

Technical Document

Niagara Enterprise Security Reference

April 23, 2020

niagara⁴

Niagara Enterprise Security Reference

Tridium, Inc.

3951 Westerre 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 © 2020 Tridium, Inc. All rights reserved.

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

Contents

About this reference	15
Document change log	15
Related documentation	16
Chapter 1 Home	17
Standard control buttons	17
Column Chooser view.....	19
Controller (System) Setup views.....	20
User interface	21
Graphics configuration	21
Standard properties	24
Chapter 2 Monitoring views	25
Alarm Console — ConsoleRecipient view	25
Alarm Console control buttons	26
Alarm Console columns	27
Alarm Console Info icons	28
Alarm Console links	28
Show Alarm Details window.....	29
Notes window.....	30
Alarm Filter window	31
Multi Source View Options window	32
AX Alarm console.....	33
Console Layout window.....	34
Activity Monitor view.....	35
Edit (configure) Activity Monitor view, Activity Monitor tab.....	38
Activity Monitor Alarm Classes tab.....	38
Activity Monitor Filter window	39
Video monitoring views	40
Surveillance viewer	40
Playback viewer	41
Chapter 3 Personnel views	45
People view	45
Quick Edit window	47
People View Filter window.....	47
Add New (or edit) Person view.....	48
New person Summary tab.....	50
New Person Access Rights tab.....	51
Change Assignment Properties window	52
Access Rights Summary window	52
Add Access Rights filter window	53
Badges tab	54
Badges Summary tab.....	55
Badges view.....	56
Quick Edit window	57

- Badges Filter window 58
- Enroll New Badge view 59
 - Enroll New Badge Summary tab 59
- Add (or edit) New Badge view 60
 - Add New Badge Summary tab 62
 - Badge tab 62
- Batch Enroll Badges view, Badge tab 63
 - Batch Enroll Summary tab 64
- Range Create Badges view, Badge tab 65
 - Range Create Badges Summary tab 66
- Access Rights view 67
 - Access Rights Summary tab 68
 - Quick Edit window 69
 - Filter window 70
- Add New (and edit) Access Rights view, Access Right tab 71
 - People tab 72
 - Readers tab 73
 - Readers tab, Summary window 74
 - Readers tab, Filter window 75
 - Floors tab 75
 - Floors tab, Filter window 76
- Tenants view 77
 - Tenants Summary window/tab 78
 - Filter window 78
- Add (or edit) a New Tenant view 79
 - Tenants Niagara Integration IDs tab 79
 - Tenants Intrusion Pins tab 80
 - Tenants People tab 80
 - Tenants Badges tab 81
 - Tenants Threat Level Groups tab 82
 - Tenants Access Rights tab 83
- Additional Personnel Data view 84
 - Additional Personnel Data Summary window/tab 84
 - Additional Personnel Data Filter window 85
- Add (or edit) an Info Template view 85
- Chapter 4 Reports views 87**
 - Advanced Time Range Options window 88
 - Access History Report and Summary window 88
 - Purge Config window (simple) 90
 - Purge Config window (expanded) 90
 - Access History Filter window 91
 - Manage Reports window 92
 - Add (or edit) Report window 92
 - Schedule Emailed Report window 93
 - Alarm History report 94
 - Alarm history Summary window 95

Review Video view.....	96
Alarm history Filter window	96
Attendance History Report and Summary window	97
Manual Add (attendance record) window	98
Manual Hide (confirmation) window	98
Attendance History Filter window	99
Intrusion History report and Summary window	99
Intrusion History Filter window	100
Audit History Report and Summary window	101
Log History Report and Summary window	103
Log history Filter window	104
Hardware reports.....	104
Doors Report and Filter window	104
Readers Report and Filter window	105
Inputs Report and Filter window	106
Outputs report and Filter window	107
Elevators Report and Filter window.....	107
Remote Modules Report and Filter window	108
BACnet Points and Filter window	109
Intrusion Displays Report and Filter.....	110
Consolidated Intrusion Displays report.....	110
LDAP Audit History report	111
Miscellaneous reports.....	112
Person Access Right Report.....	112
Person Reader Report	113
Access Right Reader Report and Filter window.....	114
Personnel Changes report and Summary window	115
Personnel Changes Filter window	116
Chapter 5 Controller (System) Setup–Schedules.....	117
Schedules view.....	117
Add a new Schedule window	118
Schedules Quick Edit window	118
Schedules Filter window	119
Add New (edit or duplicate) Schedule view.....	120
Schedule, Summary tab	120
Scheduler tab.....	121
Schedule Setup (weekly schedules) tab.....	123
Special Events tab	124
Access Rights tab	130
Intrusion Pins tab.....	131
Calendar Schedules view	133
Calendar Schedules Filter window.....	134
Add New (or edit) Calendar Schedule view	135
Events tab.....	135
Schedule Setup (calendar schedules) tab	136

Chapter 6 Controller (System) Setup-User Management	139
Users view	139
Configure window	140
Quick Edit window	142
Filter window	143
Add New (and edit) User view	143
Roles tab.....	147
Roles view.....	147
Filter window	148
Add New (or edit) Role tab	148
Users tab	150
Change Password view	151
Chapter 7 Controller (System) Setup-Backup views	153
Backups view	153
System Backup/Local Backup window	155
Backup Archive tab Summary window	155
Backup Archive tab Restore windows	156
Backup Schedule tab	156
Recent Backup History tab.....	157
Recent Backup History tab Filter window	158
Restore from Backup Distribution File or System Backup File views	158
Chapter 8 Controller (System) Setup-Remote Devices	159
Remote Drivers view	161
Manage Drivers window	162
Add Driver windows	162
Enable/Disable Networks window.....	163
Filter window	163
Remote Modules menu.....	163
Access Device Manager – Database (Remote Module Setup) view	164
Add Device windows	165
Add device window, discovered reader	167
Add device window, discovered Azure ID Client Device	168
Device modules views	168
Modules tab.....	169
Video Setup window.....	169
Doors tab.....	170
Elevators tab.....	170
Additional Points tab.....	171
Reader Modules view, Burglar Panels tab	171
Door Setup view, Readers tab	172
Door view, Manual Override window.....	172
Strike tab	173
Sensor tab	175
Exit Request tab.....	176

Alarm Relay tab.....	177
Override Input	177
ADA tab.....	178
Relay Out tab.....	179
Reader configuration options.....	179
Reader view, Summary tab.....	180
Reader Setup view, Reader tab	181
Activity Alert Exts tab.....	183
Output Configuration tab	183
Alarm Relay tab.....	186
Elevators Setup view, Elevator tab	187
Schedule Floors window	189
Floors tab	190
Readers tab	193
Burglar Panel view.....	193
Edit Unlock Input view.....	194
Edit Power Monitor view	195
Remote Module Network Identification view	195
Fade Rate window.....	197
Wink Device window	197
Output Test window.....	197
Access Network view and tab	198
Manual Override window.....	199
Niagara Integration IDs view.....	199
Add New (or edit) Niagara Integration ID view and tab	200
Niagara Integration, Summary tab	201
Access Rights tab	201
Quick Edit window	202
BACnet Network view, BacNet Network tab	202
IP Port tab.....	203
Mstp Port tab.....	204
Door Control tab.....	205
BACnet BDT Manager (Broadcast Distribution Table) view	205
New (or edit) Entry views.....	206
Station Manager - Database view	206
Add (or edit) Station windows	208
Settings windows	209
Schedules tab	210
Join (Add) Station view	210
Distributed Schedule Manager - Database view	212
Recover Station view	214
Station Device Properties view.....	214
Device Ext tab.....	215
Certificate Management view	215
Generate Self-Signed Certificate window	218
Private Key Password window.....	219

- Video Network views..... 219
 - Axis Video Network tab..... 221
 - Milestone Network tab..... 224
 - Milestone X Protect Network tab..... 225
 - Maxpro Network tab..... 226
- DVR and NVR views..... 228
 - Milestone DVRs tab..... 228
 - Milestone Dvr tab..... 229
 - Milestone New DVR window..... 233
 - Milestone Displays tab..... 234
 - X Protect DVRs tab..... 234
 - X Protect Management Server tab..... 235
 - X Protect Recording Servers tab..... 239
 - X Protect Recording Server tab..... 240
 - Maxpro Nvrs tab..... 241
 - Maxpro NVR tab..... 241
 - Maxpro New and Edit NVR windows..... 245
 - Maxpro camera Preferences window..... 246
 - Maxpro New and Edit camera windows..... 246
- Video camera views..... 248
 - Display camera grid..... 248
 - Axis Cameras tab..... 249
 - Axis New camera window..... 250
 - Axis Video Camera tab..... 253
 - Axis camera Preferences window..... 257
 - Axis Events tab..... 258
 - Milestone Cameras tab..... 259
 - Milestone Camera tab..... 260
 - Milestone New camera window..... 262
 - Milestone Events tab..... 264
 - X Protect Cameras tab..... 265
 - X Protect Camera tab..... 266
 - Maxpro Cameras tab..... 269
 - Maxpro Camera tab..... 270
 - Maxpro Events tab..... 273
- Edit Point view, Configuration tab..... 274
 - Inputs..... 277
 - Outputs..... 278
 - Alarm Setup tab (inputs only)..... 278
 - Active Schedule tab (outputs only)..... 279
 - Edit meta data window..... 280
 - Video Setup window..... 281
 - Link To tab..... 282
- SmartKey Discovery view..... 283
 - Discover and Preferences windows..... 284
- SmartKey Device Manager - Database view..... 284

Chapter 9 Controller (System) Setup–Access Setup	287
Access Zones views	287
Add New (or edit) Access Zone view	288
Add new Access Zone Summary tab	290
Access zone Activity Alerts Ext tab	291
Occupants tab	292
Access Zone Supervisors tab	293
Entry Readers tab	293
Exit Readers tab	294
Grouping tab	295
Card Formats view	296
Wiegand Format Editor view, Wiegand Format tab	297
Wiegand Format Summary tab	299
Access Control Setup view	300
Additional Personnel Entry — Import Info tab	301
Data to import	301
Export Personnel Records window	303
Chapter 10 Controller (System) Setup–Intrusion Setup	305
Intrusion Pins view	305
Add New (or edit) Intrusion Pin view, Intrusion Pin tab	306
Intrusion Pins Summary tab	306
PIN Intrusion Zones tab	307
Intrusion Zones views	308
Add New (or edit) Intrusion Zone view	308
Manual Override window	310
Intrusion Zone Summary tab	311
Intrusion Displays tab (learn mode)	312
Readers tab	312
Points tab	313
Grouping tab	314
Recipients tab	315
Escalation Level tabs	315
Relay Links tab	316
Edit Existing Intrusion Pin view	317
Intrusion Displays views	318
Add New (or edit) Intrusion Display view	319
Virtual Display tab	321
Intrusion Display tab (configuration)	321
Intrusion displays Activity Alert Exts tab	322
Display Intrusion Zones tab	322
Chapter 11 Controller (System) Setup–Alarm Setup	325
Alarm Classes views	325
Add New (or edit) Alarm Class view	326
Recipients tab	328
Relay Links tab	329

Alarm Instructions view.....	330
Edit Instructions window	331
Master Instructions window	331
Alarm Relays view (Alarm Count Relays)	332
Add New (or edit) Alarm Count To Relay view	332
Alarm Classes tab.....	333
Relays tab	334
EmailService view (Email Accounts)	335
Outgoing Account tab.....	335
Incoming Account tab	338
Email Recipients view	339
Add New (or edit) Email Recipient view	340
Alarm Classes tab.....	342
Alarm Consoles view	342
Add (or edit) Alarm Console view, Alarm Classes tab.....	343
Video Alarm Classes (Video Alarm Recipient) view	345
Alarm Classes tab.....	346
Station Recipients views	347
Add New (or edit) Station Recipient view	347
Alarm Classes tab.....	348
Power alarm Setup (PlatformServices) view	349
Alarm Extensions view.....	350
Edit Alarm Extension properties (Alarm Source Info tab).....	350
Chapter 12 Controller (System) Setup–Miscellaneous.....	353
Keypad Formats (Keypad Configuration) view	353
Add New (or edit) Keypad Format view.....	354
Pdf Styles view	355
Add New (or edit) PDF Styles view	355
License Manager view	356
Network TCP/IP Settings view	357
Maintenance view (Server).....	361
Update Reader Count window	364
Get Corrupt Pin Numbers window	365
Configure Database view, Database Services tab.....	365
Database Configuration tab (HsqlDbDatabase).....	367
Database configuration tabs (MySQL and SqlServer databases)	367
Web Service view	369
Job Service view.....	371
System Date Time Editor view	372
End User Licenses Agreement view.....	372
Third Party Licenses view.....	372
Controller TimeServers Settings.....	372
Supervisor TimeServers Settings	374
Chapter 13 Controller (System)–Miscellaneous Graphics	377

