property	Value	Description
		(0).
Units	drop-down list	Defines the unit of measure. Should be the same as the parent proxy point's facets.
Fault Cause	read-only	Indicates the reason why a system object (network, device, component, extension, etc.) is not working (in fault). This property is empty unless a fault exists.

Resistive Input points

This is a NumericPoint that reads a resistive signal within a 0-to-100K ohm range and produces either an ohms value or a linear, scaled output value.

Figure 314. Resistive Input tab



You access this view from the main menu by clicking **Controller Setup > Remote Devices > Remote Drivers**, followed by double-clicking the NrioNetwork driver, selecting and double-clicking a module, clicking the Point Manager link, followed by clicking the hyperlink to the right end of the Restive Input point.

Property	Value	Description
Facets	additional properties	Refer to <a href="#">Resistive Input Facets</a> .
Proxy Ext	additional properties	Refer to <a href="#">Resistive Input Proxy Ext properties</a> .
Out	read-only	Reports the current value of the proxy point and its status.

Property	Value	Description
linearCalibration	additional properties	Refer to <a href="#">Resistive Input, Linear Calibration Ext properties</a> .

Resistive Input Facets

Facets determine how a point’s value displays in the station. Resistive input facets include a minimum, maximum, and decimal precision.

**Figure 315.** Resistive Input Facets and Edit facets window

Edit

Quantity

electric resistance (m<sup>2</sup>·kg·s<sup>-3</sup>·A<sup>-2</sup>)

Unit

ohm (Ω)

Min

-Infinity

Max

Infinity

Precision

1

Ok

Cancel

The Edit window opens when you click the **Edit** button.

Property	Value	Description
Quantity	drop-down list	Defines the formula.
Unit	defaults to ohm	Configures the default unit.
Max	number, defaults to Infinity	Defines the maximum ohm value.
Min	number, defaults to negative Infinity	Defines the minimum ohm value.
Precision	number, defaults to one	Defines the number of decimal places allowed.

Resistive Input Proxy Ext properties

These properties configure the proxy point extension.

Figure 316. Resistive Input Proxy Ext properties

Save

Manage Extensions

Point Manager

Go to Module

Resistive Input

Link To

Edit

Facets

1. max=+inf

2. min=-inf

3. precision=1

4. units= $\Omega$

Nrio Resistive Input Proxy Ext

Status

{disabled,fault,stale}

Fault Cause

Enabled

true

Conversion

Default

Proxy Ext

Tuning Policy Name

Default Policy

Read Value

0.00  $\Omega$  {ok}

Write Value

0.00  $\Omega$  {ok}

Poll Frequency

Normal

Instance

4

Ui Type

Ai \_ Resistive

Out

0.0  $\Omega$  {disabled,fault,stale}

Linear Calibration Ext

Scale

1.00000

Offset

0.00000

linearCalibration

Units

Quantity

electric resistance (m<sup>2</sup>·kg·s<sup>-3</sup>·A<sup>-2</sup>)

Unit

ohm ( $\Omega$ )

Fault Cause

In addition to the standard properties (Status, Fault Cause, and Enabled), these properties support resistive input proxy extensions.

Property	Value	Description
Conversion	Drop-down list (defaults to Default)	<div>Defines how the system converts proxy extension units to parent point units.</div> <div>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</div>



Property	Value	Description
		<p><b>NOTE:</b> In most cases, the standard <code>Default</code> conversion is best.</p> <p><code>Linear</code> applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the <code>Scale</code> and <code>Offset</code> properties to convert the output value to a unit other than that defined by device facets.</p> <p><code>Linear With Unit</code> is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on <code>"Device Value"</code> or <code>"Proxy Value"</code>. The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><code>Reverse Polarity</code> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the <code>Ui</code> input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p>

Property	Value	Description
		<p>Generic Tabular applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list (defaults to Default Policy)	<p>Selects a network tuning policy by name. This policy defines stale time and minimum and maximum update times.</p> <p>During polling, the system uses the tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.</p>
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only (applies to writable types only)	Displays the last value written using device facets.
Poll Frequency	drop-down list (defaults to Normal)	<p>Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its value. The network's Poll Service or Poll Scheduler defines these rates in hours, minutes and seconds. For example:</p> <p>Fast may set polling frequency to every second.</p> <p>Normal may set poll frequency to every five seconds.</p> <p>Slow may set poll frequency to every 30 seconds.</p> <p>This property applies to all proxy points.</p>

Property	Value	Description
Instance	number	Defines the point's I/O terminal address based on its hardware type.  If duplicated (same instance as same hardware type, same board), the point reports a fault status.  If an edit attempt is made to an instance already in use by another proxy point, the system discards the edit, and retains the previous instance value.
Ui Type	read-only	Identifies the Nrio Universal Input point type: Resistive Input, Boolean Output, etc.

Resistive Input, Linear Calibration Ext properties

These properties calibrate the calculated resistance value before it is applied to the Out slot, where [(calculatedValue x Scale) + Offset] = Out value. Usage is optional, although **Offset** and **Units** are commonly configured.

**NOTE:** In most cases where the parent Nrio proxy point's facets have been changed from defaults, you must edit the **Units** value in this extension to match the units in the point facets, otherwise the parent proxy point reports a fault for status!

Typically, you see this fault status immediately after you add a new input point, for example a VoltageInputPoint or ResistanceInputPoint, and configure it with a Linear conversion type (including a scale and offset), and then specify the point's facets. It may not be immediately clear that the problem is in this Linear Calibration Ext, where you must match its Units value to the units in the point's facets.

Figure 317. Resistive Input Linear Calibration properties

linearCalibration

Linear Calibration Ext

Scale

1.00000

Offset

0.00000

Units

Quantity

electric resistance (m<sup>2</sup>·kg·s<sup>-3</sup>·A<sup>-2</sup>)

Unit

ohm (Ω)

Fault Cause

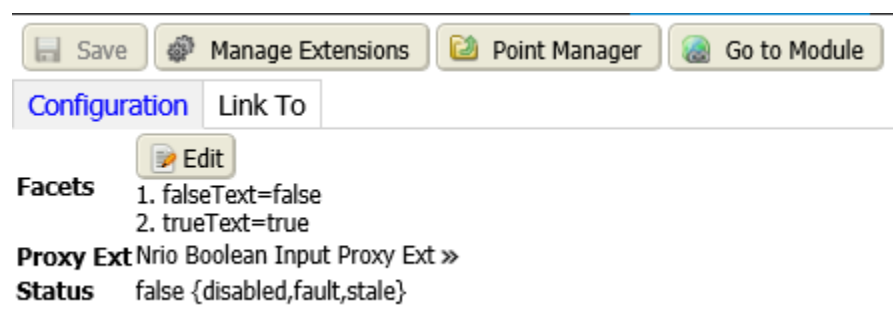
Property	Value	Description
Scale	number, defaults to 1.0	Defines a scale value. Usually you leave this value set to the default. One exception is if you copied this extension under a CounterInputPoint

Property	Value	Description
		for the purpose of returning a scaled total.
Offset	positive or negative number, defaults to 0.0	Can compensate for signal error introduced by sensor wiring resistance. If under a CounterInputPoint, leave it at zero (0).
Units	drop-down list	Defines the unit of measure. Should be the same as the parent proxy point's facets.
Fault Cause	read-only	Indicates the reason why a system object (network, device, component, extension, etc.) is not working (in fault). This property is empty unless a fault exists.

Digital input points

Configures a Boolean Input proxy point.

Figure 318. Digital Input, Configuration tab



You access this view from the main menu by clicking **Controller Setup > Remote Devices > Remote Drivers**, followed by double-clicking the NrioNetwork driver, selecting and double-clicking a module, clicking the **Point Manager** link, clicking the Digital Points tab, followed by clicking the hyperlink on a Digital Input point.

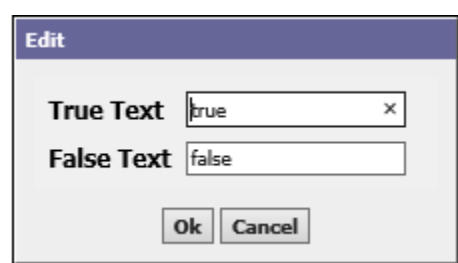
The input facets and proxy extension properties are the same as those documented for other Nrio proxy points.

Property	Value	Description
Facets	additional properties	Refer to "Edit Window" below.
Proxy Ext	additional properties	Refer to "Digital Proxy Ext properties" below.

Property	Value	Description
Status	read-only	<p>Reports the condition of the entity or process at last polling.</p> <p>{ok} indicates that the component is licensed and polling successfully.</p> <p>{down} indicates that the last check was unsuccessful, perhaps because of an incorrect property, or possibly loss of network connection.</p> <p>{disabled} indicates that the <b>Enable</b> property is set to <code>false</code>.</p> <p>{fault} indicates another problem. Refer to <b>Fault Cause</b> for more information.</p>

Edit window

**Figure 319.** Facets Edit window



This window opens when you click the **Edit** button.

Property	Value	Description
True Text	text	Sets up the text to appear when <code>status</code> for the point is true.
False Text	text	Sets up the text to appear when <code>status</code> for the point is false.

Digital Proxy Ext properties

Figure 320. Digital Proxy Ext properties

Status

Fault Cause

Enabled

Conversion

Proxy Ext Tuning Policy Name

Read Value

Write Value

Poll Frequency

Instance

Ui Type

{fault,stale}

true ▾

Default ▾

Default Policy ▾

false {ok}

false {ok}

Normal ▾

4

Di \_ Normal ▾

In addition to the standard properties (Status, Fault Cause and Enabled), these properties configure this extension.

Property	Value	Description
Conversion	Drop-down list (defaults to Default)	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy</p>

Property	Value	Description
		<p>Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p>500 Ohm Shunt applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p>Tabular Thermistor applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p>Thermistor Type 3 applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p>Generic Tabular applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list (defaults to Default Policy)	<p>Selects a network tuning policy by name. This policy defines stale time and minimum and maximum update times.</p> <p>During polling, the system uses</p>

Property	Value	Description
		the tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written using device facets.
Instance	number	<p>Defines the point's I/O terminal address based on its hardware type.</p> <p>If duplicated (same instance as same hardware type, same board), the point reports a fault status.</p> <p>If an edit attempt is made to an instance already in use by another proxy point, the system discards the edit, and retains the previous instance value.</p>
Poll Frequency	drop-down list (defaults to <code>Normal</code> )	<p>Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its value. The network's Poll Service or Poll Scheduler defines these rates in hours, minutes and seconds. For example:</p> <p><code>Fast</code> may set polling frequency to every second.</p> <p><code>Normal</code> may set poll frequency to every five seconds.</p> <p><code>Slow</code> may set poll frequency to every 30 seconds.</p> <p>This property applies to all proxy points.</p>
Ui Type	drop-down list	Identifies the Nrio Universal Input point type: Resistive Input, Boolean



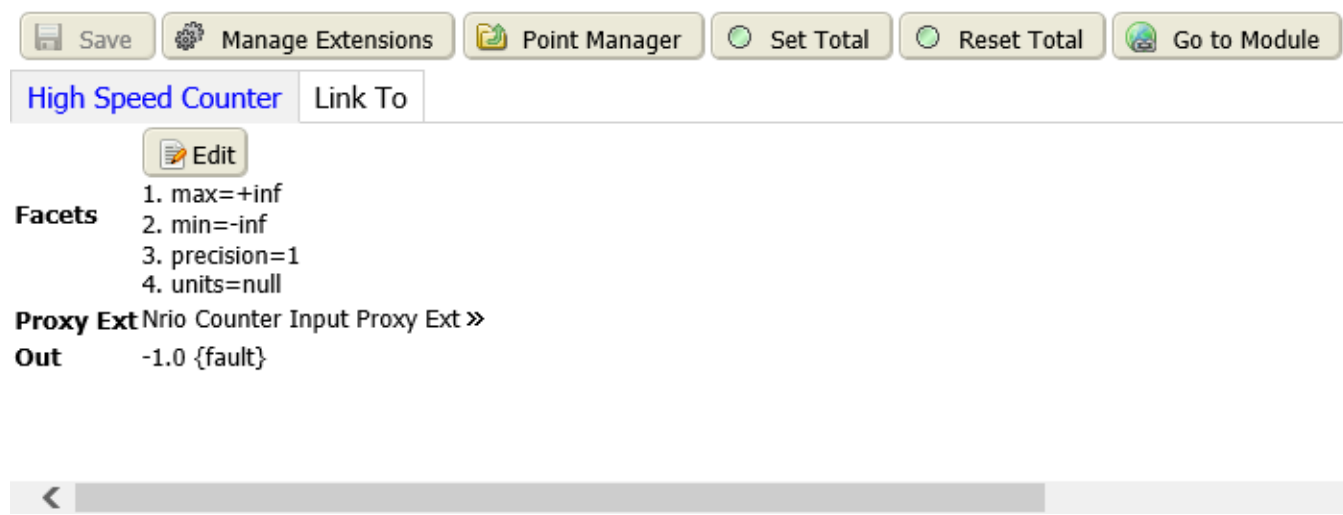
Property	Value	Description
		Output, etc.

High Speed Counter

This is a NumericPoint that configures a Ui to count dry-contact pulses up to 20 Hz, as well as to calculate a numeric rate.You specify which value is to appear in the Out slot (either Count or Rate) as a status numeric.

The proxy extension contains configuration properties for rate calculation, and a status property for total number of pulses counted since the counter was last set or reset.

Figure 321. High Speed Counter tab



You access this view from the main menu by clicking **Controller Setup > Remote Devices > Remote Drivers**, double-clicking the **NrioNetwork** driver, double-clicking a module, clicking the **Point Manager** link, followed by clicking the hyperlink to the right end of the High Speed Counter point.

Property	Value	Description
Facets	button and additional properties	Determine how values are formatted for display depending on the context and the type of data. Examples include engineering units and decimal precision for numeric types, and descriptive value (state) text for boolean and enum types.  With the exception of proxy points (with possible defined device facets), point facets do not affect how the framework processes the point's value.

Property	Value	Description
		<p>Besides control points, various other components have facets too. For example, many <code>kitControl</code> and <code>schedule</code> components have facets. Details about point facets apply to these components too, unless especially noted.</p> <p>You access facets by clicking an <code>Edit</code> button or a chevron <code>&gt;&gt;</code>. Both open an <code>Edit Facets</code> window.</p>
Proxy Ext	additional properties	Refer to <a href="#">High Speed Counter Proxy Ext properties</a> .
Out (general)	read-only	<p>Displays the current value of the proxy point including facets and status.</p> <p>The value depends on the type of control point.</p> <p>Facets define how the value displays, including the value's number of decimal places, engineering units, or text descriptors for Boolean/enum states. You can edit point facets to poll for additional properties, such as the native <code>statusFlags</code> and/or <code>priorityArray</code> level.</p> <p>Status reports the current health and validity of the value. Status is specified by a combination of status flags, such as <code>fault</code>, <code>overridden</code>, <code>alarm</code>, and so on. If no status flag is set, status is considered normal and reports <code>{ok}</code>.</p>

High Speed Counter Facets

Facets determine how a point's value displays in the station. High Speed Counter facets include a minimum, maximum, and decimal precision.

**Figure 322.** High Speed Counter Facets and Edit facets window

Edit

Quantity

misc ()

Unit

null (null)

Min

-Infinity

Max

Infinity

Precision

1

Ok

Cancel

The Edit window opens when you click the **Edit** button.

Property	Value	Description
Quantity	drop-down list, defaults to misc ()	Configures the formula.
Unit	defaults to null	Configures the default unit.
max	number, defaults to Infinity	Defines the maximum high speed counter value.
min	number, defaults to negative Infinity	Defines the minimum high speed counter value.
precision	number, defaults to 1	Defines the number of decimal places allowed.

High Speed Counter Proxy Ext properties

Figure 323. High Speed Counter Proxy Ext properties

Nrio Counter Input Proxy Ext ⌵

Status

{disabled,fault,stale}

Fault Cause

Enabled

true ⌵

Conversion

Default ⌵

Tuning Policy Name

Default Policy ⌵

Read Value

0.00 {ok}

Write Value

0.00 {ok}

Poll Frequency

Normal ⌵

Proxy Ext Instance

7

Ui Type

Di \_ High Speed ⌵

Output Select

Count ⌵

Total

-1

Rate

0.00

Rate Calc Type

nrio:FixedWindowRateType

In addition to the standard properties (Status, Fault Cause, and Enabled), these properties support high speed counter proxy extensions.

Property	Value	Description
Conversion	Drop-down list (defaults to Default)	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p>

Property	Value	Description
		<p><code>Linear With Unit</code> is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><code>Reverse Polarity</code> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list (defaults to <code>Default Policy</code> )	Selects a network tuning policy

Property	Value	Description
		<p>by name. This policy defines stale time and minimum and maximum update times.</p> <p>During polling, the system uses the tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.</p>
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only (applies to writable types only)	Displays the last value written using device facets.
Poll Frequency	drop-down list (defaults to <code>Normal</code> )	<p>Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its value. The network's Poll Service or Poll Scheduler defines these rates in hours, minutes and seconds. For example:</p> <p><code>Fast</code> may set polling frequency to every second.</p> <p><code>Normal</code> may set poll frequency to every five seconds.</p> <p><code>Slow</code> may set poll frequency to every 30 seconds.</p> <p>This property applies to all proxy points.</p>
Instance	number	<p>Defines the point's I/O terminal address based on its hardware type.</p> <p>If duplicated (same instance as same hardware type, same board), the point reports a fault status.</p> <p>If an edit attempt is made to an instance already in use by another proxy point, the system</p>

Property	Value	Description
		discards the edit, and retains the previous instance value.
Ui Type	read-only	Identifies the Nrio Universal Input point type: Resistive Input, Boolean Output, etc.
Output Select	drop-down list, defaults to <code>Count</code>	Specifies if count total ( <code>Count</code> ) or count rate ( <code>Rate</code> ) is at the Out slot as a status numeric.
Total	read-only	Reports the total number of pulses counted since the proxy extension was last set or reset.
Rate	read-only	Reports the calculated rate based on the <code>Rate Calc</code> configuration.
Rate Calc Type	drop-down list	<p>Defines the type of rate calculation: The purpose of these calculations is to report a meaningful value:</p> <p><code>FixedWindowRateType</code> waits for the interval defined under the <code>Rate Calc</code> slot to elapse. Then it recalculates the rate based on the interval.</p> <p><code>SlidingWindowRateType</code> calculates the rate based on the specified interval every interval/window number of seconds. This updates the rate more frequently while maintaining the calculation based on the specified interval.</p> <p><code>TriggeredRateType</code> adds a <code>recalculateRate</code> action to the parent point.</p>
Rate Calc	additional properties	<p>Provides one to three properties to use in the rate calculation:</p> <p><code>scale</code> (defaults to 1) depends on the item quantity/pulse and desired rate units.</p> <p><code>Interval</code> (not available if <code>Rate Calc Type</code> is <code>Triggered Rate type</code>) defaults to one (1) minute.</p>

Property	Value	Description
		Windows (available only if Rate Calc Type is SlidingWindowRateType defaults to six (6)).
Rate Calc Time	read-only	Reports the timestamp of the last rate calculation.

### Relay Output points (digital)

Configures up to 16 digital Nrio relay output point terminals.

**Figure 324.** Relay Output, Configuration tab

Save

Manage Extensions

Point Manager

Manual Override

Go to Module

Configuration

Active Schedule

Link To

Link From

Edit

Facets

1. falseText=false

2. trueText=true

Proxy Ext

Nrio Relay Output Proxy Ext »

Status

false {disabled,fault,stale}

In1

- {null}

In2

- {null} »

In3

- {null} »

In4

- {null} »

In5

- {null} »

In6

- {null}

In7

- {null} »

In8

- {null}

In9

- {null} »

In10

- {null} »

In11

- {null} »

In12

- {null} »

In13

- {null} »

In14

- {null} »

In15

- {null} »

In16

- {null} »

Fallback

false {ok} »

Override Expiration

31

Dec

1969

07

:

00

PM

EST

Min Active Time

+

00000

h

00

m

00

s

Min Inactive Time

+

00000

h

00

m

00

s

Set Min Inactive Time On Start

false

You access this view from the Nrio Point Manager by clicking the Digital Points tab, followed by clicking the hyperlink on a Relay Output point.



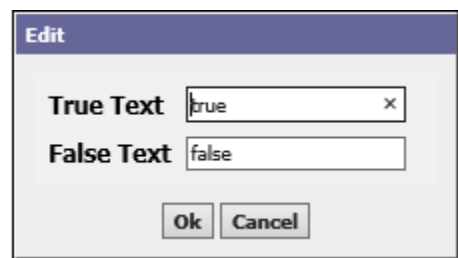
Property	Value	Description
Facets	additional properties	Refer to <a href="#">Relay Out Facets</a> .
Proxy Ext	additional properties	Refer to <a href="#">Relay out Proxy Ext properties</a> .
Status	read-only	<p>Reports the condition of the entity or process at last polling.</p> <p><code>{ok}</code> indicates that the component is licensed and polling successfully.</p> <p><code>{down}</code> indicates that the last check was unsuccessful, perhaps because of an incorrect property, or possibly loss of network connection.</p> <p><code>{disabled}</code> indicates that the <b>Enable</b> property is set to <code>false</code>.</p> <p><code>{fault}</code> indicates another problem. Refer to <b>Fault Cause</b> for more information.</p>
In2-5, 7, and 9-16	true or false, defaults to false	<p>Configures the amount of voltage coming from each of 16 inputs.</p> <p>When null is checked, the value displayed defaults to the incoming value from the device. If you remove the check mark you can configure the <code>In</code> value.</p>
Fallback	true or false, defaults to false	Pre-defines and output value in case of a null input.
Override Expiration	Date and time drop-down lists.	Defines an expiration date and time.
Min Active Time	hours, minutes, seconds	Specifies a minimum amount of time that a device must run once it is started.
Min Inactive Time	hours, minutes, seconds	Specifies a minimum amount of time that a device must be idle once it is stopped.
Set Min Inactive Time On Start	true or false, defaults to false	Configures the system to set the minimum inactive time when the station starts.

Property	Value	Description
		Minimum active and inactive times prevent short-cycling of equipment controlled by a point.

Relay Out Facets

As a Boolean writable, these proxy points support two states, which default to `true` or `false`.

Figure 325. Relay Output Configuration Facets

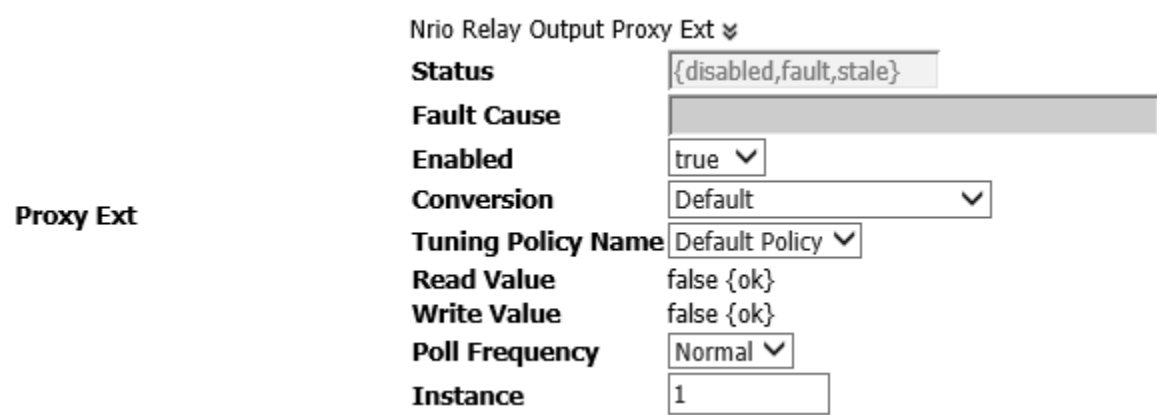


You use this window to configure different text (other than `true` and `false`) when the station writes this Boolean value.

Relay out Proxy Ext properties

The proxy extension properties are the same as those documented for other Nrio proxy points.

Figure 326. Relay Out Proxy Ext properties



In addition to the standard properties (`Status`, `Fault Cause` and `Enabled`), the relay out proxy extension provides these properties

Property	Value	Description
Conversion	Drop-down list (defaults to <code>Default</code> )	Defines how the system converts

Property	Value	Description
		<p>proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p>500 Ohm Shunt applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p>Tabular Thermistor applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p>Thermistor Type 3 applies to an</p>

Property	Value	Description
		<p>Thermistor Input point, where this selection provides a “built-in” input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p>Generic Tabular applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the “Thermistor Tabular” conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list (defaults to Default Policy)	<p>Selects a network tuning policy by name. This policy defines stale time and minimum and maximum update times.</p> <p>During polling, the system uses the tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.</p>
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only (applies to writable types only)	Displays the last value written using device facets.
Poll Frequency	drop-down list (defaults to Normal)	<p>Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its value. The network’s Poll Service or Poll Scheduler defines these rates in hours, minutes and seconds. For example:</p> <p>Fast may set polling frequency to every second.</p> <p>Normal may set poll frequency to every five seconds.</p>

Property	Value	Description
		<p><code>Slow</code> may set poll frequency to every 30 seconds.</p> <p>This property applies to all proxy points.</p>
Instance	number	<p>Defines the point's I/O terminal address based on its hardware type.</p> <p>If duplicated (same instance as same hardware type, same board), the point reports a fault status.</p> <p>If an edit attempt is made to an instance already in use by another proxy point, the system discards the edit, and retains the previous instance value.</p>

Voltage Output points

This is a NumericWritable point that represents a 0-to-10Vdc analog output (AO).

Figure 327. Voltage Output tab

Voltage Output

Link To

Link From

Edit

Facets

1. max=10

2. min=0

3. precision=1

4. units=V

Proxy Ext

Nrio Voltage Output Proxy Ext »

Out

0.0 V {disabled,fault,stale}

In1

- {null}

In2

- {null} »

In3

- {null} »

In4

- {null} »

In5

- {null} »

In6

- {null} »

In7

- {null} »

In8

- {null}

In9

- {null} »

In10

- {null} »

In11

- {null} »

In12

- {null} »

In13

- {null} »

In14

- {null} »

In15

- {null} »

In16

- {null} »

Fallback

0.0 V {ok} »

Override Expiration

31

Dec

1969

07

:

00

PM

EST

You access it from the Nrio Point Manager, Analog Points tab by clicking the hyperlink on a Voltage Output point.