Graphics view (Graphics Management).....	377
Add a graphic window	378
Modify Settings window	378
Edit Nav window	379
Types of bindings	379
View Graphic.....	386
Graphic Editor view.....	386
About the Graphic Editor canvas.....	387
About Graphic Editor objects (widgets).....	388
About the Graphic Editor toolbar.....	389
About the side bar pane	389
Graphic Editor pop-up menu - available video cameras	390
Images view	392
Add New Image view	393
Display Image view.....	393
Navigation Groups view	393
Add New (or edit) Nav Group view.....	394
Chapter 14 Threat Levels.....	395
Threat level groups view.....	395
Threat Level Group filter.....	396
Activate Threat Level window	396
Retrieve Active Level Activation Status window	397
Add New (or edit) Threat Level Group view	397
Summary Tab	399
Activation Badges tab	400
Access Rights tab	400
Remote Stations tab.....	401
Threat Level Setup view.....	402
Activation alerts	403
Add (or edit) threat level window	404
Edit instructions window.....	405
Edit metadata windows	405
Chapter 15 LDAP network driver views, tabs and windows.....	407
LDAP Network view	407
Ldap Servers tab	409
New (and Edit) LDAP server window	410
Import Preferences window	412
Ldap Server view.....	413
Attributes tab	418
Add attribute window	421
Groups tab.....	421
LDAP Audit History view.....	423
Periodic Purge Schedule	424
Chapter 16 Nrio Driver views, tabs and windows	425
Nrio Device Manager view.....	425

- Nrio Module view 426
- Nrio Point Manager, Analog Points tab 428
 - Manage Nrio Points windows 428
 - Go to Module window 429
 - Digital Points tab 429
- Nrio Point Edit view 430
 - Voltage Input points properties 430
 - Temperature Input points 435
 - Resistive Input points 438
 - Digital input points 442
 - High Speed Counter 446
 - Relay Output points (digital) 449
 - Voltage Output points 453
 - Manage Extensions windows 457
 - History Setup tab 457
 - Active Schedule tab 458
 - Link to tab 459
 - Link From tab 460
- History Extension view 460
 - Set COM Port window 463
 - Upload window 463
 - Download window 464
 - Filter window 464
- Chapter 17 Obix Network view 465**
 - Obix links 465
- Chapter 18 Photo ID management 467**
 - Photo ID Network view 467
 - Photo ID Add device window 468
 - Settings window 468
 - Configure window 469
 - Asure ID Client Device view 470
 - Templates tab 471
 - Asure ID Device.[template] view 472
 - Tenants tab 472
 - Badges tab 472
 - Edit Photo ID Template Data view 473
 - Photo ID Viewers view 473
 - Photo ID Viewer (surveillance) view 474
- Chapter 19 Workbench components in the entsec module 475**
 - entsec-SecurityActivityMonitor (AX Alarm Console) 475
 - entsec-SecurityAlarmConsoleOptions 476
 - entsec-EnterpriseSecurityService 477
 - entsec-MonitorSysDefSecurity (AX Property Sheet) 478
 - entsec-AlarmClasses (Wb Query Table View) 479
 - entsec-AlarmConsoles (WB Query Table View) 479

entsec-EmailRecipients (WB Query Table View)	480
entsec-StationRecipients (WB Query Table View).....	480
entsec-AlarmHistory (Wb Query Table View)	480
entsec-AlarmSourceExts (Wb Query Table View)	481
entsec-AlarmExtInstructions (Wb Query Table View).....	481
entsec-AlarmClassRelayLinks (Wb Query Table View).....	482
entsec-BacnetPoints (WB Query Table View)	482
entsec-NiagaraStationQuery (WB Query Table View)	483
entsec-SecurityAuditHistory (Orion History View)	484
entsec-SecurityLogHistory (Orion History View).....	486
entsec-SecurityHistoryConsolidator (Orion History View)	487
entsec-ScheduleRecs (App Table View).....	489
entsec-CalendarSchedules (WB Query Table View)	489
entsec-Tenants (App Table View)	490
entsec-ThreatLevelGroupRecs (Ac Table View)	490
entsec-ThreatLevelSetup (AX Property Sheet)	491
entsec-PxGraphics (WB Query Table View)	491
entsec-EntsecNavGroupQuery (Wb Query Table View)	491
entsec-ChangePassword (AX Property Sheet).....	492
entsec-ChangePasskey (AX Property Sheet)	492
entsec-UserQuery (Wb Query Table View).....	492
entsec-EntsecRoleQuery (Wb Query Table View)	493
entsec-SystemBackups (AX Property Sheet)	493
entsec-PlatformSetup (AX Property Sheet)	494
entsec-VideoSubsystem (AX Property Sheet).....	494
entsec-EndUserLicenseAgreement (AX Property Sheet).....	494
entsec-ThirdPartyLicenses (AX Property Sheet).....	495
entsec-AccessControlService (AX Property Sheet)	495
entsec-Dashboard (AX Property Sheet)	496
entsec-Personnel (Ac Table View).....	496
entsec-Badges (Badges View)	497
entsec-AccessRights (AC Table View)	498
entsec-AccessZones (AC Table View)	499
entsec-Doors (Wb Query Table View)	499
entsec-SecurityHistoryConsolidator (Orion History View)	500
entsec-AttendanceHistoryConsolidator (Orion History View)	502
entsec-WiegandFormats (Ac Table View).....	503
entsec-KeypadFormats (Ac Table View).....	503
entsec-InfoTemplates (Ac Table View)	504
entsec-NiagaraIntegrationIDs (Ac Table View)	504
entsec-PersonAccessRightReport (App Table View)	505
entsec-PersonReaderReport (App Table View).....	505
entsec-AccessRightReaderReport (App Table View).....	506
entsec-PersonnelChanges (Orion History View)	506
entsec-ReplicationService (AX Property Sheet)	507

Chapter 20 Workbench components in the accessDriver module.....509

- accessDriver-AccessAlarmSourceExt 509
- accessDriver-AccessDoor..... 509
- accessDriver-AccessElevator..... 510
- accessDriver-AccessFloor 510
- accessDriver-AccessInputOutputModule..... 511
- accessDriver-AccessNetwork 512
- accessDriver-AccessProxyExt..... 515
- accessDriver-AccessReader..... 517
- accessDriver-AccessRex..... 520
- accessDriver-AccessSdi..... 521
- accessDriver-AccessStrike..... 522
- accessDriver-Remote2ReaderModule..... 526
- accessDriver-Remote2ReaderPoints 527
- accessDriver-ActivityAlertExt..... 528

Chapter 21 Workbench plugins529

- Access Device Manager 529
- R2 R Point Manager..... 530

Chapter 22 Windows533

- Edit remote reader module window 533

Index.....535

About this reference

Niagara Enterprise Security 4.9 (the system) is a fully-featured product designed to manage building access control in both small and large installations. This document is especially valuable for learning about individual properties, views, windows and reports.

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.

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 \(System\) Setup — Remote Devices](#) chapter.
- 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*

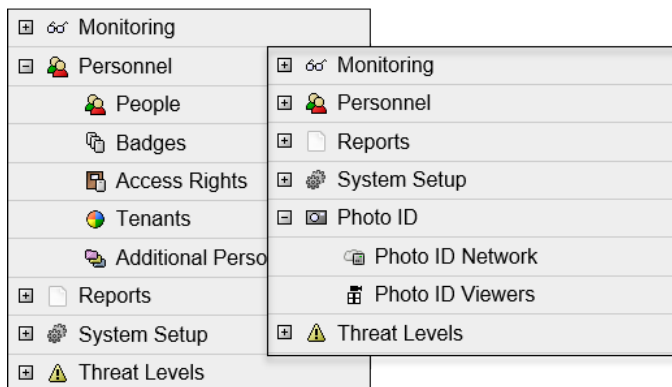
Chapter 1 Home

Topics covered in this chapter

- ◆ Standard control buttons
- ◆ Column Chooser view
- ◆ Controller (System) Setup views
- ◆ User interface
- ◆ Graphics configuration
- ◆ Standard properties

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.

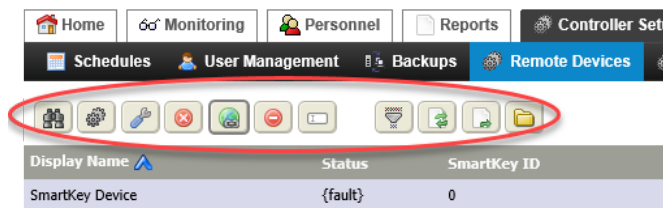
- **Monitoring** provides access to the alarm console, activity monitor and video monitoring menu items.
- **Personnel** provides access to people-related views, such as badge, access right, tenant, and personnel views.
- **Reports** provides access to history reports (such as alarm history and attendance 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:

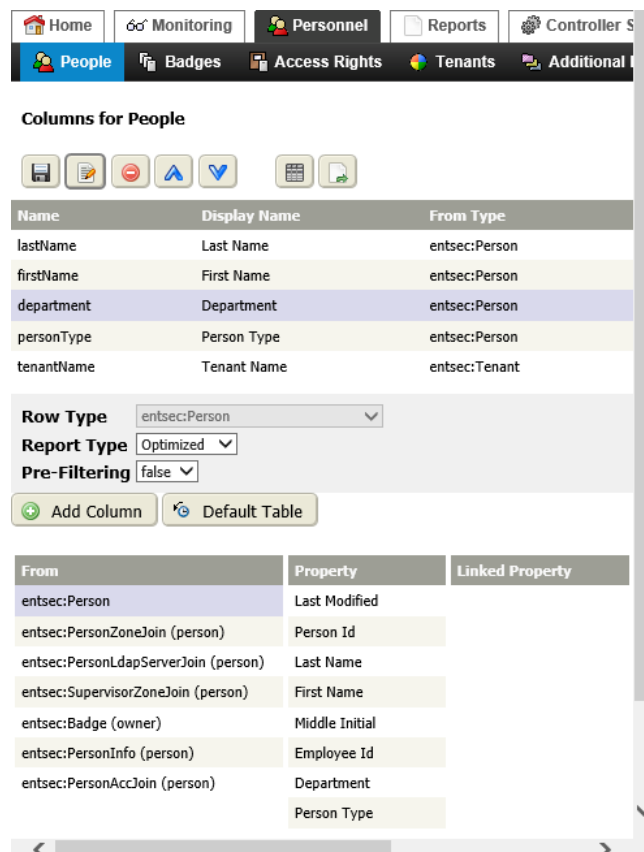
-  Add opens a view or window for creating a new record in the database.
-  Assign Mode buttons open and close the **Unassigned** pane.
-  Column Chooser opens the **Columns for . . .** view from which you can add data columns to, remove them from, and reorder them in the current table.
-  Delete removes 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.

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





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.

Properties

Property	Value	Description
Row Type	read-only	
Pre-Filtering	true or false (default)	Controls the availability of filtering options. true opens the Filter window each time the system opens a Person page. false opens the Filter window only when you click the Filter button ().
From column	drop-down list	Selects the source tables from which to select additional columns for the current table.
Property column	drop-down list	Lists the source table's properties from which to choose an additional column. Clicking Add Column adds this property to the current table. Some properties are linked to the additional properties. Clicking a property in the Property column populates the Linked Property column.
Linked Property	drop-down list	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. 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 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.

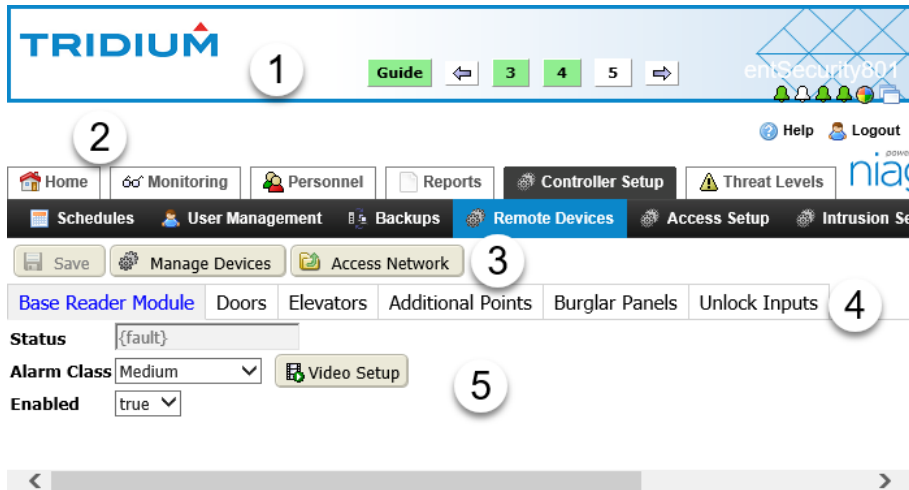
In a Supervisor station, the views are part of **System Setup**, whereas, in a remote host controller station, these views are part of **Controller Setup**. The differences have to do with configuring Supervisory components vs. configuring the devices connected to each controller. Many functions are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

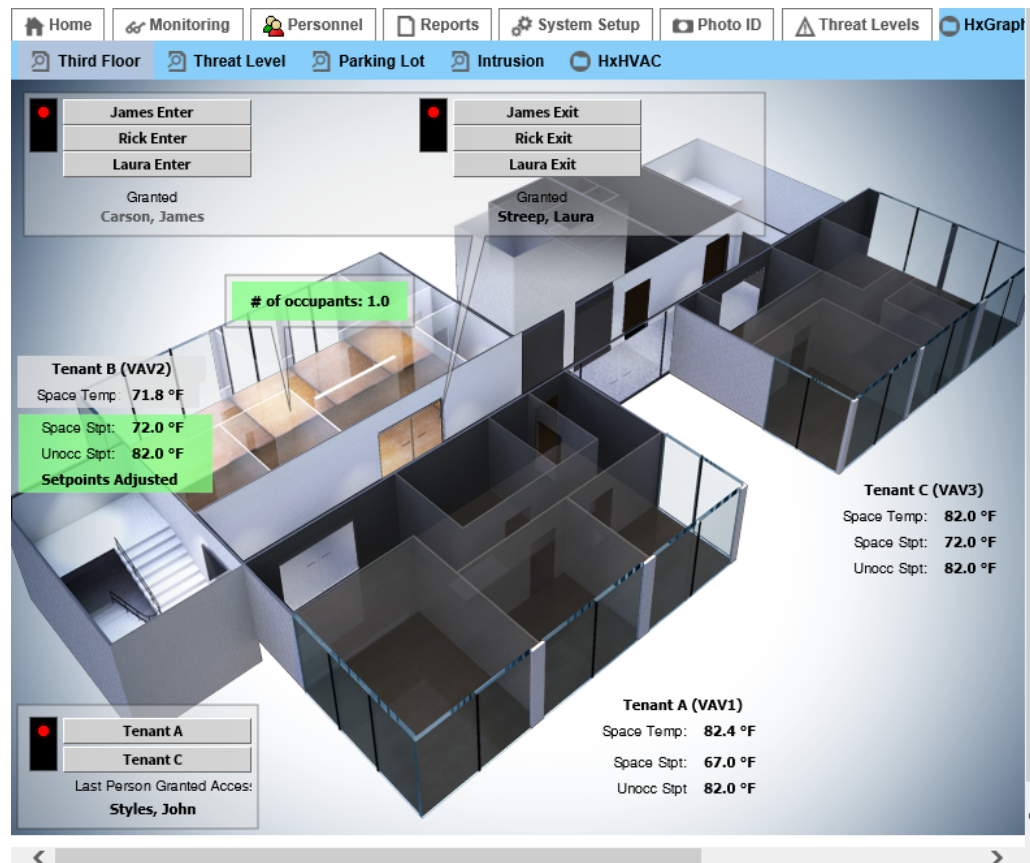
Consider carefully the basic capabilities and limitations of each technology. Obviously, a mobile phone is limited as to what it can useably display when compared to a graphic viewed in a web browser running on a computer. Keep this in mind, and test your views in all target media as you develop them.

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 entity is licensed and polling successfully.</p> <p>{down} indicates that the last poll was unsuccessful, perhaps because of an incorrect property.</p> <p>{disabled} indicates that the Enable property is set to false.</p> <p>{fault} indicates another problem.</p> <p>Depending on conditions, multiple status flags may be set including {fault} and {disabled}, combined with {down}, {alarm}, {stale}, and {unackedAlarm}.</p>
Enabled	true or false	Turns the feature on (true) and off (false).
Fault Cause	read-only	Reports the reason why a network, component, or extension is in fault. Fault Cause is blank unless a fault exists.
Health	read-only	Reports the status of the network or component. This advisory information, including a time stamp, can help you recognize and troubleshoot network problems but it provides no direct network management controls.
Alarm Source Info	additional properties	Links to a set of properties for 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).

Chapter 2 Monitoring views

Topics covered in this chapter

- ◆ Alarm Console — ConsoleRecipient view
- ◆ Activity Monitor view
- ◆ Edit (configure) Activity Monitor view, Activity Monitor tab
- ◆ Video monitoring views

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

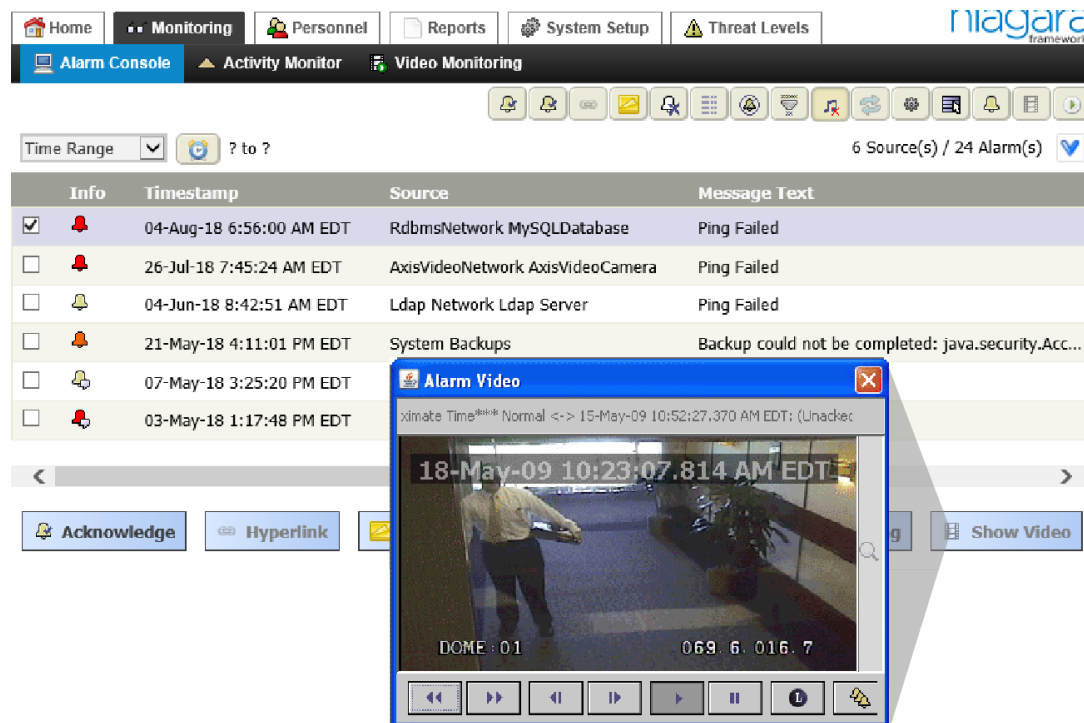
The monitoring views include the:

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

Alarm Console — ConsoleRecipient 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)



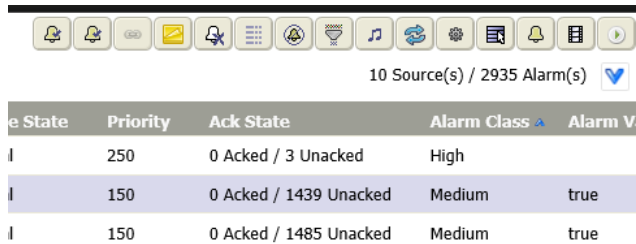
You access this view by clicking the **Monitoring** in the menu tree or by expanding **Monitoring** and clicking **Alarm Console**.
















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.
-  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: <ul style="list-style-type: none"> • Offnormal (normal to offnormal) • Alert (normal to alert) • Fault (normal to fault) • Normal (offnormal, alert, or fault to normal)
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 <code>Display Name</code> 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 (<code>true</code>) or not (<code>false</code>).
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 Alarm Data, page 28 .
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	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> .

Column	Description
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

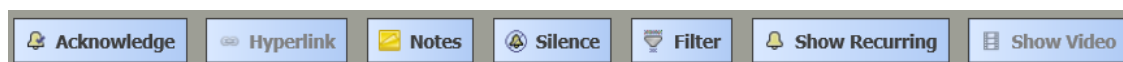
These icons appear under the Info column in the alarm console. Color coding and symbolic images represent the state of each alarm.

-  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: <ul style="list-style-type: none"> • Offnormal (normal to offnormal)

Name	Description
	<ul style="list-style-type: none"> Alert (normal to alert) Fault (normal to fault) Normal (offnormal, alert, or fault to normal)
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 <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.
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 Alarm Data , page 30.

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.

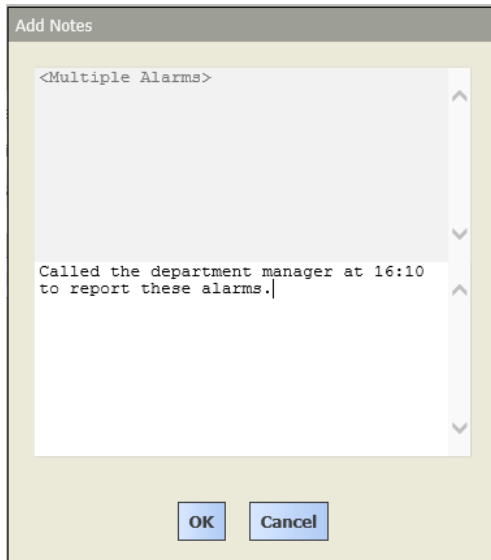
Links


- **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



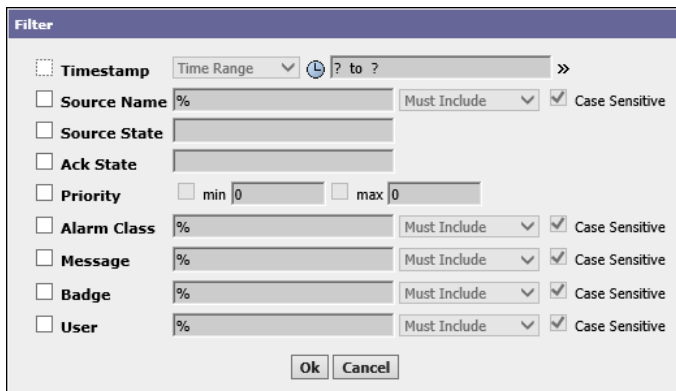
You open this window by selecting an alarm in the table and clicking the Notes button () on the **Alarm Console** view.

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.

Figure 11 Alarm Filter window



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

Alarm Filter search criteria

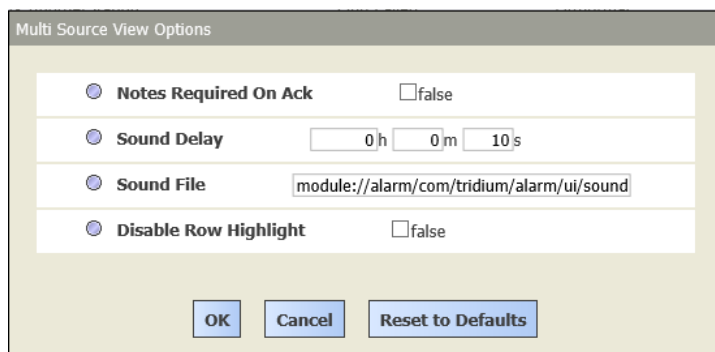
Criterion	Value	Description
Timestamp	Time chooser	Sets up start and end dates and times, days of the week or a schedule to use as filter criteria. The time in each alarm record identifies when the point's status changed from normal to offnormal.
Source Name	text	Reports the name of the alarm source. If you use the default script setting (%parent.displayName%), the source name

Criterion	Value	Description
		property shows the display name of the alarm extension parent. You can edit this script, or type in a literal string, to display here.
Source State	text	Identifies the component state transition: <ul style="list-style-type: none"> • Offnormal (normal to offnormal) • Alert (normal to alert) • Fault (normal to fault) • Normal (offnormal, alert, or fault to normal)
Ack State	text	Reports the state of the alarm (unacknowledged, acknowledged).
Priority	min and max numbers	Defines 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, and from offnormal, fault and alert to Normal). The lower the number, the more significant the alarm. The highest priority alarm is number 1.
Alarm Class	text	Defines alarm routing options and priorities. Typical alarm classes include High, Medium and Low. An alarm class of Low might send an email message, while an alarm class of High 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.