Property	Value	Description
Facets	additional properties	Refer to <a href="#">Voltage Output Facets properties</a> .
Proxy Ext	additional properties	Refer to <a href="#">Voltage Output Proxy Ext properties</a> .
Out	read-only	Reports the current value of the proxy point and its status.
In2-7 and 9-16	number of volts between 0.00 and 10.0, defaults to 0.0	Configures the number of output volts.
Fallback	number of volts between 0.00 and	Creates a pre-defined output value in

Property	Value	Description
	10.0, defaults to 0.0	case of a null input.
Override Expiration	Date and time drop-down lists.	Defines when a waiting period is over and an action is automatically issued to a point.

Voltage Output Facets properties

Facets determine how a point’s value displays in the station. Voltage Output facets include voltage numbers and decimal precision.

Figure 328. Voltage Output facets and Edit facetw window

Edit

Quantity

electric potential (m<sup>2</sup>·kg·s<sup>-3</sup>·A<sup>-1</sup>)

Unit

volt (V)

Min

0.0

Max

10.0

Precision

1

Ok

Cancel

Property	Value	Description
Quantity	drop-down lists, defaults to electric potential.	Configures the formula.
Unit	defaults to Volts	Configures the default unit.
max	number, defaults to 0.0	Defines the maximum high speed counter value.
min	number, defaults to 10.0	Defines the minimum high speed counter value.
precision	number, defaults to 1	Defines the number of decimal places allowed.

Voltage Output Proxy Ext properties

Nrio-capable controllers and external I/O modules typically have some number of relay-type digital outputs (DO) and/or 0-to-10Vdc analog output (AO) terminals.

The driver supports two writable points:

- RelayOutputWritable, which is a standard BooleanWritable point with an NrioRelayOutputWritable proxy extension.

This point defaults to normal logic, that is, an input value of `true` closes the contacts. A `Conversion` type

of `Reverse Polarity` reverses the Boolean state going from input to output, thus opening the contacts.

- `VoltageOutputWritable`, which is a standard `NumericWritable` point with an `NrioVoltageOutputWritable` proxy extension.

This point represents a 0-to-10Vdc analog output with additional override properties.

**Figure 329.** Voltage Output Proxy Ext properties

Nrio Voltage Input Proxy Ext ⌵

Proxy Ext

Status

{disabled,fault,stale}

Fault Cause

Enabled

true ⌵

Conversion

Default ⌵

Tuning Policy Name

Default Policy ⌵

Read Value

0.00 V {ok}

Write Value

0.00 V {ok}

Poll Frequency

Normal ⌵

Instance

1

Ui Type

Ai\_0to10\_vdc ⌵

In addition to the standard properties (`Status`, `Fault Cause`, and `Enabled`), these properties support voltage output proxy extensions.

Property	Value	Description
Conversion	Drop-down list (defaults to <code>Default</code> )	<p>Defines how the system converts proxy extension units to parent point units.</p> <p><code>Default</code> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard <code>Default</code> conversion is best.</p> <p><code>Linear</code> applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the <code>Scale</code> and <code>Offset</code> properties to convert the output value to a unit other than that defined by device facets.</p> <p><code>Linear With Unit</code> is an extension to the existing linear conversion property. This specifies whether</p>



Property	Value	Description
		<p>the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><code>Reverse Polarity</code> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list (defaults to <code>Default Policy</code> )	Selects a network tuning policy by name. This policy defines stale time and minimum and maximum update times.

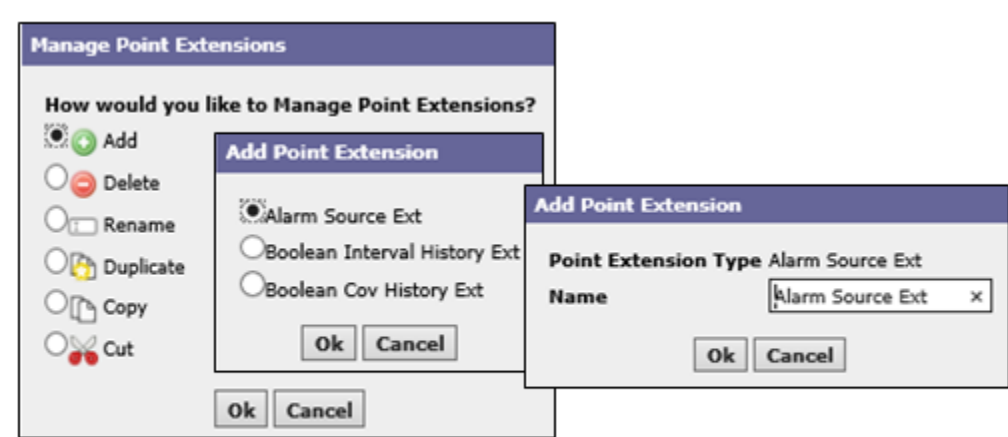
Property	Value	Description
		During polling, the system uses the tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written using device facets.
Poll Frequency	drop-down list (defaults to <code>Normal</code> )	<p>Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its value. The network's Poll Service or Poll Scheduler defines these rates in hours, minutes and seconds. For example:</p> <p><code>Fast</code> may set polling frequency to every second.</p> <p><code>Normal</code> may set poll frequency to every five seconds.</p> <p><code>Slow</code> may set poll frequency to every 30 seconds.</p> <p>This property applies to all proxy points.</p>
Instance	number	<p>Defines the point's I/O terminal address based on its hardware type.</p> <p>If duplicated (same instance as same hardware type, same board), the point reports a fault status.</p> <p>If an edit attempt is made to an instance already in use by another proxy point, the system discards the edit, and retains the previous instance value.</p>
Ui Type	read-only	Identifies the Nrio Universal Input

Property	Value	Description
		point type: Resistive Input, Boolean Output, etc.

Manage Extensions windows

These windows add extensions to the Point Manager views. Both analog and digital views support the addition of extensions. The extensions appear as additional tabs on the input and output views.

Figure 330. Add Extensions windows



You can access this view from the Manage Extensions view by clicking the Manage Point Extensions tab, and following the wizard.

Following are the buttons in the Manage Point Extensions Window:

You can add Alarm Source extensions, History Extensions, and create links between appropriate points using standard assign Mode features.

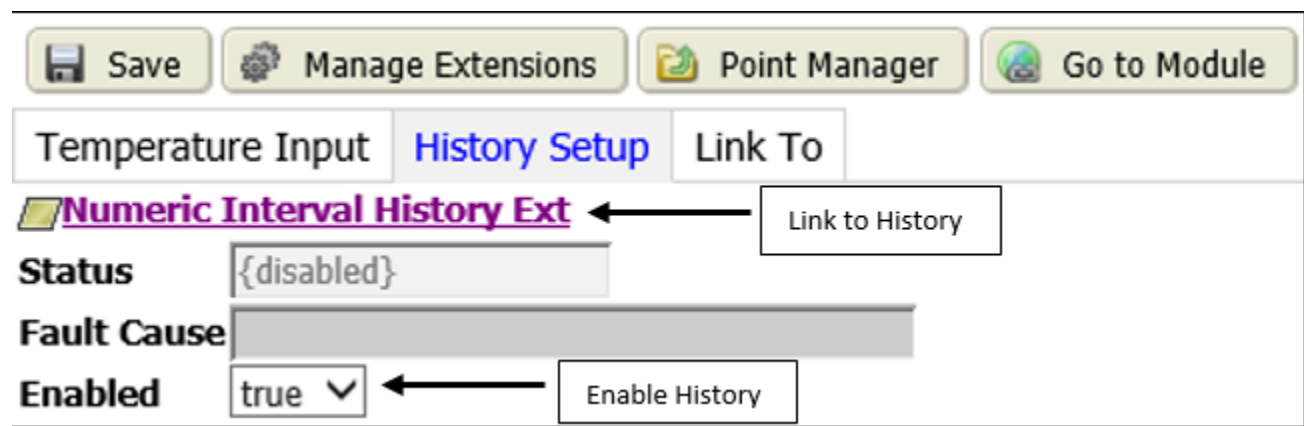
Extension properties are sensitive to point types (digital, analog, output, input).

History Setup tab

This tab configures one or more history extensions associated with a specific point. This history extension could go on any point. When added to a point it appears as a tab on the point’s view.

Links

**Figure 331.** History Setup tab



The system displays this tab when you click the **Manage Extensions** button at the top of a proxy point view and create a Numeric Interval or Numeric Cov History Extension. To start recording history records, you must enable the extension on this tab.

Once created, you access this tab from the Nrio Point Manager by clicking the hyperlink for one of the input, counter or output points.

In the History Setup tab, click on the point History Ext link to navigate to the History Extension tab, where you can refer to details about the history record.

The links at the top of this tab provide these functions:

- **Point Manager** opens the Nrio Point Manager view.
- **Go To Module** opens the **Go to Module** window for navigating to another Nrio module under the controller’s Nrio Network. The system populates this window only when there are two or more Nrio modules on the network.

Active Schedule tab

This extension learns and assigns the active schedule to an output point. It may be used for multiple points.

Columns

Figure 332. Active Schedule tab

SaveManage ExtensionsPoint ManagerManual OverrideGo to Module

ConfigurationHistory SetupActive ScheduleLink ToLink From

Newly Assigned

Display Name	Usage	Status	Out Source	Out	Next Time	Next Value	To Display Path String
Boolean Schedule	Access Right	{ok}	Default Output	false {ok}	07-Oct-18 12:30 AM EDT	false {ok}	/Services/EnterpriseSecurityService/schedules/Boolean Sch

Unassigned

Display Name	Usage	Status	Out Source	Out	Next Time	Next Value	To Display Path String
Boolean Schedule	Access Right	{ok}	Default Output	false {ok}	07-Oct-18 12:30 AM EDT	false {ok}	/Services/EnterpriseSecurityService/schedules/Boolean Sch

You access this view by clicking **Controller Setup > Remote Devices > Remote Drivers**, followed by double-clicking the NrioNetwork row in the table, double-clicking a module row in the Nrio Device Manager view, clicking the **Point Manager** button, clicking the Digital Point tab, clicking the link to an output point, and clicking the Active Schedule tab.

Column	Description
Display Name	Displays the schedule name.
Usage	Displays the aspect of the system controlled by the schedule.
Status	Indicates the health of the schedule.
Out Source	Reports the current schedule’s source, such as “Week: Monday,” “Special Event: Christmas Break”
Out	Indicates the health of the output source.
Next Time	Indicates the next time an event is scheduled to occur.
Next Value	Indicates the expected value the next time the event occurs.
To Display Path String	Identifies the path in the station where the schedule is stored.

Link to tab

These learn mode tabs link points to other discovered points. This tab is available on multiple point extensions.

Figure 333. Nrio edit point view (showing Link To error)

ConfigurationHistory SetupActive ScheduleLink ToLink From

Newly Assigned

Display Name	Out	In10	In16	To Display Path String
Beeper	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 1/Reader 1/beeper

Unassigned

Page1of:

Display Name	Out	In10	In16	To Display Path String
Beeper	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 1/Reader 1/beeper
Beeper	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 2/Reader 2/beeper
Green	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 2/Reader 2/green
Green	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 1/Reader 1/green
Invalid Badge	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 1/Reader 1/invalidBadge
Invalid Badge	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 2/Reader 2/invalidBadge
Red	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 1/Reader 1/red
Red	false {ok} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/Door 2/Reader 2/red
Ro1	false {disabled,stale} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/ro1
Ro2	false {disabled,stale} @ def	- {null}	- {null}	/Drivers/Access Network/Remote Reader Module1/points/ro2

You access this view from the Nrio Point Manager by clicking the hyperlink next to a point on the Analog Points or Digital Points tab, followed by clicking the Link To tab.

Table 75. Link To columns

Column	Description
Display Name	Identifies the name of the point.
Out	Reports the Out value.
In10	Reports the In10 value.
In16	Reports the In16 value
To Display Path String	Reports the path to the point.

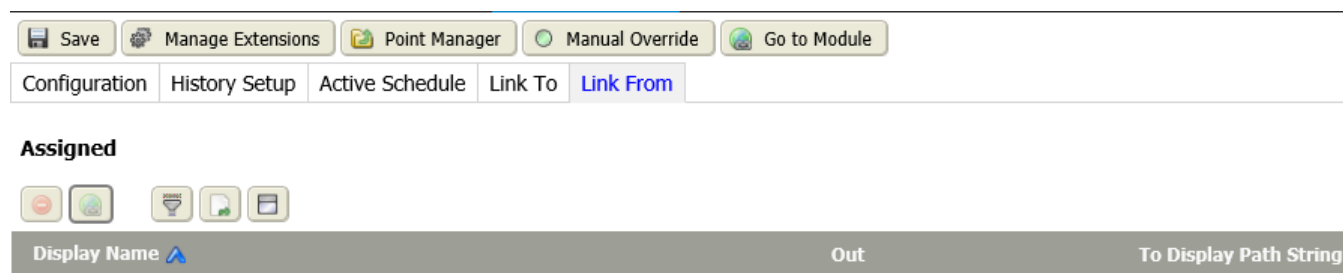
Link From tab

These learn mode tabs link from points to other discovered points. This tab is available for analog voltage output, and digital relay output points only. This tab is available on multiple point extensions.

442

March 25, 2025

**Figure 334.** Link From tab



You access this view from the Nrio Point Manager by clicking Digital Points tab, the hyperlink next to the Relay Output point, followed by clicking the Link From tab.