Figure 12 Multi Source View Options window



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

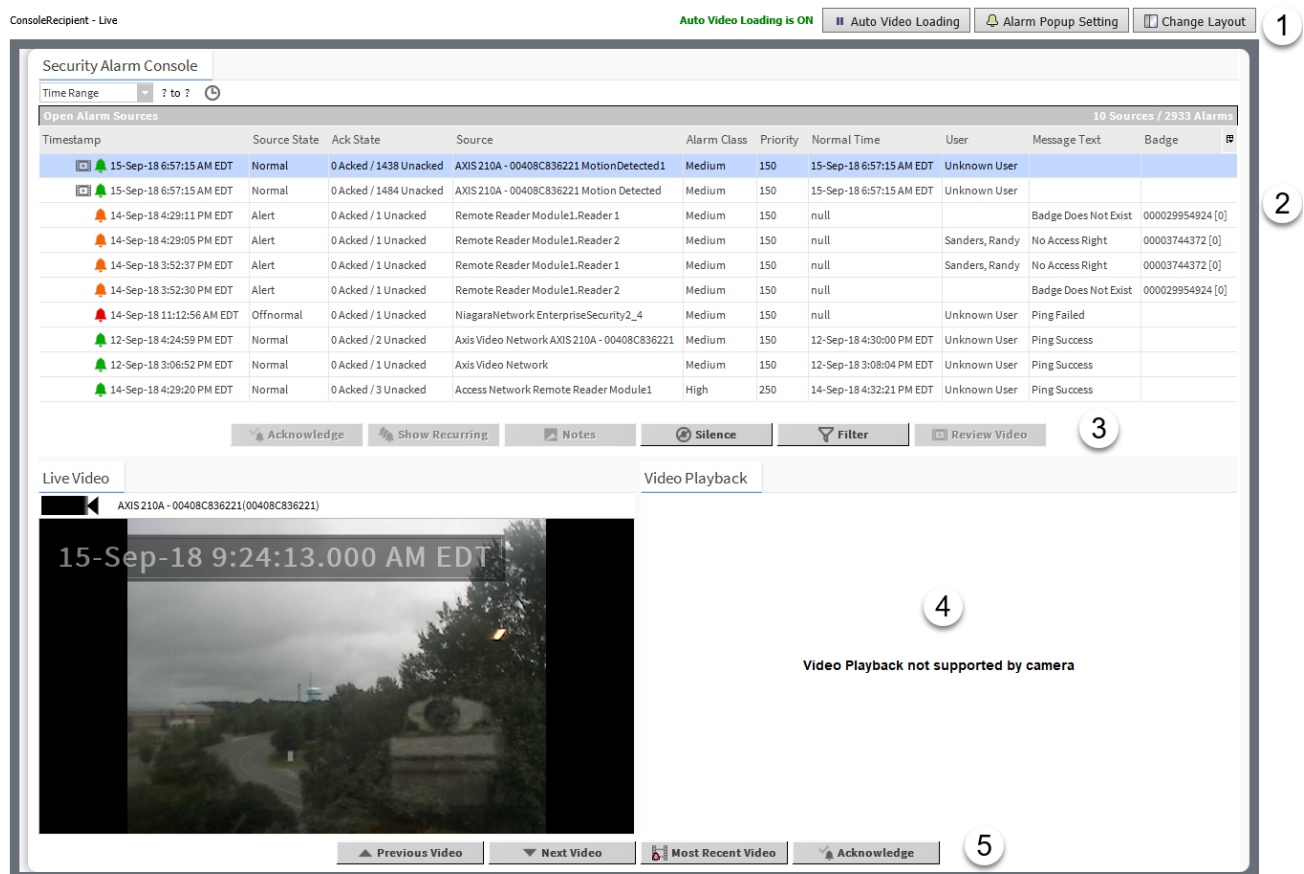
Properties

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



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.

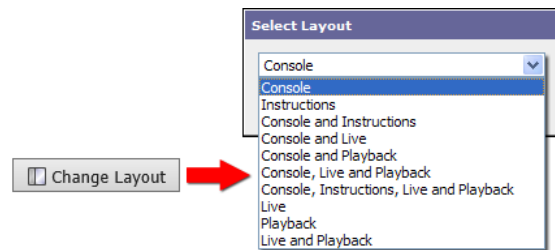
Video alarm controls

- **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

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 transition from normal occurred, triggering the alarm.
Record Type	Reports the type of information the record represents: Access, Audit, Log, Alarm, Alert, Unacked, Intrusion. Refer to About record types, page 36 .
Activity	Identifies the event (for example, Login, Exit Request) that prompted the system to generate the record. Refer to About activities, page 36 .
Station	Reports the station in which the event occurred.
Authority	Identifies the person responsible for the event.
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.

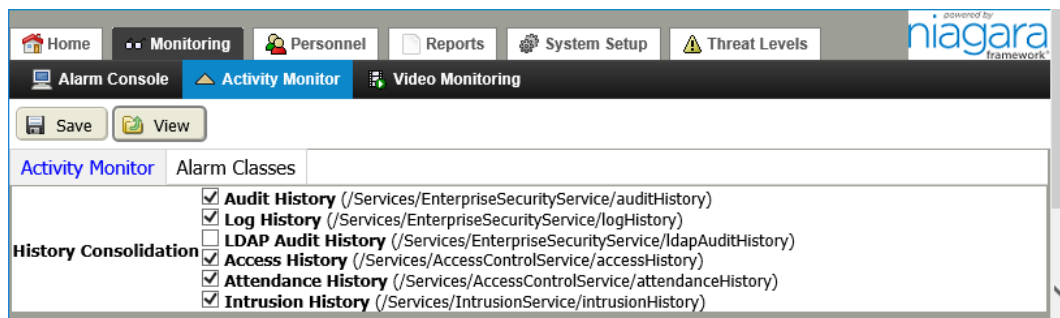
Activity value	Description
Badge Not Assigned	Access denied because the badge exists, but has not yet been assigned to a person.
No Active Schedule	Access denied for lack of a schedule.
No Access Right	Access denied because the person lacks the right to access the location.
Unknown Wiegand Format	Access 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 (Controller (System) Setup → Access Setup → Access Zones) defines the Passback Timeout 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 Passback Violation	Access permitted, but the person is attempting to enter again (pass back) before the Passback Timeout expired.
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.

Activity value	Description
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 Time-out 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



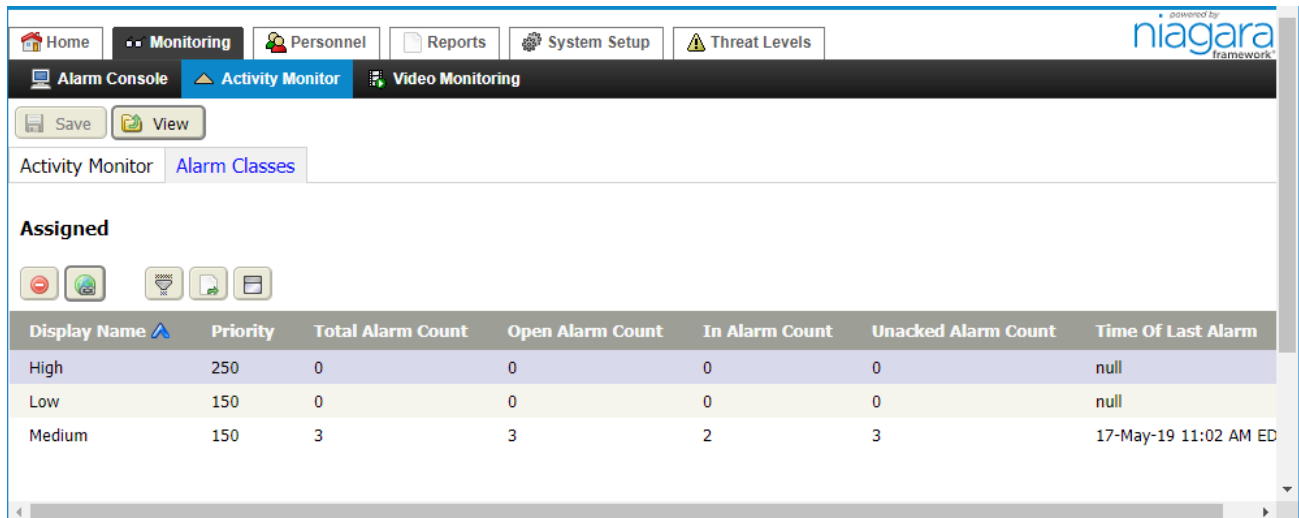
This view displays when you click the **Configure** button  in the **Activity Monitor** view.

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.

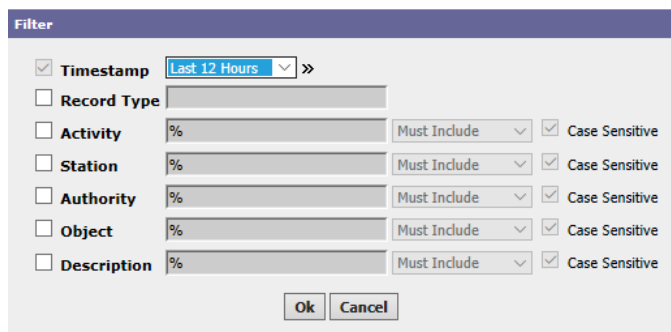
Activity Monitor columns


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



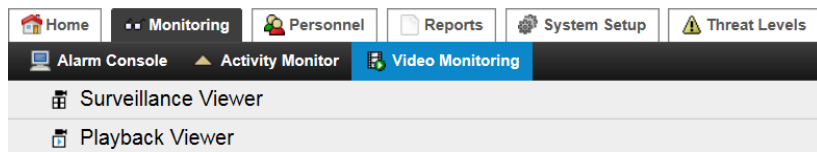
You open this window by clicking the Filter button () on the **Activity Monitor** view.

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.

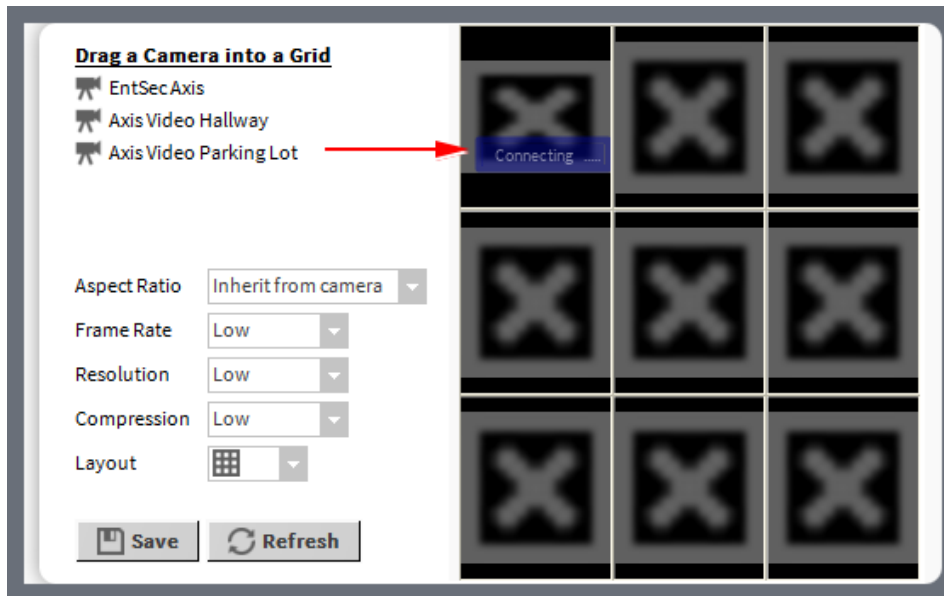


The *Video Framework Guide* contains additional information about configuring video cameras for supported camera models.

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**.

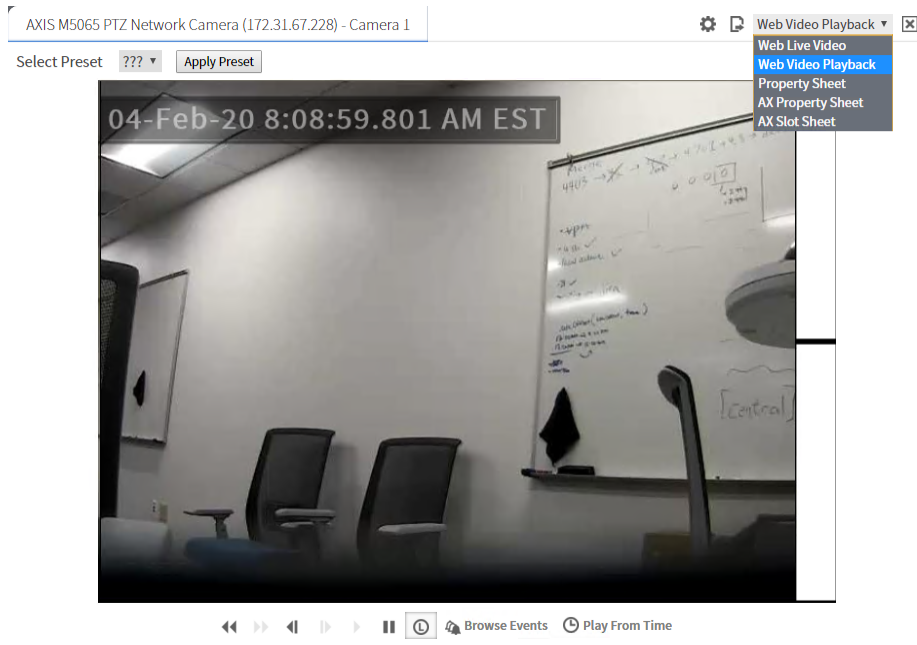
The view consists of a four-pane grid. Each pane links to an active surveillance camera.

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.




Video controls

Figure 21 Video controls





Table 3 Video playback controls

Control	Description
 Fast Play Reverse	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. 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.
 Fast Play Forward	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. 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.
 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.

Control	Description
 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 Video Playback view).


Event controls

Table 4 Event Controls

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

Video indicators

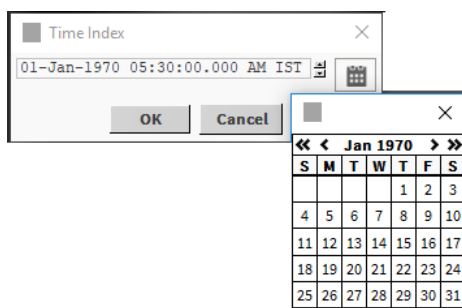
The driver displays these indicators in the video playback window:

-  (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 22 Time Index window



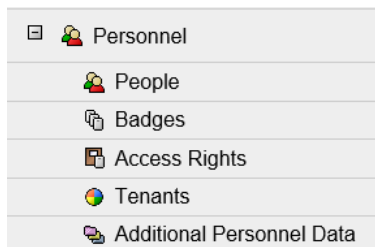
Chapter 3 Personnel views

Topics covered in this chapter

- ◆ People view
- ◆ Add New (or edit) Person view
- ◆ Badges view
- ◆ Enroll New Badge view
- ◆ Add (or edit) New Badge view
- ◆ Batch Enroll Badges view, Badge tab
- ◆ Range Create Badges view, Badge tab
- ◆ Access Rights view
- ◆ Add New (and edit) Access Rights view, Access Right tab
- ◆ Tenants view
- ◆ Add (or edit) a New Tenant view
- ◆ Additional Personnel Data view
- ◆ Add (or edit) an Info Template view

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.

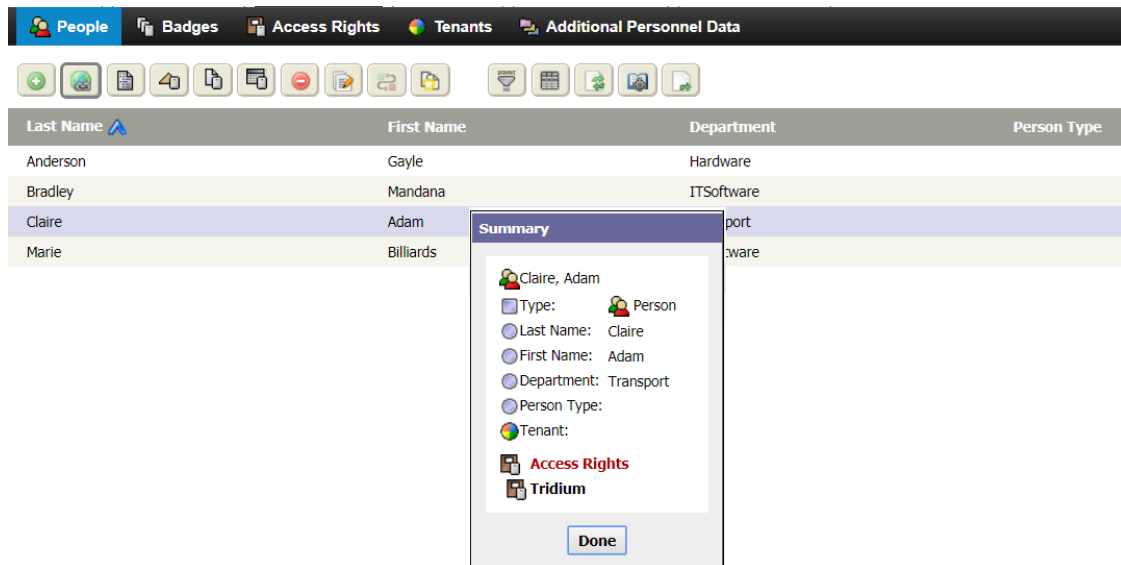
Figure 23 Personnel menu



People view

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

Figure 24 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.

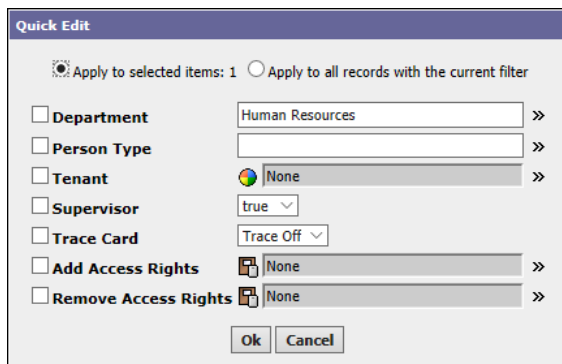
Default People view columns


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 25 Quick Edit window



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.

Figure 26 People View filter

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


People view filter criteria


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 27 Add Person view

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.

Properties

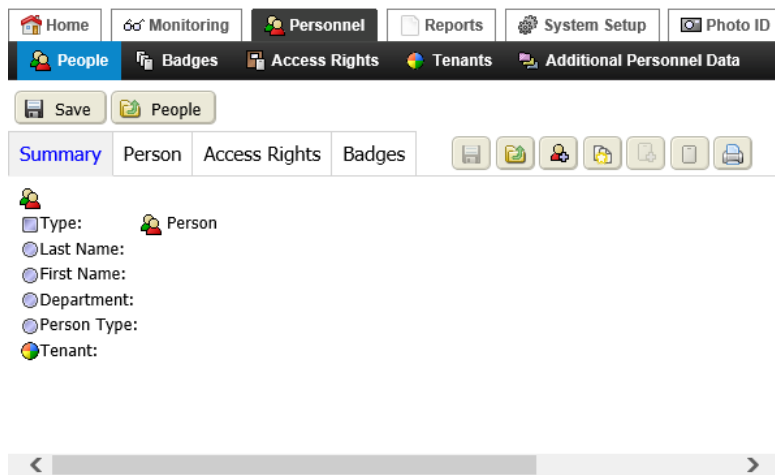
Property	Value	Description
Last Name	text	The person's family name.
First Name	text	The person's given name.
Middle Initial	text	The person's middle initial.
Employee Id	text	Assigns an ID to the person.
Department	text	Defines the department name.
Person Type	String Chooser	Defines something about the person to track. 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	text	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.

Property	Value	Description
PIN (Personal Information Number)		This personnel code is used for keypad entry.
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 28 Summary tab



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

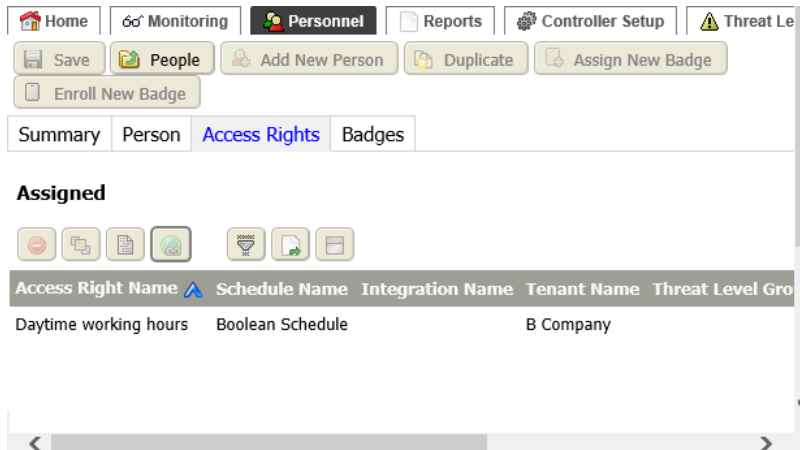
If access rights and a badge are assigned to the person, hyperlinks at the bottom of the **Summary** tab link to the relative records.

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.
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 29 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

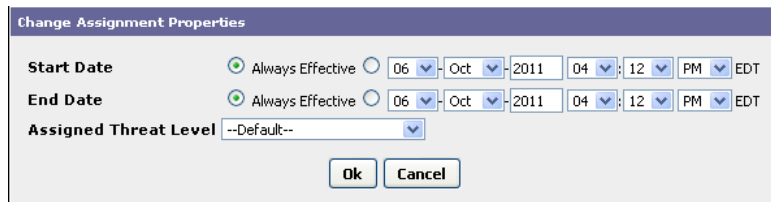
Column	Description
Access Right Name	Identifies the title of the access right associated with the entity.
Schedule Name	Reports the name of the associated schedule (if any).
Integration Name	Reports the name of the associated integration ID The system performs building automation actions, such as turning 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.

Column	Description
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 30 Change Assignment Properties window



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 .

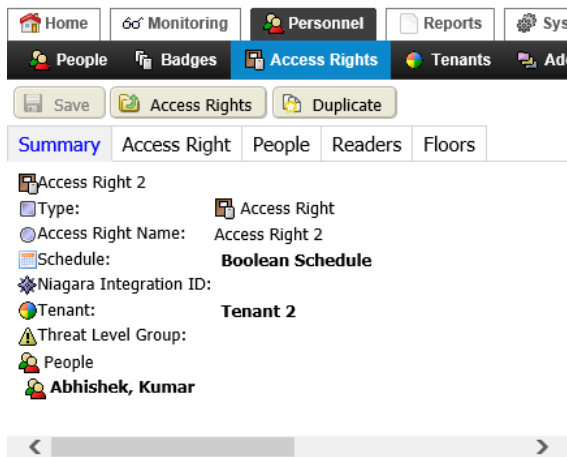
Property	Value	Description
Start Date	date	Determines when an access right becomes valid for a specific person.
End Date	date	Determines when an access right is no longer valid for a specific person.
Assigned Threat Level	drop-down list, defaults to <code>Default</code>	Directly assigns a threat level to the person. To break the connection between the access right and threat level group, this property must be configured to something other than <code>Default</code> . 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 31 Access Rights Summary window

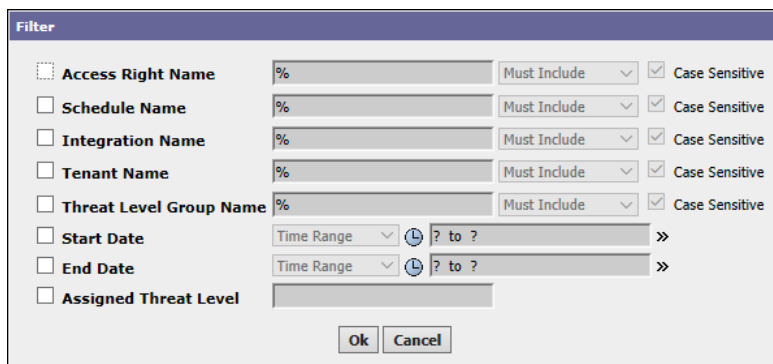



Property	Description
Type	Reports the type of database record.
Access Right Name	Identifies the associated access right.
Schedule	Identifies the schedule associated with the access right.
Niagara Integration ID	Identifies the integration ID associated with the access right.
Tenant	Reports the name of 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 32 Add New Person Access Rights filter window



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.

Property	Value	Description
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 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 33 Badges tab

The screenshot shows the 'Badges' tab interface. At the top, there are control buttons: Save, People, Add New Person, Duplicate, Assign New Badge, and Enroll New Badge. Below these are tabs for Summary, Person, Access Rights, and Badges. The 'Newly Assigned' pane has a toolbar with icons for Remove, Summary, Hyperlink, Unassign, Add, and Enroll. It contains a table with columns: Credential, Facility Code, Description, Wiegand Format Name, and Status. The 'Unassigned' pane also has a toolbar with icons for Add, Summary, Hyperlink, Unassign, and Enroll. It contains a table with the same columns as the 'Newly Assigned' pane. The 'Unassigned' table has one row with the following data: Credential: 000000000023450, Facility Code: 0, Description: (empty), Wiegand Format Name: 55-Bit Wiegand Format, Status: Issueal.

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.

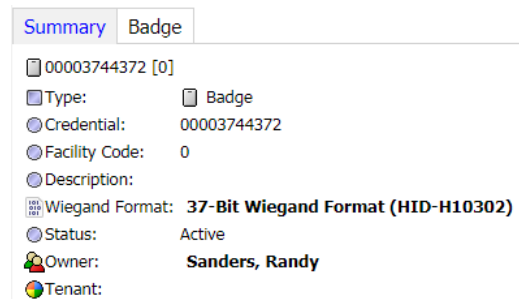
Columns

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 state of the badge: Issuable (currently unassigned), Active, Disabled, Lost or Unknown.
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.

Figure 34 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.

Properties

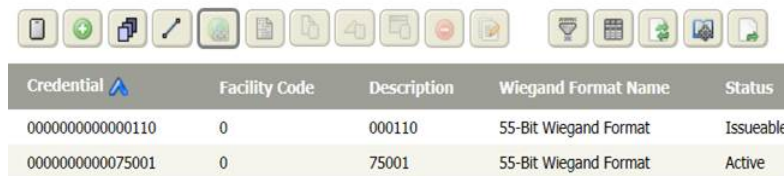
Property	Description
Type	Identifies this summary as containing badge data.
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may be used.
Description	Provides a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Identifies the badge format.
Status	Reports the current state of the badge: Issuable (currently unassigned), Active, Disabled, Lost or Unknown.

Property	Description
Owner	Reports the person to whom the badge is assigned.
Tenant	Reports the tenant with whom the person is associated.

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.

Figure 35 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

Control buttons

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 state of the badge: Issuable (currently unassigned), Active, Disabled, Lost or Unknown.
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 36 Badges Quick Edit window

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

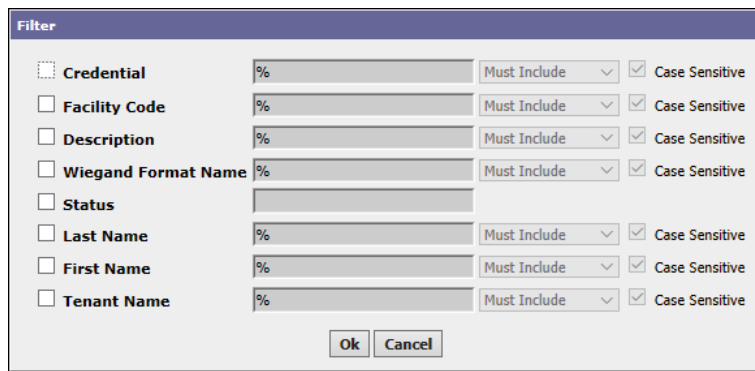
Property	Value	Description
(application)	radio buttons	Apply to selected items: 1 executes the change(s) for only the selected badge. Apply to all records.... executes the change(s) for all badges in the view. If the view is filtered, changes apply to only the filtered badges.
Description	text	Defines a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Status	drop-down list	Reports "Issuable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue Date	radio buttons	Defines when each badge is authorized for use. Two choices are possible: TBA (to be assigned) allows issue date to be defined at a later time.