**Table 76.** Link From columns

Column	Description
Display Name	Identifies the name of the point.
Out	Reports the Out value.
To Display Path String	Reports the path to the point.

## History Extension view

This view configures each history extension.

## Properties

**Figure 335.** Example of a Numeric Cov History Ext view

Numeric Cov History Ext (history:NumericCovHistoryExt)	
Status	
Fault Cause	
Enabled	
Active Period	
Active	
History Name	
History Config	Interval: irregular, Record Type: numeric trend record, Capacity: 500 records, Full Policy: Roll »
Last Record	Interval: irregular, Record Type: numeric trend record, Capacity: 500 records, Full Policy: Roll ▼
Change Tolerance	Id     /
Precision	Source 0 Ords
Min Rollover Value	Time Zone NULL (+0) ▼
Max Rollover Value	Record Type history:NumericTrendRecord
	Capacity Record Count ▼ 500 records
	Full Policy Roll ▼
	Interval irregular ▼
	System Tags
	Edit
valueFacets	1. max=10 2. min=0 3. precision=1 4. units=V
minRolloverValue	<input checked="" type="checkbox"/> null 0.00
maxRolloverValue	<input checked="" type="checkbox"/> null 0.00
precision	32 bit ▼

Refresh Save

Edit

	Facet Key	Facet Value	
<input type="checkbox"/>	max	10	Add
<input type="checkbox"/>	min	0	
<input type="checkbox"/>	precision	1	Delete
<input type="checkbox"/>	units	volt (V) »	

Ok Cancel

The screen capture uses the Numeric Cov History Ext as an example view. The other extensions support similar properties.

You access this view from the Nrio Point Manager by clicking the hyperlink next to a point on the Analog Points or Digital Points tab, followed by clicking the History Setup tab and the history name hyperlink.

In addition to the standard properties (**Status**, **Fault Cause**, and **Enabled**), these properties support the history extension.

Property	Value	Description
Active Period	read-only	Indicates when data are being collected.
Active	true or false	Indicates if data collection is currently active, as defined by the <b>Active Period</b> properties.



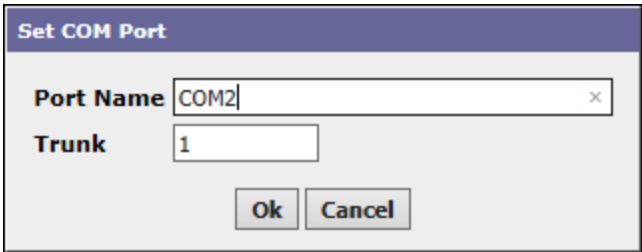
Property	Value	Description
History Name	wild card (%), defaults to % parent.name%	Names each history using a standardized formatting pattern. The default format automatically names histories with the name of the parent component and appends a sequential number to additional names, as necessary.
History Config, ID	read-only	Displays the value configured in the history extension's <b>History Name</b> property. An error string here indicates that the <b>History Name</b> property is incorrectly defined.
History Config, Source	read-only ORD	Displays the ORD of the active history extension.
History Config, Time Zone	read-only text	Displays the time zone of the active history extension.
History Config, Record Type	read-only text	Displays the data that the record holds in terms of: extension type (history) and data type (BooleanTrendRecord, numericTrendRecord, and so on).
History Config, Capacity	number, defaults to 500	Defines local storage capacity for histories.
History Config, Full Policy	drop-down list	Defines what happens when a history table reaches its maximum record count.
History Config, Interval	read-only, defaults to 500	Reports the number of records the system stores in the local station. In general, 500 or less is adequate for a controller station because local records are exported to the Supervisor station. A large number, such as 250,000 is acceptable for Supervisor stations. <i>Unlimited</i> is not recommended even for a Supervisor station.
History Config, System Tags	read-only	Reports any additional metadata (the System Tag) included in a history extension. Tags are separated by semicolons. Tags can be used to filter the import and export of histories.
History Config, valueFacets	read-only	Defines the units to use when displaying the data.
History Config, minRolloverValue	read-only	Reports the smallest difference between timestamped values


Property	Value	Description
		recorded.
History Config, maxRolloverValue	read-only	Reports the largest difference between timestamped values recorded.
History Config, precision	read-only	Reports the number of bits used for history data logging. The 64-bit option permits high precision, but consumes memory than 32-bit logging.
Last Record	read-only	Serves as a container for sub-properties that describe attributes of the last recorded change. The properties reported include date/time, time zone, the operation that generated the record, and the user who made the change.
Change Tolerance	Defaults to 0.00	Defines a value outside of which the system records a history record for each change of value. A change of value triggers a history record. To minimize the quantity of records created, you can configure the system to ignore changes that fall within the tolerance amount. If a change exceeds the <b>Change Tolerance</b> value, the system records a history record.
Precision	Defaults to 32	Reports the number of bits used for history data logging. The 64-bit option permits high precision, but consumes memory than 32-bit logging.
Min Rollover Value	read-only	Reports the smallest difference between timestamped values recorded.
Max Rollover Value	read-only	Reports the largest difference between timestamped values recorded.

### Set COM Port window

This window configures the COM port used by Nrio devices.

**Figure 336.** Set COM Port for Nrio devices

A dialog box titled "Set COM Port" with a purple header. It contains two input fields: "Port Name" with the text "COM2" and a small 'x' button to its right, and "Trunk" with the number "1". At the bottom are "Ok" and "Cancel" buttons.

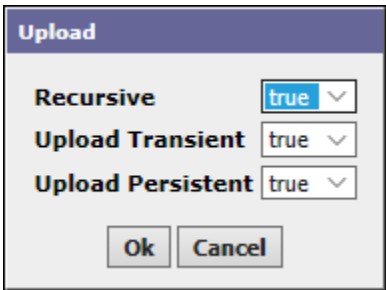
This window opens from the Nrio Device Manager when you click the Set COM Port button ().


Property	Value	Description
Port Name	text name of the port	Defines the communication port to use: none, COM2 or COM3.
Trunk	number	Specifies which trunk the port is connected to.  Each RS485 connection is called a trunk. If your network has multiple RS485 trunks, a separate network and remote I/O module are required to support each.

Upload window

The upload function reads transient (nvs) and persistent (ncis and cps) data from the device and writes them to the station database. This window selects the type of data to upload.

**Figure 337.** Upload window

A dialog box titled "Upload" with a purple header. It contains three dropdown menus: "Recursive" set to "true", "Upload Transient" set to "true", and "Upload Persistent" set to "true". At the bottom are "Ok" and "Cancel" buttons.

This window opens from the Nrio Device Manager when you click the Upload button ().

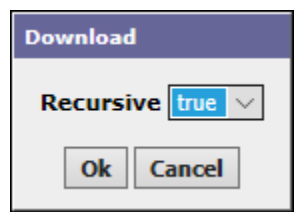
Typically, you leave the upload properties at their default settings of `true`.

Property	Value	Description
Recursive	true or false	Recursive data are data that may contain other values of the same type. These data define dynamic structures, such as lists and trees. Such data can dynamically grow in response to runtime requirements. The uploading of recursive data is always recommended.
Upload Transient	true or false	Transient data typically store current session information, which the system clears when it resets the device.
Upload Persistent	true or false	Persistent data are frequently accessed and not likely to be modified.

Download window

This window configures the Nrio download function, which writes data from the system database to the target device.

Figure 338. Download window



This window opens from the Nrio Device Manager when you click the Download button ()

The single download property turns the download function off (*false*) and on (*true*).

Typically, you leave this property at its default setting of *true*.

Filter window

This window defines search criteria for limiting the number of Nrio devices displayed in the Nrio Device Manager view.

**Figure 339.** Nrio Device Manager Filter window

Filter

☐ Display Name

%

Must Include

☒ Case Sensitive

☐ Enabled

false

☐ Status

%

Must Include

☒ Case Sensitive

☐ Device Type

☐ Uid

%

Must Include

☒ Case Sensitive

☐ Installed Version

%

Must Include

☒ Case Sensitive

☐ Available Version



%

Must Include

☒ Case Sensitive

Ok

Cancel

this window opens from the Nrio Device Manager view when you click the Filter button ( ).

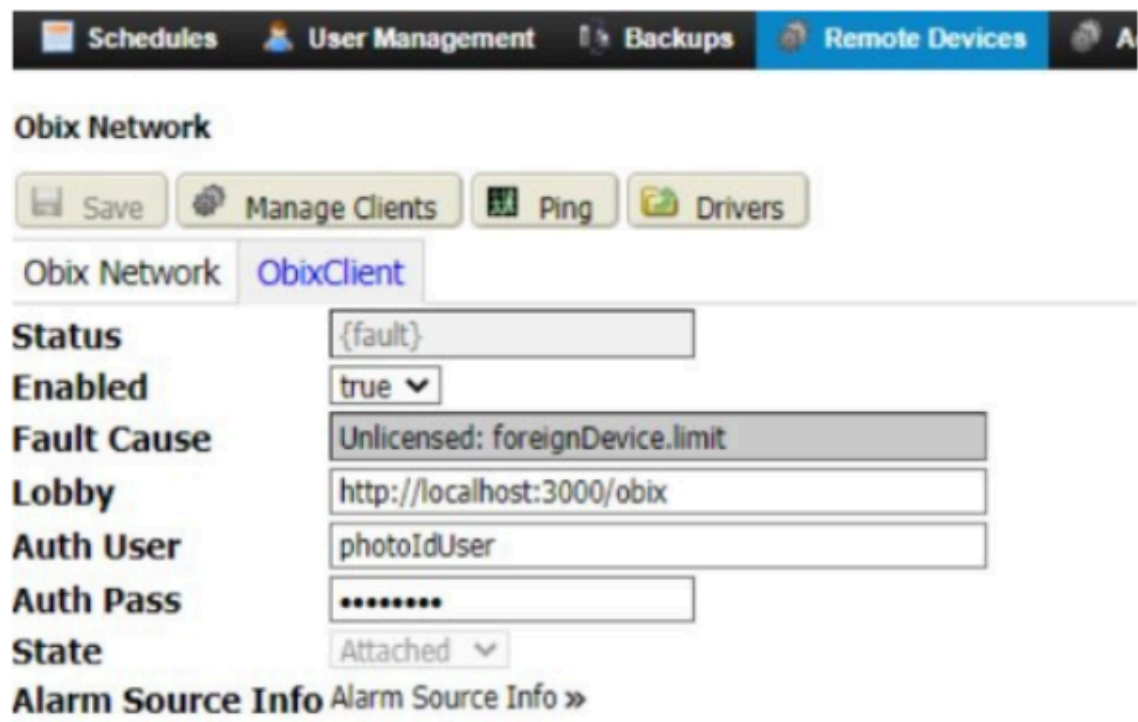
Property	Value	Description
Display Name	wild card (%)	Searches based on the name of the device.
Enabled	true or false	Searches based on if the device is currently enabled (true) or disabled (false).
Status	wild card (%)	Searches based on the current state of the device.
Device Type	Enums chooser	Searches based on the type of device (None, Base Board Reader, Remote Reader, Remote Input Output, Io16, Io16 V1, Io34, Io34sec).
Uid	wild card (%)	Searches based on the device's Universal ID.
Installed Version	wild card (%)	Searches based on the software version installed in the device.
Available Version	wild card (%)	Searches based on the software version.



# Chapter 16. Obix Network view

The Obix Network view includes tabs for configuring the Obix Network and Obix clients.

Figure 340. Obix Network view



You access this view from the Supervisor’s main menu by clicking **System Setup > Remote Devices > Remote Drivers** followed by double-clicking the Obix Network row in the drivers table. If the driver has not been added

yet to the view, click the Manage Devices button (  ) and add the Obix Network to the database. Add <http://localhost:3000/obix> as the lobby for ObixClient.

## Obix links

The control links appear across the top of the view.

These links include the following:

- **Save** updates any configuration changes made in the view.
- **Manage Clients** opens the Manage Clients window for adding, deleting, renaming, duplicating, copying or cutting, and pasting clients in the view.
- **Ping** initiates a job that pings the Obix Network and any clients under the network. The system displays job results (success or failure).
- **Drivers** links to the Drivers view.

The standard properties (**Status**, **Fault Cause**, and **Enabled**) support this driver.






# Chapter 17. Photo ID management

These views manage the applications that together issue photo ID badges and monitor building entry.

**NOTE:** The Photo ID Network is available to run in the Supervisor station. It does not run in a controller station.

If you have not added the driver to the Supervisor station, click **System Setup > Remote Devices > Remote Drivers**, click the Manage Devices button (  ) and add the Photo ID Network. This requires a station restart.

## Photo ID Network view




This view manages the applications that together issue photo ID badges and monitor building entry.


Database pane



Assuming the Photo ID Network is set up and the station has restarted, you access this view from the Supervisor’s main menu by clicking **Photo ID**

In addition to the standard control buttons (Hyperlink, Delete, Rename, Filter, Reports, and Export), the Photo ID Network pane contains these specific buttons:

-  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 point values as well as properties provided by the database.
-  Manage Devices/Drivers opens the Manage Drivers or Manage Devices window, which is used to Add, Delete, Rename, Duplicate, Copy, and Cut system drivers or devices.
-  Settings opens the Photo ID Settings window.

-  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

In addition to the standard control buttons (Filter and Export), the Photo ID Network pane contains these specific buttons:



-  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.)

Photo ID Add device window

This window configures the properties of a new PhotoID device.