Property	Value	Description
		Six date options: Month, Day, Year, hour, minutes, and AM/PM.
Expiration Date	radio buttons	The date and time that 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	text	Identifies the tenant associated with the badge.

Badges Filter window

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

Figure 37 Badges filter window



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

Criterion	Value	Description
Credential	wildcard (%)	Assigns a sequential number to a badge. The card reader uses this number to validate access.
Facility Code	wildcard (%)	Identifies the physical building, organization or campus where the badge may be used.
Description	wildcard (%)	Defines a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	wildcard (%)	Defines the wiring standard for the card reader.
Status	drop-down list	Reports "Issueable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Last Name	wildcard (%)	The person's family name.
First Name	wildcard (%)	Defines the given name of the person.
Tenant Name	wildcard (%)	Defines the company 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 38 Badge tab - Enroll New Badge view

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 39 Summary tab for Enroll New Badge

Summary Badge

0 [0]

Type: Badge

Credential: 0

Facility Code: 0

Description:

Wiegand Format:

Status: Issueable

Owner:

Tenant:

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 purpose or characteristics of the badge.
Wiegand Format	Identifies the wiring standard for the card reader.
Status	Reports the current state of the badge: Issuable (currently unassigned), Active, Disabled, Lost or Unknown.
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 40 Add New Badge view

Save Badges

Summary **Badge**

Credential 0000000000001110

Facility Code 0

Description Headquarters

Wiegand Format 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	Assigns a sequential number to a badge. The card reader uses this number to validate access.
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	Defines the wiring standard for the card reader.
Status	drop-down list	Reports "Issueable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue date	radio buttons	Defines when each badge is authorized for use. Two choices are possible: TBA (to be assigned) allows issue date to be defined at a later time. Six date options: Month, Day, Year, hour, minutes, and AM/PM.
Expiration date	radio buttons	The date and time that 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.
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 41 Add New Badge Summary tab

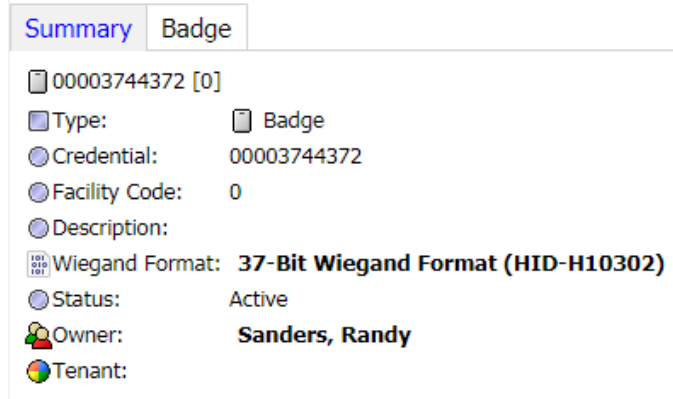
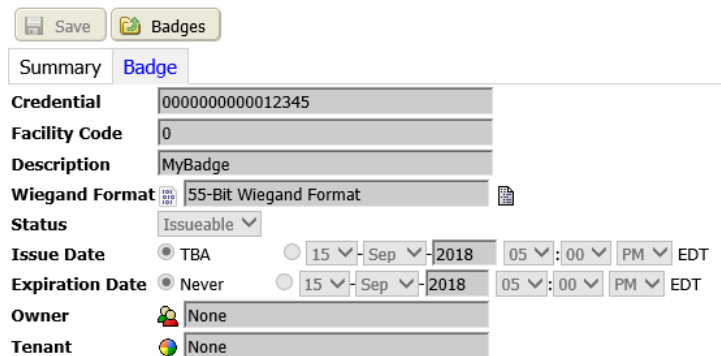



Table 8 Add New Badge Summary tab fields

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 state of the badge: Issuable (currently unassigned), Active, Disabled, Lost or Unknown.
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.



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.

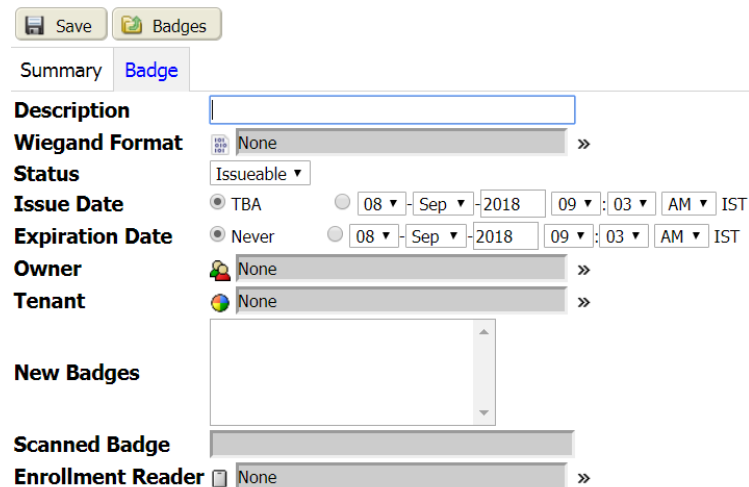
Properties

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	Defines 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 42 Batch Enroll Badges, Badge tab



Save Badges

Summary **Badge**

Description

Wiegand Format »

Status

Issue Date TBA 08 Sep 2018 09:03 AM IST

Expiration Date Never 08 Sep 2018 09:03 AM IST


Owner »

Tenant »

New Badges

Scanned Badge

Enrollment Reader »

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	text	Defines a meaningful word or short phrase to help you remember the purpose or characteristics of the badge.
Wiegand Format	Ref chooser	Defines the wiring standard for the card reader.
Status	drop-down list	Reports "Issueable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue date	radio buttons	Defines when each badge is authorized for use. Two choices are possible: TBA (to be assigned) allows issue date to be defined at a later time. Six date options: Month, Day, Year, hour, minutes, and AM/PM.
Expiration date	radio buttons	The date and time that 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.
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.
New Badges	read-only list of numbers	Displays each new badge as the reader scans it.
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 43 Batch Enroll Badges Summary tab

The screenshot shows the 'Batch Enroll Badges Summary tab' interface. At the top, there are two tabs: 'Summary' (selected) and 'Badge'. Below the tabs, there is a list of fields with their current values:

- Type: Badge
- Credential: 0
- Facility Code: 0
- Description:
- Wiegand Format:
- Status: Issueable
- Owner:
- Tenant:

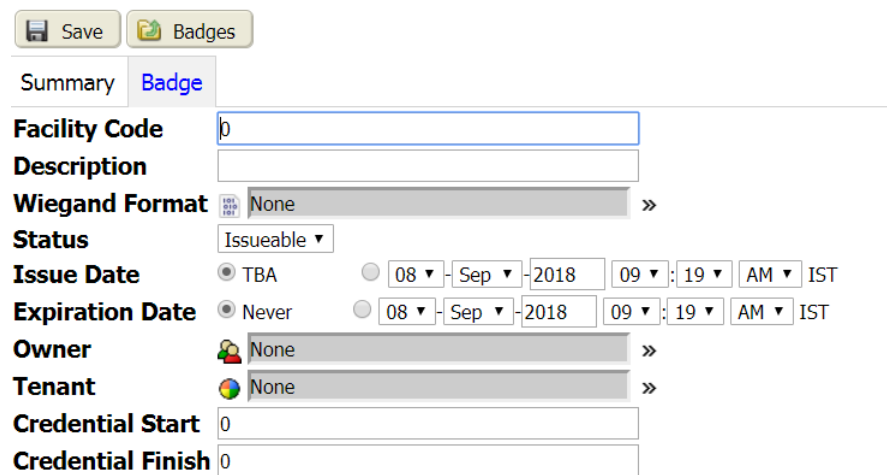
Table 9 Enroll New Badge Summary tab properties

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 state of the badge: Issuable (currently unassigned), Active, Disabled, Lost or Unknown.
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 44 Range Create Badges view, Badge tab



Save Badges

Summary **Badge**

Facility Code 0

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 0

Credential Finish 0

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.

Property	Value	Description
Wiegand Format	Ref chooser	Defines the wiring standard for the card reader.
Status	drop-down list	Reports "Issueable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Issue date	radio buttons	Defines when each badge is authorized for use. Two choices are possible: TBA (to be assigned) allows issue date to be defined at a later time. Six date options: Month, Day, Year, hour, minutes, and AM/PM.
Expiration date	radio buttons	The date and time that 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.
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 45 Range Create Badges Summary tab

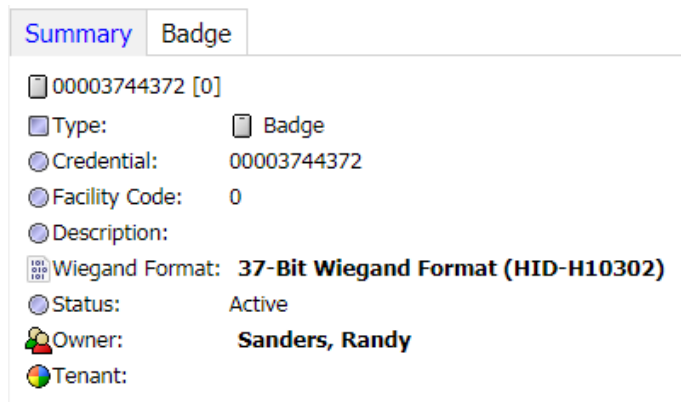


Table 10 Range Create Badges Summary tab properties

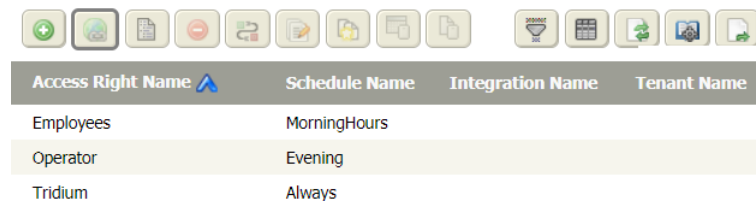
Property	Description
Type	Identifies this summary as reporting badge enrollment information.
Credential	Reports the sequential number assigned to the badge. The card reader uses this number to validate access.
Facility Code	Identifies the physical building, organization or campus where the badge may 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 state of the badge: Issuable (currently unassigned), Active, Disabled, Lost or Unknown.
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 46 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

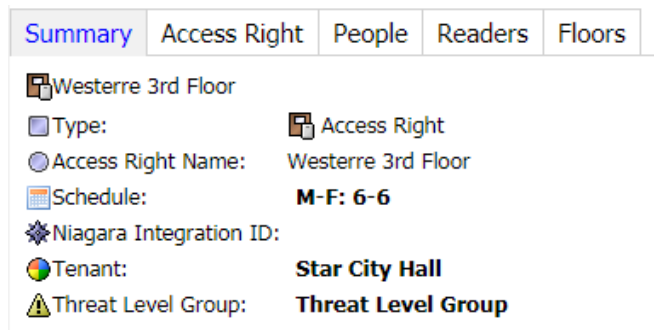
Column	Description
Access Right Name	Identifies the title of the access right associated with the entity.
Schedule	Reports the name of the associated schedule (if any).
Niagara Integration ID	Reports the name of the associated integration ID The system performs building automation actions, such as turning 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 47 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.

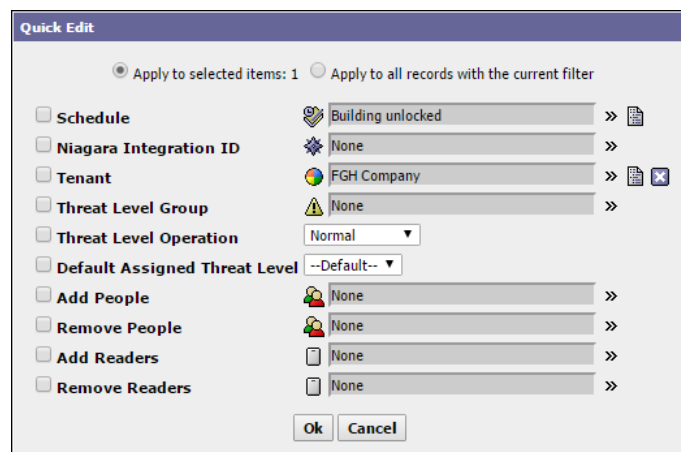
Table 12 Summary of access right properties


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.
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 48 Access Rights Quick Edit view



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.