Figure 341. PhotoID Add Device window

Add Device

Device Type

Asure ID Client Device

Name

Asure ID Client Device


Host Name

Entsec AsureID Port

3001

Ok

Cancel

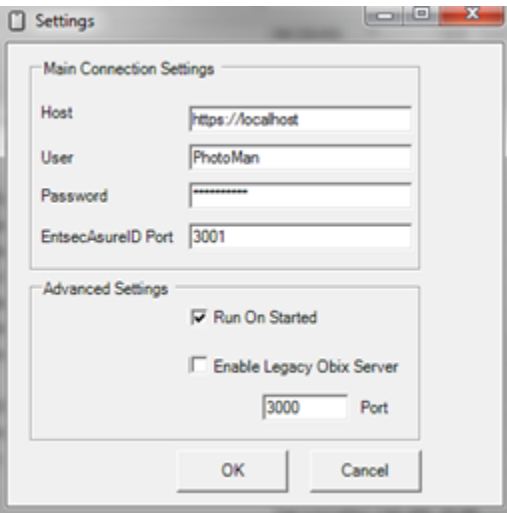
You access this view from the Supervisor’s main menu by clicking **Photo ID** followed by clicking the Manage Devices button () , clicking Add, selecting the Asure Id Client Device, and clicking **Ok**.

Property	Value	Description
Device Type	read-only	Identifies the type of device: server or client.
Name	text	Provides a unique name for the Asure ID Device.
Host Name	text	Defines the IP address and path

Property	Value	Description
		to the video server. It is required for HTML5 streaming and to record motion-detected video.
Entsec AsureID Port	number (defaults to 3000)	Identifies the port used for the EntsecAsureId connector.

Settings window

Use this window to establish the connection between the Obix Network and the EntsecAsureID running in the Photo ID workstation.



To open this window on the Photo ID workstation, right-click the EntsecAsureID icon (🖥️) in the system tray, and select the Settings menu option.

Property	Value	Description
Host	https://<frameworkStation> or http://<frameworkStation>	Defines the address of the PC or remote controller that is running the <frameworkStation>, where <frameworkStation> is an IP address or URL. You can use localhost if the Photo ID workstation shares the same platform as the framework Supervisor station.  Secure communication (https:) is the recommended approach. Http: is not secure. Using it exposes your system to being hacked.
User, Password	text	Define the login credentials for the

Property	Value	Description
		Obix Network connection as configured in the station by the oBIX user and role.
EntsecAsureID Port	number	Defines the port number for oBIX host communication.
Run On Started	check box	When enabled, starts the applet when the host computer starts. This can also be set from the EntsecAsureID menu. You should enable this property.
Enable Legacy Obix Server	check box	Turns on and off support for legacy oBIX operations.

Configure window

This window configures the photographs taken by the camera.

Configure

Default Image Ratio

Ratio

width: 3

height: 4

Default Image Format

JPG

Max Image File Size

5000

KB [1 - +inf]

PhotoID Timeout

00000

h

00

m

00

.

000

s [0ms - +inf]

PhotoID Format

%lastPersonName%

%validateTimestamp%


%lastBadgeActivity%

Photo I D Font Size

17

Ok

Cancel

This window opens when you click the Settings button () on the Photo ID Network view.

Property	Value	Description
Default Image Ratio	drop-down list and numeric fields.	Controls the aspect ratio of the photograph:  Ratio sets the default ratio for

Property	Value	Description
		photos created to conform to the photo property defined by the Asure ID template. <i>Freehand</i> allows the person taking the photo to use the freehand tool to crop the photo.
Default Image Format	drop-down list	Defines the default format: JPG or PNG. You can still use the other format for individual photos.
Max Image File Size	number (defaults to 5000 KB)	Defines the maximum size of the photo. Photos, especially those uploaded from another source, cause an error if the exceed this size.
PhotoID Timeout	hours, minutes, seconds	Controls how long a photo remains visible for surveillance purposes. The default is 0 (zero), which indicates no timeout. Set this value so that you are always monitoring current activity.
PhotoID Format	text	Controls the text that appears along with the photo. This feature uses standard BFormat notation.
Photo Id Font Size	printer's points	Controls the size of the font used to display the text that appears along with the photo.

Asure ID Client Device view

This view configures Asure ID as a client device of the Photo ID station (the server).

Links

Figure 342. Asure ID Client Device tab

Home

Monitoring

Personnel

Reports

System Setup

Photo

Save

Ping

Photo ID Network

Asure ID Client Device

Templates

Status

{down,alarm,unackedAl

Enabled

true

Fault Cause

Health

Fail [07-Sep-18 1:15 PM EDT] AsureIDClient has not been identified

Alarm Source Info

Alarm Source Info >>

Key

Host Name

Entsec AsureID Port

3001

Timeout

+ 00000 h 01 m 00 s

<

>

You access this view from the Supervisor’s main menu by clicking **Photo ID** followed by double-clicking the Asure ID Client Device row in the Photo ID Network table.

In addition to the Save link, these links support the Asure ID client device.

- Ping sends a message to the device to confirm that it is on line.
- Photo ID Network returns to the Photo ID Network view.

Properties

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support an Asure ID client device.

Property	Value	Description
Key	read-only	Displays a unique identifier for a particular EntsecAsureID (non-legacy) device and is provided automatically during discovery. After manually adding the EntsecAsureID device, you match with the discovered device to populate this property.
Host Name	text	Defines the IP address and path to the video server. It is required for HTML5 streaming and to record motion-detected video.

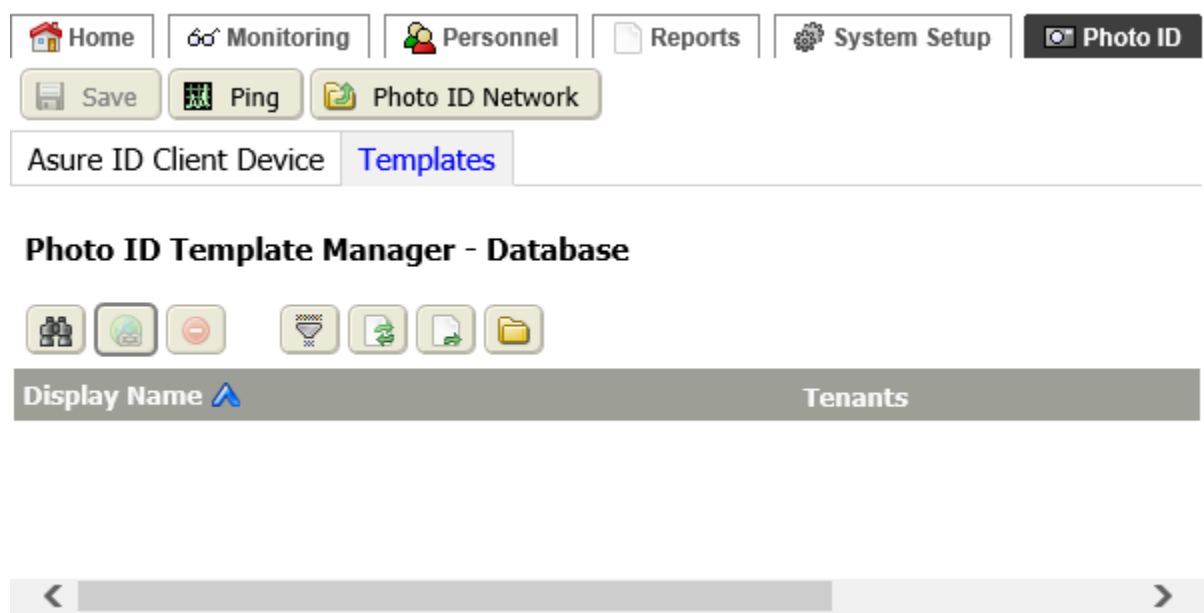
Property	Value	Description
EntsecAsureID Port	text	Identifies the port used for the EntsecAsureID connector.
Timeout	hours minutes seconds	Defines how long to wait for network communication to begin before returning a fault.

Templates tab

This view opens the Photo ID Template Manager - Database view. This discovery view locates Asure ID templates to add to the database.

Links

Figure 343. Templates tab



You access this view from the Supervisor’s main menu by clicking **Photo ID**, double-clicking the Asure ID Client Device row in the table and clicking the Templates tab.

Use this tab to discover the template(s) created using the Asure ID software.



**NOTE:** Once a template is found and associated with a tenant, do not change the name of the template file. Renaming a template removes the associated tenant.

In addition to the Save link, these links support the Asure ID client device.

- **Ping** sends a message to the device to confirm that it is on line.
- **Photo ID Network** returns to the Photo ID Network view.

Buttons

In addition to the standard buttons (Discover, Delete, Filter, Refresh, and Export), these buttons support Asure ID templates in the Database pane.

-  Hyperlink opens the Badge view for the selected template.
-  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.).

In addition to the standard buttons (Add, Filter, and Export), the Match button () in the Discovered pane associates a discovered template with one that is already in the database.

Columns

Column	Description
Display Name	Identifies the template.
Tenants	Indicates the tenants to which it applies.

Asure ID Device.[template] view

This view opens a set of tabs for configuring badge templates. It opens to the Template Data tab.

You access this view from the Supervisor’s main menu by clicking **Photo ID**, followed by double-clicking the Asure ID Client Device row in the Photo ID Network table, and clicking the Templates tab.

The Template Data tab is a discovery view. You use it to discover new properties to add to the selected template. To edit a property, double-click its row in the table.




Tenants tab

This tab on the Photo ID badge view lists the tenants assigned to the selected template.

Buttons

You access this tab from the main menu by clicking **Photo ID** followed by double-clicking the Asure ID Client Device row in the Photo ID Network table, clicking the Templates tab, double-clicking a template row in the table, and clicking the Tenants tab.

In addition to the standard buttons in the Database pane (Unassign, Filter, and Export), these buttons support associating tenants with Asure ID templates.

-  Summary displays the tenant details as entered in using the Personnel views.
-  Hyperlink opens the tenant information for editing.
-  Assign Mode buttons open and close the Unassigned pane.

Badges tab




This tab lists the badges to which the selected template has already been assigned. This is a discovery view. Use it to discover unassigned badges and assign them to this template.

Buttons

You access this tab from the main menu by clicking **Photo ID** followed by double-clicking the Asure ID Client Device row in the Photo ID Network table, clicking the Templates tab, double-clicking a template row in the table, and clicking the Badges tab.

In addition to the standard buttons in the Database pane (Unassign, Filter, and Export), these buttons support associating tenants with Asure ID templates.



-  Summary displays the badge details as entered in using the Personnel views.
-  Hyperlink opens the individual badge information for editing.
-  Assign Mode buttons open and close the Unassigned pane.

Edit Photo ID Template Data view

This view edits the data that is bound to a template.

You access this view from the Supervisor’s main menu by clicking **Photo ID** followed by double-clicking the Asure ID Client Device row in the Photo ID Network table, clicking the Templates tab, and double-clicking a template row in the Template Data view table.

The title of the view is the name of the data item (property) you are editing. For example, the data item may be “First Name,” “Last Name,” or “Department.” The properties in this view vary depending on the data item. Some properties include:

Property	Value	Description
Data Type	read-only	Identifies the type of data.
Data Binding	drop-down list	Provides related options. The first property you select provides appropriate options for the second property.
Image Ratio	drop-down list, width and height	Configures the aspect ratio for a photograph.
Image Format	drop-down list	Identifies the file type for the photograph.

Photo ID Viewers view

This view associates a viewer with a camera and reader.

Buttons

Home

Monitoring

Personnel





Reports





System Setup

Photo ID

Photo ID Network

Photo ID Viewers







Display Name	Cameras	Readers
PhotoIDViewer	-	-
PhotoIDViewer1	-	-

You access this view from the main Supervisor menu by clicking **Photo ID > Photo ID Viewers**.

In addition to the standard buttons (Delete, Rename, Column Chooser, Filter, Manage Reports, and Export), these buttons support Photo ID viewers.

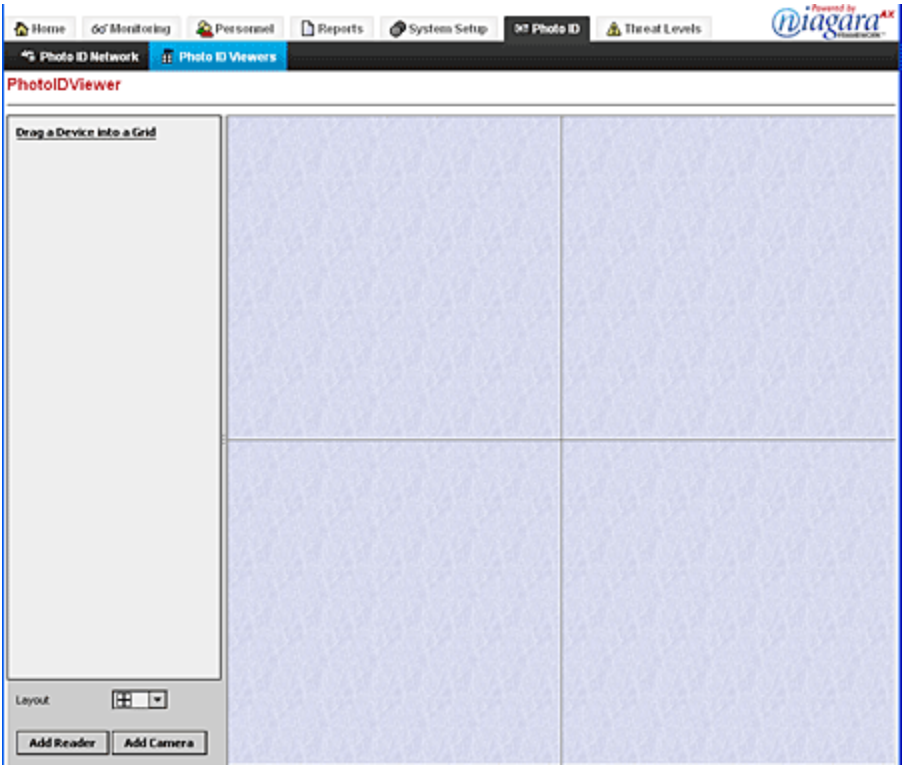
-  Add adds a new Photo ID viewer.
-  Hyperlink opens the viewer.

Columns

Column	Description
Display Name	Identifies the viewer.
Cameras	Shows the cameras whose feeds are visible from the viewer.
Readers	Shows the readers associated with the viewer.

Photo ID Viewer (surveillance) view

This view provides a pre-configured grid with various layout options for displaying all available video cameras and readers. The layout options display up to nine devices on a single view.



Cameras show video. If Photo ID badges are enabled, readers show the photo ID of the person who used the reader. Using video and reader views together an operator can verify that the person entering (as seen by the video camera) is the same person who scanned the Photo ID badge.

Camera, reader list pane

The top left corner lists the cameras and readers connected to the station. Supervisor stations show all readers in the Supervisor database. You drag cameras and readers from this list to the camera-layout pane. The list

pane contains these controls:

- The **Layout** drop-down list determines the layout pane configuration.
- The Reader button opens the Add Reader window, which provides a list of all available readers. The system adds the readers you select to the list pane.
- The Camera button opens the Add Camera window, which provides a list of all available cameras. The system adds the camera(s) you select to the list pane.

#### Right-click menu options in the list pane

- To remove a camera or reader from the list, right-click the device name in the list and click **Remove**.
- To remove a device from the layout pane, right-click the device name in the list and click **Remove from View**. The device name continues to appear in the list.

#### Camera layout pane

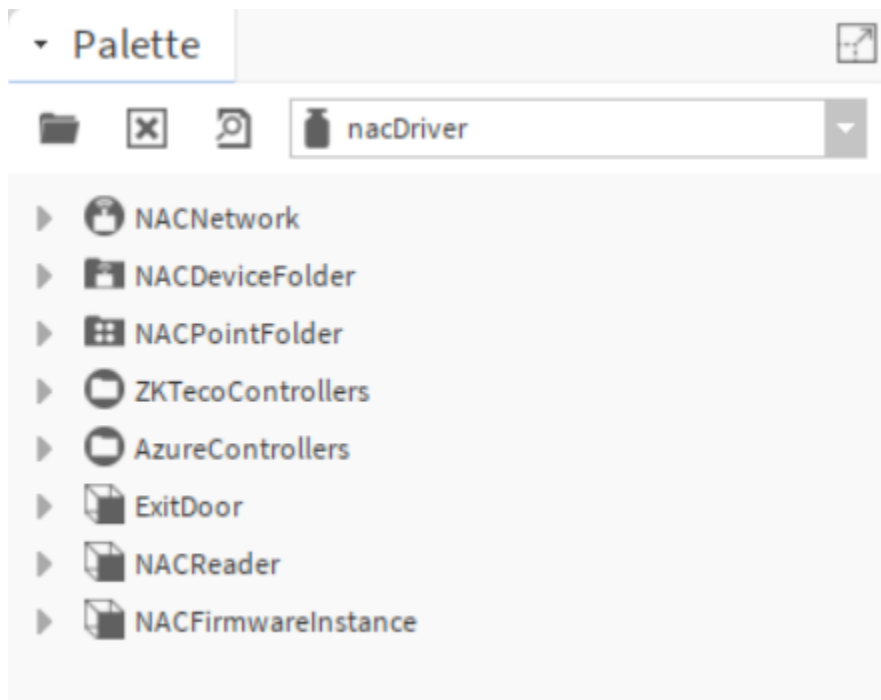
This pane shows a grid for displaying video views. This pane changes according to the option you select using the **Layout** property.



# Chapter 18. Components NAC Driver Module

These views, tabs, and windows configure NAC Driver within a building. These topics also document NAC Driver and device details.

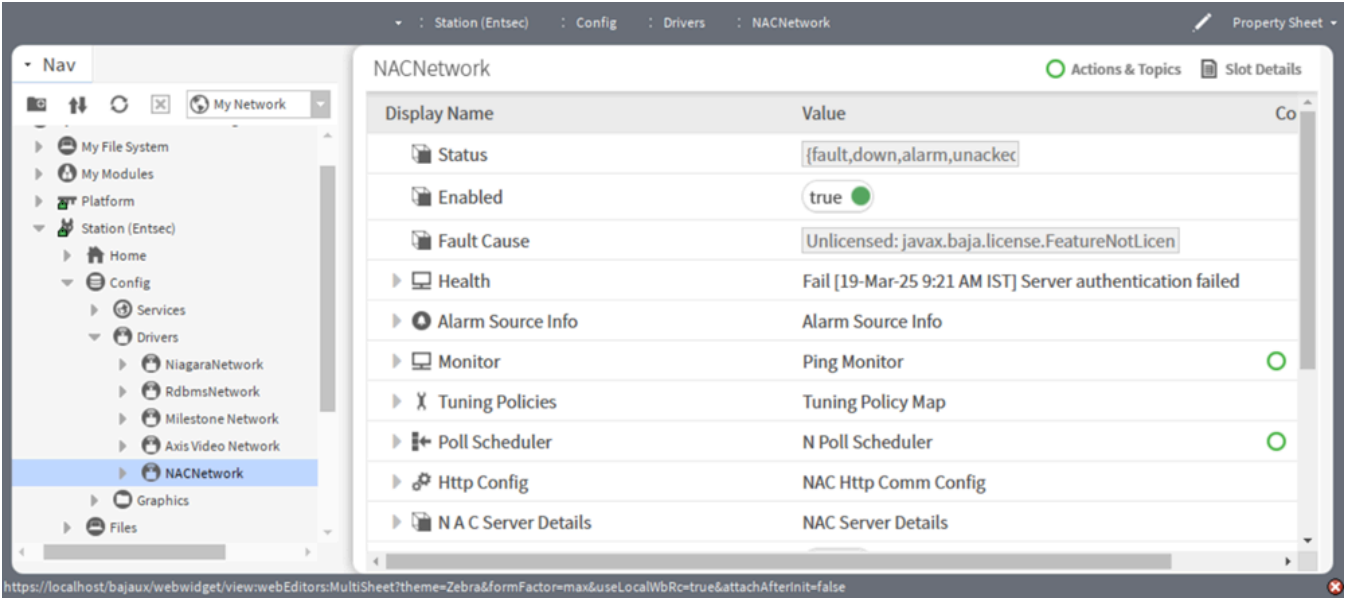
**Figure 344.** NAC Driver



## nacDriver-NACNetwork

The component provides the network configuration property for the NAC Driver.

Figure 345. NAC Network Property Sheet



- Component Location:nacDriver Palette
- To access these properties, expand **Config > Drivers > NAC Network** and right click the controller **Views > Property sheet**.
- Other than the standard properties (status, enabled, fault cause, health, Alarm Info, and poll frequency) these property supports the controller component.
- The configuration of these properties varies depending on where it is in the station.

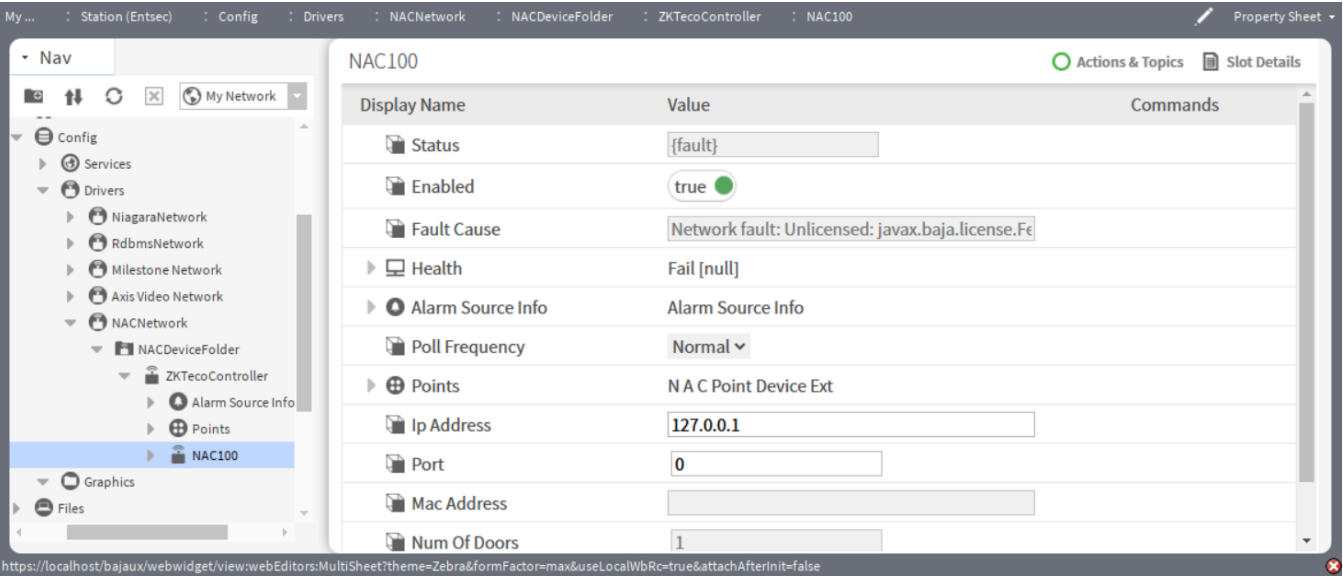
Property	Value	Description
Http Config	Additional Properties	Configuration like IP Address and port which are required to connect to the NAC server.
NAC Server Details	Server Credentials	Expand the NAC Server Details and update network credentials for the NAC network, Refer to NAC Server for more details.
Syncing To Server	False(default) or true	Displays true when the sync operation is performed by the network component.
Replication	Read Only	Expand the Replication Section to review the last replication status for NAC Network, Refer to NAC Replication for more details.
NAC Dev Change Worker	Read Only	Reports timestamp of last dev state record processed.
NAC Event Worker	Read Only	Reports timestamp of last Event record processed.

Property	Value	Description
Card Pin Template	Read Only	Stores default card pin template on adding NAC network component.
NAC Firmware Instance Container	Folder container NAC Firmware Instance component	<p>This folder consists of standard NAC firmware Instance components, used to store the required NAC firmware version in the Niagara Access Server.</p> <p>Refer to NAC Firmware Instance Container for more details.</p>
NAC Door Mode Schedules	The folder space contains NAC Door mode schedule	This component view lists all the NAC Door Mode schedules used for overriding door modes. Refer NAC Door Mode Schedules section for more details.

nacDriver-NACController

This component explains how to configure the NAC Controller.

Figure 346. NAC Controller Property Sheet



- Component Location:nacDriver Palette
- To access these properties, expand **Config > Drivers > NAC Network > NAC Device > NAC Controller** and right click the controller **Views > Property sheet**.
- Other than the standard properties (status, enabled, fault cause, health, Alarm Info, and poll frequency) these property supports the controller component.