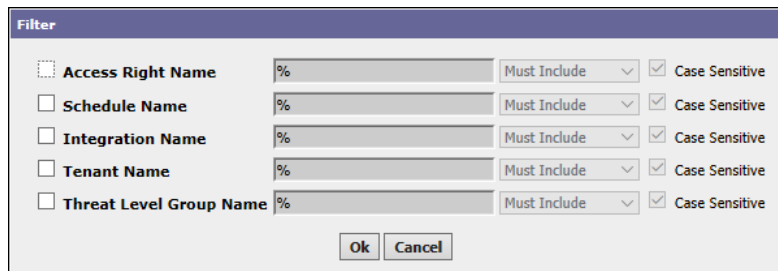
Property	Value	Description
Schedule	text	Identifies the name of the schedule (if any) that is assigned to the access right.
Niagara Integration ID	text	Defines the physically-defined space where a tenant card holder typically resides in a facility. This information may be passed to a building automation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

Property	Value	Description
Threat Level Operation	drop-down list	<p>Defines how the access right responds to a threat level.</p> <p>Normal 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>Specific Level 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>Reverse 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>Reverse allows some types of people (emergency responders) into a facility when the active threat level is elevated.</p>
Default Assigned Threat Level	drop-down list; defaults to <code>Default</code>	<p>Defines a specific threat level to associate with an access right.</p> <p>If you leave this property set to <code>-Default-</code>, the access right inherits the threat level from the Default Access Right Threat Level property as defined for the selected threat level group.</p>
Add People	Ref Chooser	Associates people to this access 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 49 Filter window for access rights



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.

Type	Value	Description
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 50 Add New Access Right view

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.

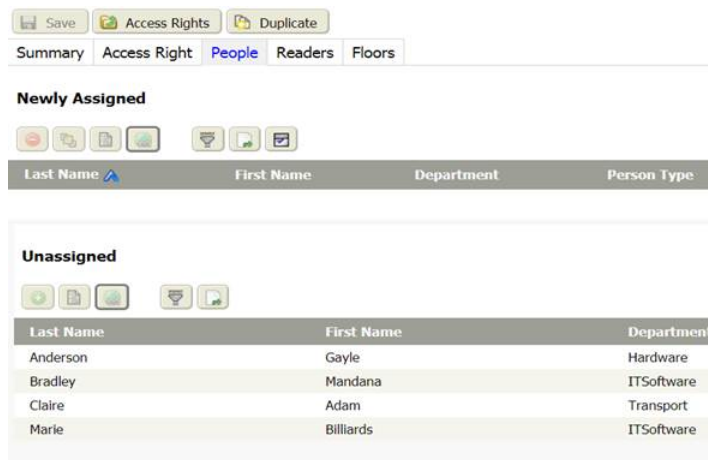
Property	Value	Description
Access Right Name	text	Provides a descriptive title for the access right.
Schedule Name	Ref chooser (required value)	Identifies the name of an existing schedule that provides a boolean (true or false) output to indicate when the access right is in effect over a 24-hour day, 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	Ref Chooser	Defines the physically-defined 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 when a person exercises this access right by entering the facility, the appropriate lighting, HVAC, and other controls adjust automatically.
Tenant	Ref chooser	Provides additional information about the access right that may be used for filtering or sorting access right records. A single tenant is assigned to an access right.
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: Threat Level Operation and Default Assigned Threat Level .


Property	Value	Description
Threat Level Operation (appears only when a Threat Level Group is assigned.)	drop-down list (defaults to Normal)	<p>Defines how the access right responds to a threat level.</p> <p>Normal 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>Specific Level 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>Reverse 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>Reverse allows some types of people (emergency responders) into a facility when the active threat level is elevated.</p>
Default Assigned Threat Level (appears only when a Threat Level Group is assigned).	drop-down list (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 Default Access Right Threat Level property as defined for the selected threat level group.</p>
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 51 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

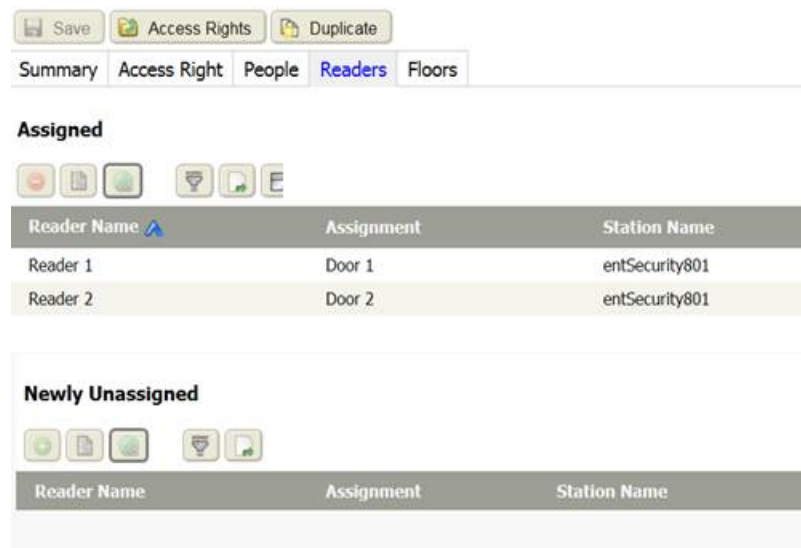
Table 13 Access Rights, People tab columns

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 date the access right became effective.
End Date	If the employee has been terminated, the last day of employment.
Assigned Threat Level	Reports the threat level associated with the access right.

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 52 Access Rights, Readers tab



Save Access Rights Duplicate

Summary Access Right People **Readers** Floors

Assigned

Reader Name	Assignment	Station Name
Reader 1	Door 1	entSecurity801
Reader 2	Door 2	entSecurity801




Newly Unassigned

Reader Name	Assignment	Station Name
-------------	------------	--------------

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

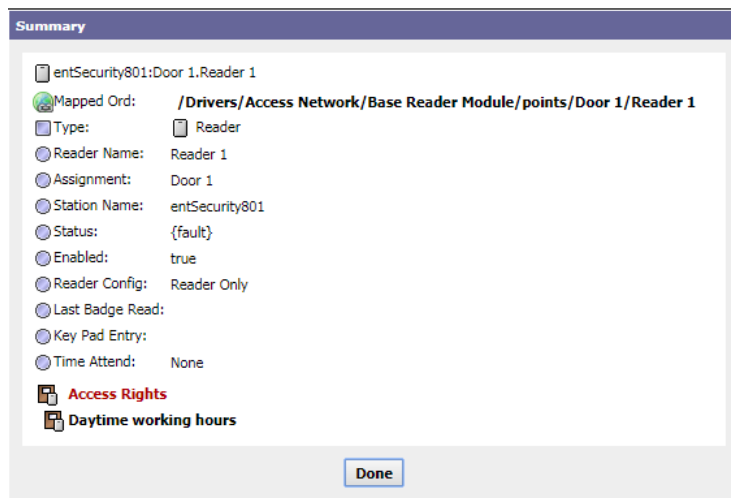
Table 14 Access Rights, People tab columns

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 53 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

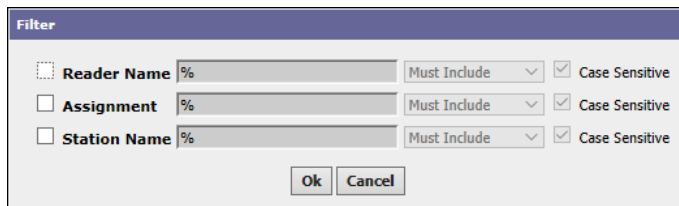
Property	Description
Mapped Ord	Locates the device in the station.
Type	Indicates the type of device.
Reader Name	Indicates the name of the reader.

Property	Description
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 54 Readers tab Filter window



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 55 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 56 New Access Right, Floors tab Filter window

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.

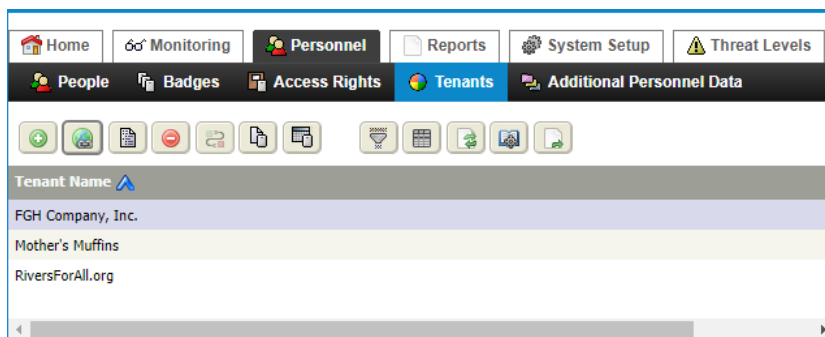
You open this window by clicking the Filter button ()

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 57 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.)

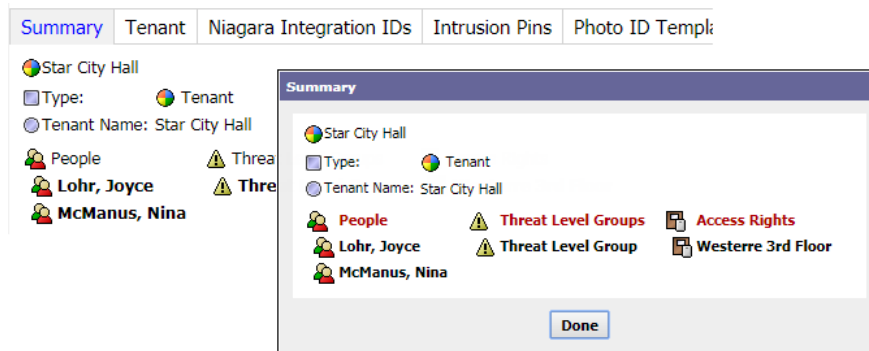
-  Show Readers opens the **Person Reader Report**. The *Reports* chapter documents this report.
-  Show Expirations opens the **Person Access Right Report** view.


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 58 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.

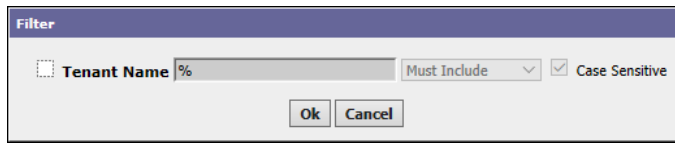
Table 17 Tenant properties

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, and Badges.

Filter window

This window sets the search criterion for tenant records.

Figure 59 Tenants Filter window



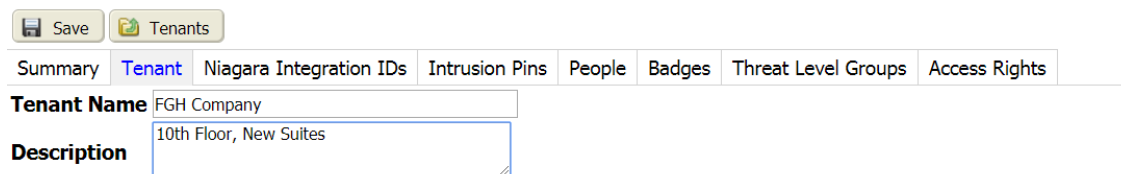
The tenant name serves as the sole criterion for searching.



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 60 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:

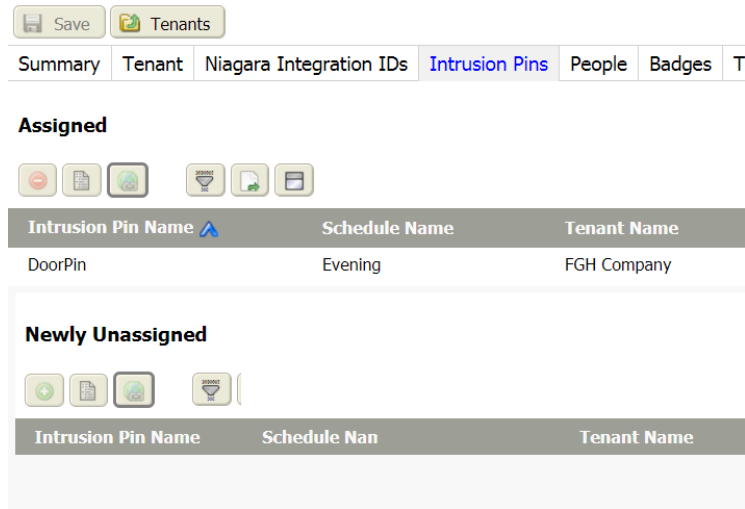
-  Unassign disassociates the integration ID from the tenant.
-  Summary opens a window that summarizes the selected integration ID's properties.
-  Hyperlink opens the integration ID view for the selected ID. This view is documented in the *Controller Setup—Remote Devices* chapter.

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 61 Intrusion Pins tab



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 62 Tenant tab

The screenshot shows the 'Tenant' tab interface. At the top, there are 'Save' and 'Tenants' buttons. Below them is a navigation bar with tabs: 'Summary', 'Tenant', 'Niagara Integration IDs', 'Intrusion Pins', 'People' (highlighted), 'Badges', and 'Threats'. The main content area is divided into two sections: 'Newly Assigned' and 'Unassigned'. Each section has a set of control buttons (Remove, Summary, Hyperlink, Assign, Export, Print) and a table with columns: 'Last Name', 'First Name', 'Department', and 'Person Type'.