Property	Value	Description
Points	Door, Reader, and other points of property	The folder space consists of NAC sensor points, NAC Device points

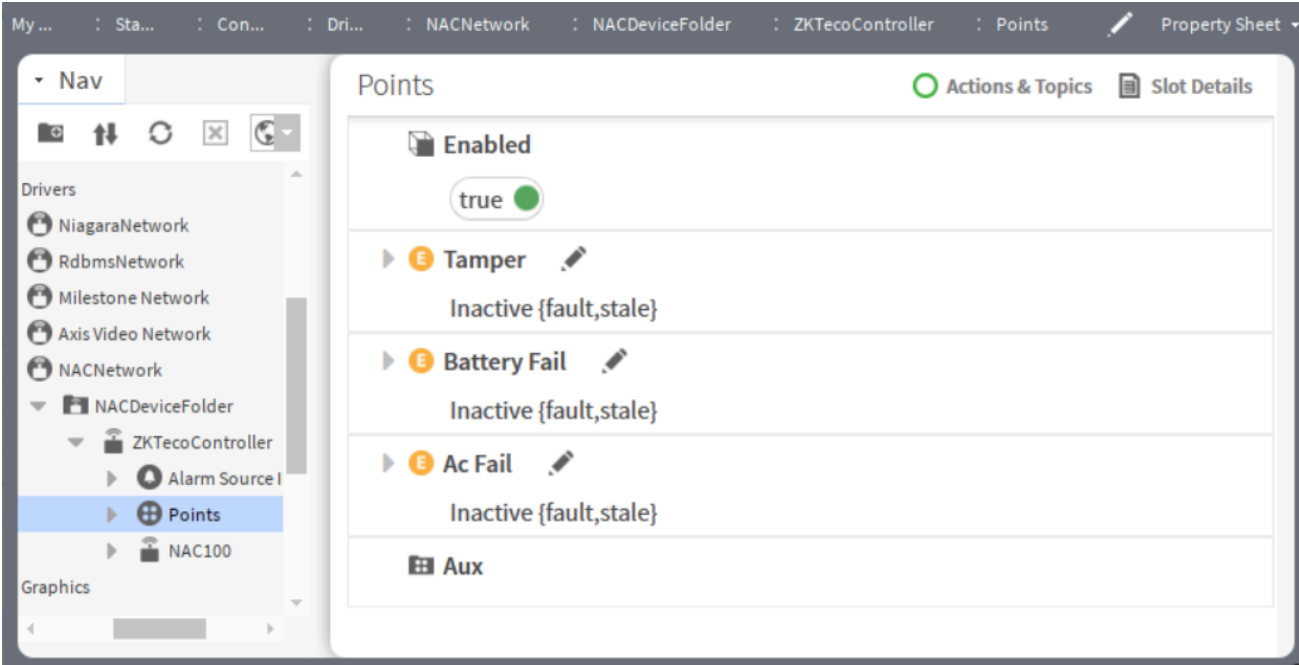
Property	Value	Description
		and multiple door component based on the controller type (1, 2, 4 Door Components). Refer Points Section for more details
IP Address	Read-only	Defines the IP address or host and port of the NAC Controller. The location can be on the network or elsewhere available on an intranet or the internet
Port	Read-only	Network port of the controller (all controllers would be updated with 443 by default)
Mac Address	Read-only	Corresponds to the MAC Address of the controller
Number of Doors	Read-only	Reports the Controller type like 1 Door, 2 Door or 4 Door and the maximum number of doors supported by the controller
Firmware version	Read-only	Represents standard controller firmware version

## nacDriver- Nac Point

Each controller comprises a single point container, an NAC Point Device Extension, or an Azure Point Device Extension. The NAC Point Device Extension or Azure Point Device Extension includes multiple NAC Sensor Points, an Auxiliary Container, and several Door Components.



• **Figure 347.** NAC Point Folder



- Component Location:nacDriver Palette
- To access these properties, expand

Config > Drivers > NAC Network > NAC Device > NAC Controller and right-click the Points folder Views > Property sheet

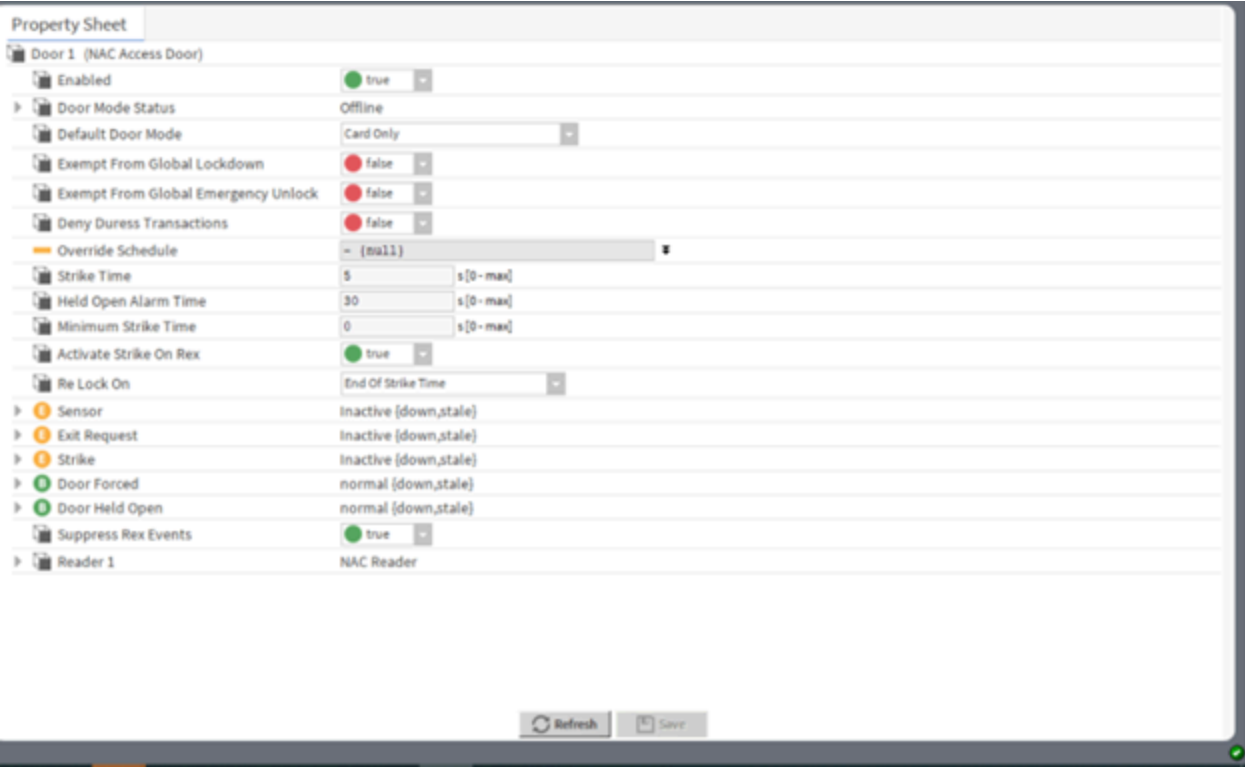
Tamper (NAC Sensor point)	Read-only Inactive(default) and Active state	<p>An Input on a Controller configured to detect physical tampering. With a case, enclosure, etc., it generates an alarm if the device is tampered with.</p> <p>Alarm states are Tamper (Active) and Tamper Restored (Inactive).</p> <p>Refer to the NAC Sensor point for a detailed description.</p>
Battery Fail (NAC Sensor point)	Read only Inactive (default) and Active state	<p>An Input on a Controller is configured to detect whether a battery is connected. Reports the Fault state of the controller by updating the status as Active and generates an alarm if a battery fault is detected. Alarm states are Battery Failure (Active) and Tamper Restored (Inactive) states. Refer to the NAC Sensor point detailed description.</p>
AC Fail (NAC Sensor point)	Read only Inactive (default) and Active state	<p>An Input on a Controller is configured to detect whether the main power is connected.</p>

		<p>Triggers Alarm if there is a power failure. Alarm states are Power off (Active) and power on (Inactive).</p> <p>Refer to the NAC Sensor point for a detailed description.</p>
AUX container	Folder Space	<p>Contains Auxiliary input and Auxiliary output points of the controller.</p> <p>Refer Auxiliary IO section for detailed information</p>
Door	NAC Door Component	<p>Contains a combination of Reader(s), Input(s), and Output(s) which electronically controls access to a physical door, or something functionally like a door in Niagara (Access network), also known as Access Point.</p> <p>Refer Niagara Access door for detailed description.</p>

**nacDriver nacDoor**

The component provides the door configuration property for the **NAC Driver**. By default, the Controller component includes a single Door component, which is equipped with a **nacReader** component, as well as **NACDevicePoint**, **NACStrikePoint**, and **NACSensorPoint** elements.

Figure 348. NAC Door Property Sheet



- Component Location:nacDriver Palette
- To access these properties, expand **Config > Drivers > NAC Network** and right-click the Controller **Door > Views > Property sheet**.
- Other than the standard properties (Enabled and Door Mode Status) these property supports the controller component.
- If a door needs to be configured as an Exit Door, the Exit Door Extension must be added from the Palette.

Property	Value	Description
Default Door Mode	drop-down list	Contains door modes to access the door like Card and Pin, Facility Code Only, Card and Bio, Card and Bio and Pin, Bio and Pin, Bio Only, etc.
Exempt From Global Lockdown	true or false (default)	Specifies a particular door that is excluded from auto-locking after it is opened.
Exempt From Global Emergency Unlock	true or false (default)	Specifies a particular door to exclude from the emergency unlock doors.
Deny Duress Transactions	true or false (default)	Allows to open the door if more pressure applied.
Override Schedule	null (default), true or false	When null is enabled, reports the incoming value from the device.

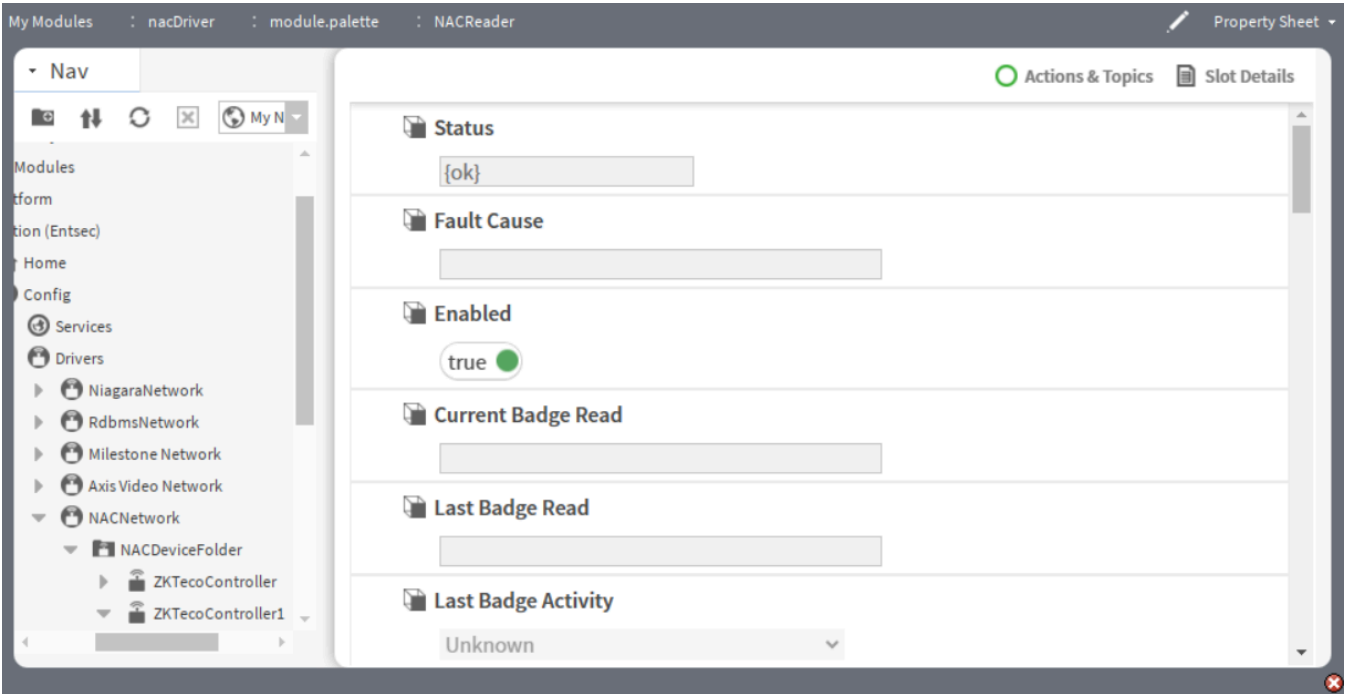
Property	Value	Description
		<p>You cannot change this value.</p> <p>To change this value, click the double-arrow to the right and remove the null check mark.</p>
Strike Time	hours minutes seconds (defaults to 5 seconds)	Sets the duration for the card swipe, ensuring it is maintained for the specified amount of time.
Held Open Alarm Time	hours minutes seconds (defaults to 30 seconds)	Configures how long the door may be held open before an alarm condition manifests.
Minimum Strike Time	hours minutes seconds (defaults to 0 seconds)	The card swipe must be maintained for at least the minimum specified duration
Activate Strike on Rex	true (default) or false	The strike is activated when a Request to Exit is initiated.
Re Lock On	drop-down list	<p>Defines what should happen with a door that has just been unlocked.</p> <p>Relock on the End of Strike Time, and locks the door as soon as strike time ends.</p> <p>Relock on Door Open, lock the door as soon as it unlocks. Relock on Door Close, lock the door either after the Access Unlock Time expires (if the door has been unlocked but not opened) or when the door closes.</p>
Sensor	Additional properties	Sensors are contact devices that monitor the state of a door
Exit Request	Additional properties	Normal exit from an access zone. Exit requests are devices that provide access to leave through a door without having to present a badge/card.
Strike	Additional properties	Defines the state of the door like lock is released or not
Door Forced	Additional properties	Configures the Door Forced Extension to set the alarm-related properties.
Door Held Open	Additional properties	Configures the Door Held Open

Property	Value	Description
		Extension to set the alarm-related properties.
Suppress Rex Event	true (default) or false	Suppresses the Exit Request events.
Reader	additional properties	This component is documented in a separate topic.

nacDriver-nacReader

The component provides the reader configuration property for the NAC Driver.

Figure 349. Nac Reader Property Sheet



- Component Location:nacDriver Palette
- To access these properties, expand Config > Drivers > NAC Network and right-click the controller Door > Views > Property sheet.
- Other than the standard properties (status, enabled, fault cause) these property supports the controller component.

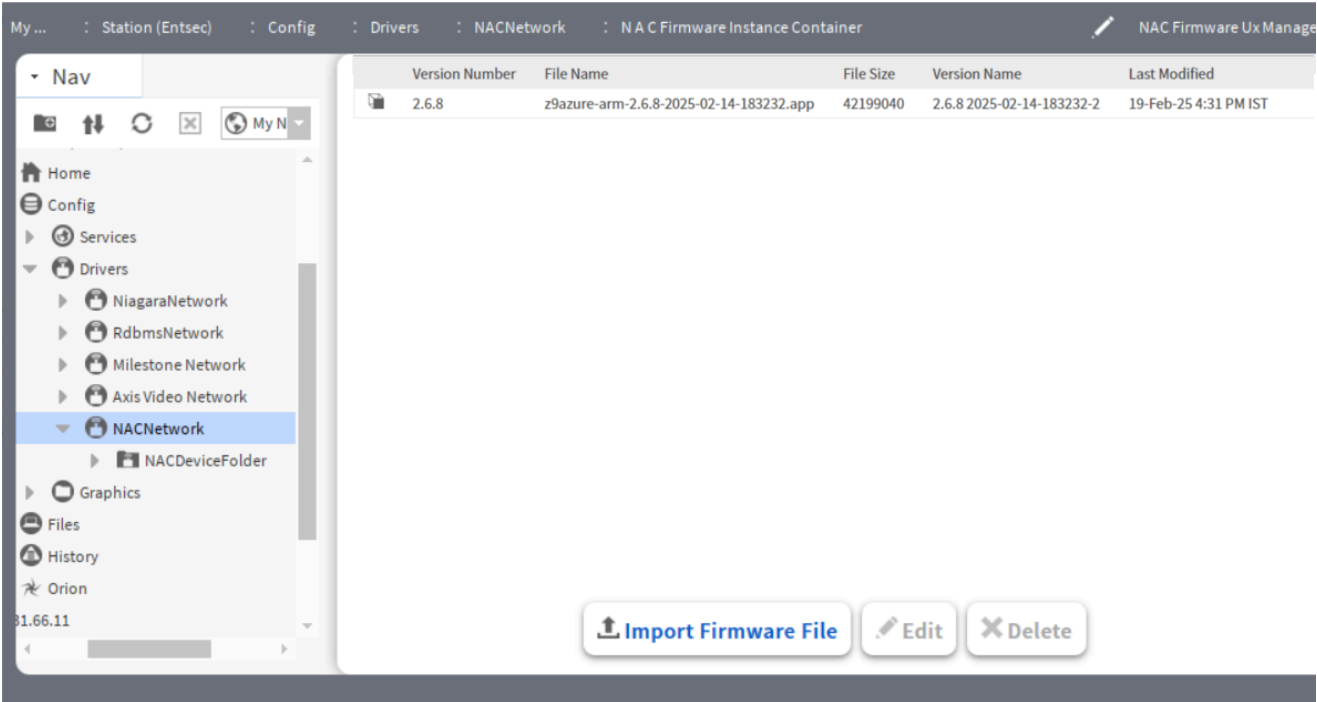
Property	Value	Description
Current Badge Read	read-only	Reports the number of the badge being processed now.
Last Badge Read	read-only	Reports the number of the last-read badge.
Last Badge Activity	read-only	Reports the last read or write using a badge.

Property	Value	Description
Last Person Name	read-only	Reports the owner of the last badge read.
Last Person Id	read-only	Reports the ID of the owner of the last badge read.
Validate Timestamp	read-only	Reports when the system validated the badge.
Reader Type	drop-down	Allows to choose protocol as per controllers between O S D P and Wiegand format to read card data.
Attendance	drop-down	Allows selection of options: <i>None</i> , <i>Check In</i> , and <i>Check Out</i> for recording attendance.
Address	number	Address for specific reader.
O S D P Address	number	Address of OSDP, if the reader is O S D P type.
Firmware Version	read-only	Displays current firmware version installed on controller.
Led Type	drop-down	The LED activates upon a card swipe, displaying either Green or a combination of Red and Green.
Assignment	read-only	Shows which door is assigned to the reader.
Reader Tamper	additional properties	Sets up the Reader Tamper Extension to define alarm-related properties in case the reader is tampered with.
Prevent Remove	false (default)	If the remove action is executed on a controller with an encrypted connection, a window appears to confirm whether or not to proceed with the removal.
Alarm Info	additional properties	Standard alarm-AlarmSourceInfo component.
Activity alert extensions	additional properties	Standard accessDriver-ActivityAlertExt. Each has the same set of alarm source info.

## nacDriver-NACFirmwareInstanceContainer

The component view consists of a list of **nacFirmwareInstance** components along with properties like **versionNumber**, **Filename**, and **Filesize**.

Figure 350. NAC Firmware Instance Property Sheet



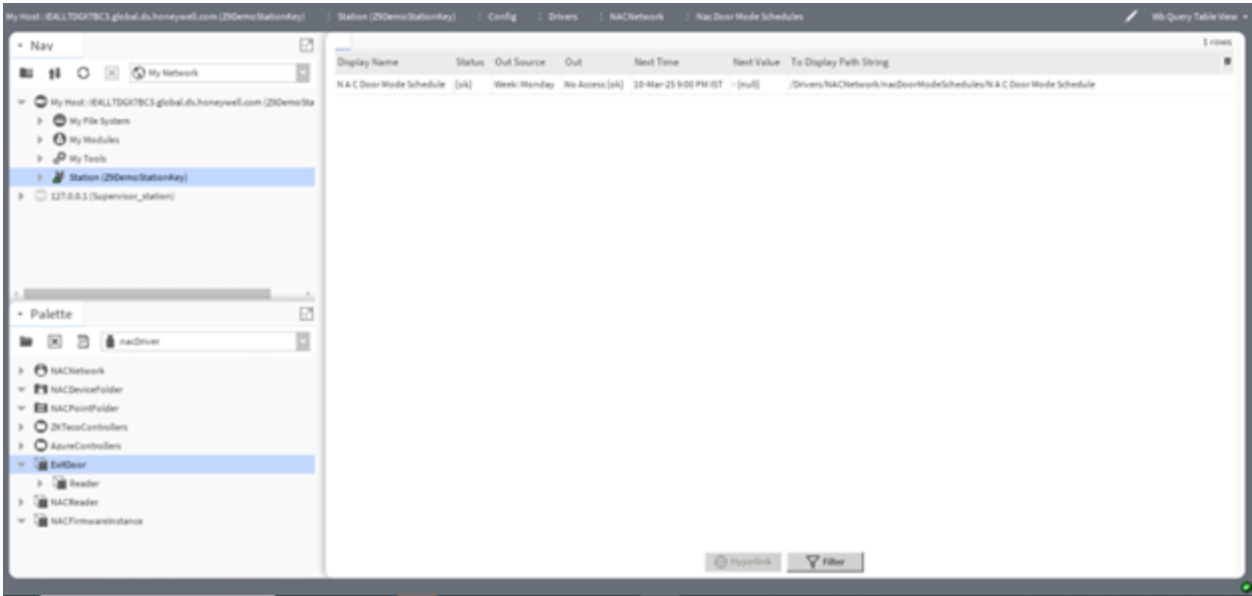
- Component Location:nacDriver Palette
- To access these properties, expand Config > Drivers > NAC Network > Views > NACProperty Sheet > NAC Firmware Instance Container .

Property	Value	Description
Version Number	read-only	Reports the version number of the firmware file uploaded.
File Name	read-only	Reports the last uploaded file name.
File Size	read-only	Reports the actual file size of the uploaded firmware instance.
Version Name	read-only	Reports the owner of the last badge read.
Last Modified	read-only	Reports the ID of the owner of the last badge read.

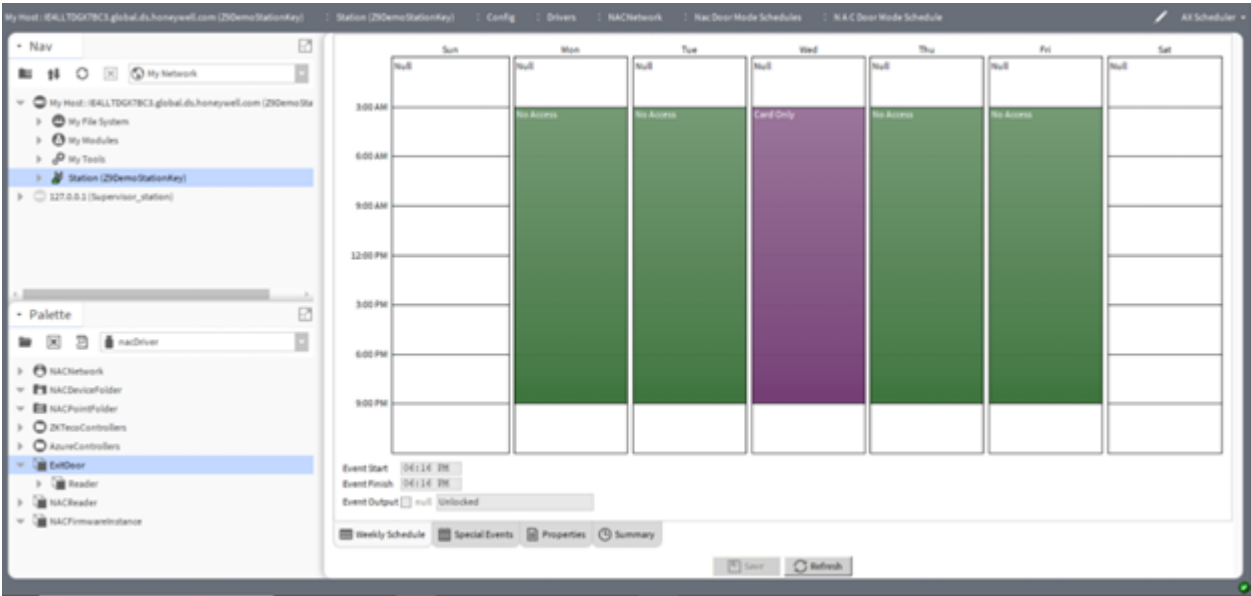
nacDriver-nacDoorModeSchedule

The view consists of a list of Door Mode schedules and configurations property for NAC Driver.

• **Figure 351.** NAC Door Mode Schedule



The Door Mode Schedule components consist of schedule property for updating the door access configurations as shown below :

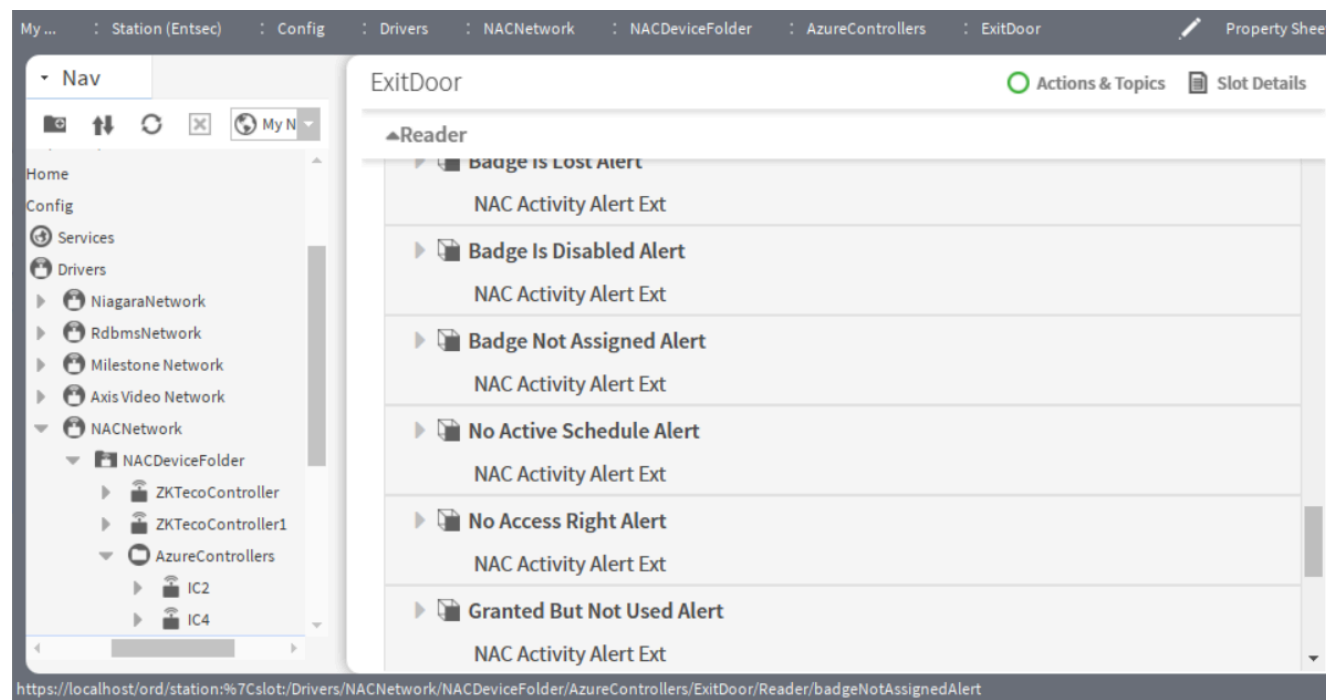


**nacDriver-nacActivityAlertView**

Each nacReader component consists of different alert extensions to invoke alarms.



Figure 352. Activity Alert View



- Component Location:nacDriver Palette
- To access these properties, expand **Config > Drivers > NAC Network > NAC Device > NAC Controller** and right click the controller **Views > Property sheet > Exit Door**.

Property	Value	Description
Activity Type	read-only	Identifies the type of activity that generates the alert.
[alert]	additional properties	This is a standard alarm-AlarmSourceInfo component
Enable logging	true (default) or false	Turns activity logging on and off
Enable Alert	true (default) or false	Turns alert on and off.