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:

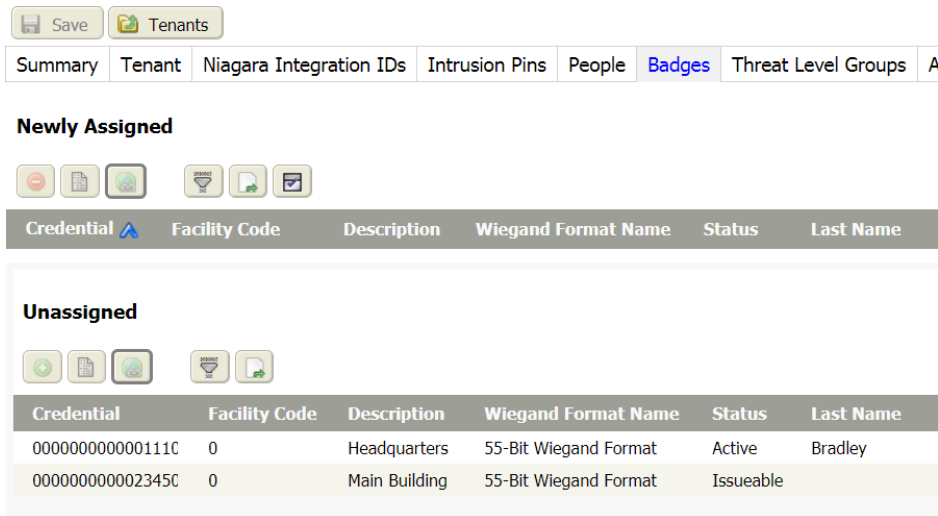
- Remove Assignment (Unassign) disassociates an assignment that was previously made.
- Summary opens the Summary window for the selected item, which shows how item properties are currently configured. Double-clicking on any row in a table opens the Summary tab, which contains the same information as 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 63 Badges tab



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:

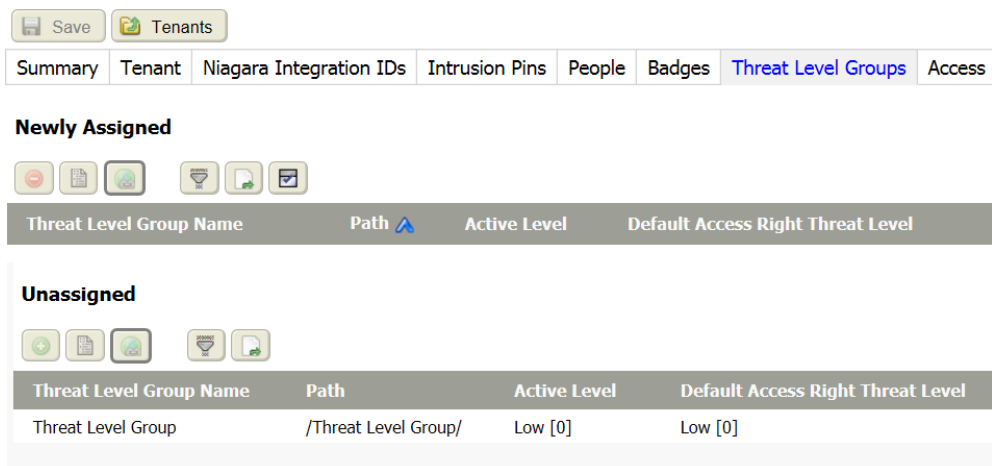
- Unassign disassociates the badge from the tenant.
- Summary opens a window that summarizes the selected badge’s properties.
- Hyperlink opens the badges view for the selected badge. This view is documented in the *Badges, views, tabs, and windows* topics.

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 64 Threat Level Group tab




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:

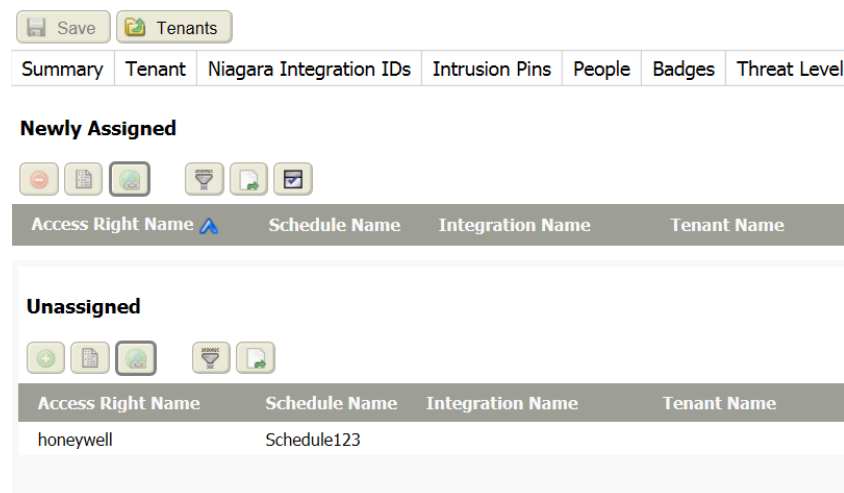
-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  Summary opens the Summary window for the selected item, which shows how item properties are currently configured. Double-clicking on any row in a table opens the Summary tab, which contains the same information as 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 65 Access Rights tab






The screenshot displays the 'Access Rights' tab interface. At the top, there are 'Save' and 'Tenants' buttons. Below this is a navigation bar with tabs: Summary, Tenant, Niagara Integration IDs, Intrusion Pins, People, Badges, and Threat Level. The 'Newly Assigned' pane is active, showing a table with columns: Access Right Name, Schedule Name, Integration Name, and Tenant Name. Below this is an 'Unassigned' pane with a table containing one row: 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:

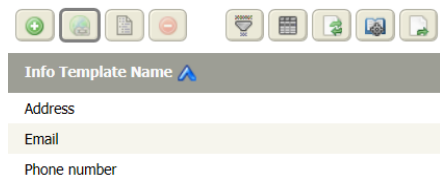
-  Remove Assignment (Unassign) disassociates an assignment that was previously made.
-  Summary opens the Summary window for the selected item, which shows how item properties are currently configured. Double-clicking on any row in a table opens the Summary tab, which contains the same information as 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 66 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

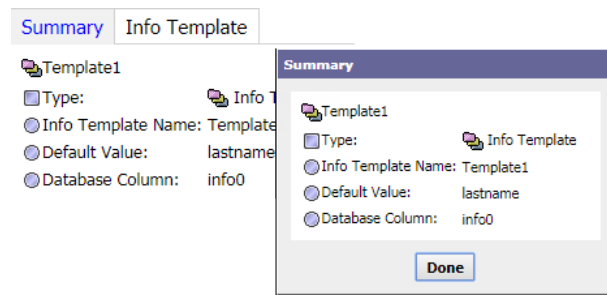
Column	Description
Info Template Name	Provides a descriptive title (display name) for the template.
Default Value	Reports the text that by default displays for the property in the Add New Person and edit person views.

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 67 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.

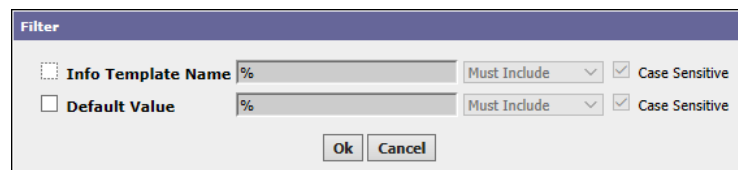
Table 19 Summary properties

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 68 Filter (Additional Personnel Data)



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 69 Add New Info Template view

Summary **Info Template**


Info Template Name

Default Value

Smart Sense

Multi Line

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 <code>true</code> , the system allows you to include a link (the <code>>></code> icon) to the String Chooser 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 <code>true</code> , this option configures the value text box for more than a single line of text.

Chapter 4 Reports views

Topics covered in this chapter

- ◆ Advanced Time Range Options window
- ◆ Access History Report and Summary window
- ◆ Alarm History report
- ◆ Attendance History Report and Summary window
- ◆ Intrusion History report and Summary window
- ◆ Audit History Report and Summary window
- ◆ Log History Report and Summary window
- ◆ Hardware reports
- ◆ Consolidated Intrusion Displays report
- ◆ LDAP Audit History report
- ◆ Miscellaneous reports

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 70 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:

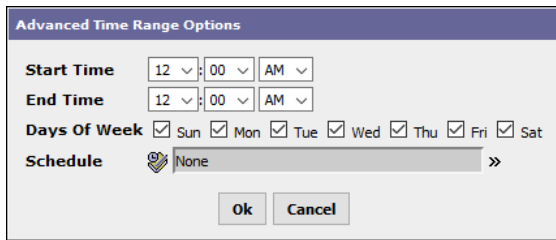
- You may filter reports to include only the records you are interested in. If you do not filter report data, the system alerts you that only the top 5,000 lines are available. You can individually edit history report record capacities.
- For reports that query an SQL database (the Orion space), you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

Figure 71 Advanced Time Range Options window



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*.

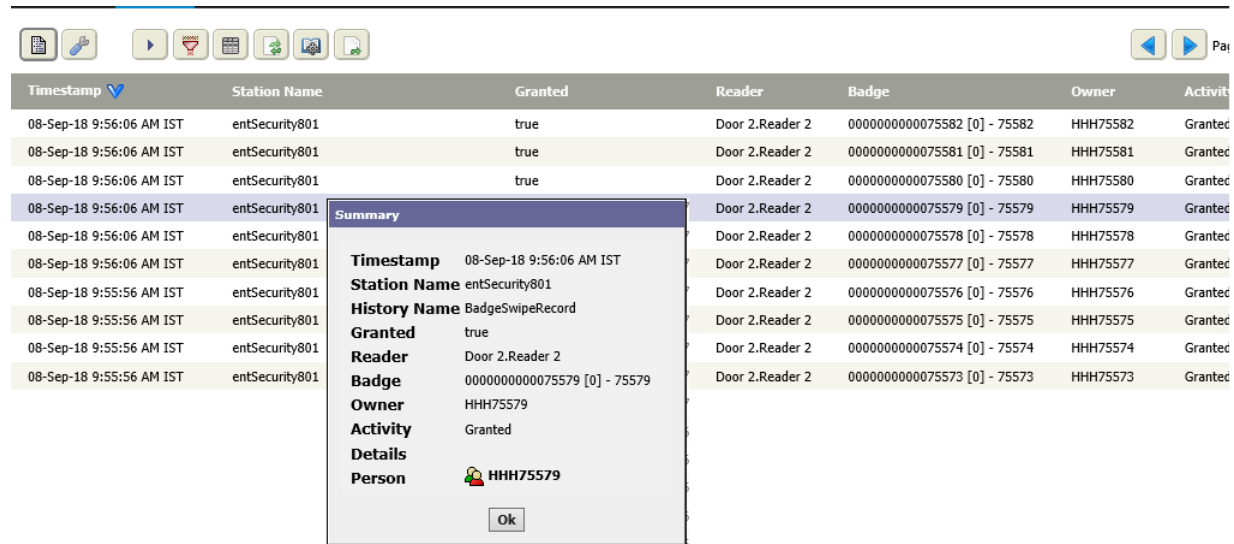
Properties

Property	Value	Description
Start Time	hour: minute	Defines a time of day to begin 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 72 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

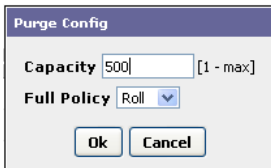
Column/Property	Description
Timestamp	Reports when the record was written to the database.
Granted	Reports if access was granted (<code>true</code>) or denied (<code>false</code>).
Reader	Identifies the reader used to grant access.
Badge	Identifies the badge number who accessed the building.
Owner	Identifies the person who accessed the building.
Activity	Reports what the person was doing: entering or exiting.
Details	Provides additional information.
Person Id	Identifies the Employee Id 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 73 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.

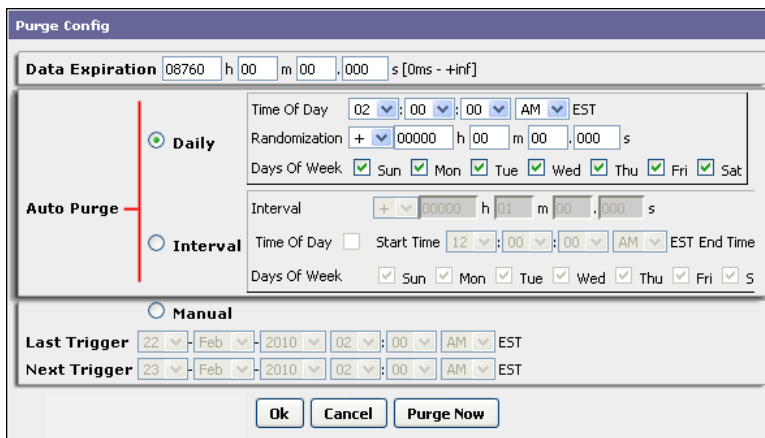
Property	Value	Description
Capacity	number	Defines the maximum number of history records allowed in the associated history table. What happens when the record count reaches Capacity depends on the Full Policy setting.
Full Policy	drop-down list	Determines what happens when the history table reaches its maximum Capacity . Stop restricts the table to the Capacity . After reaching this number, the system ignores new records. Roll replaces the oldest records with newer records.


Purge Config window (expanded)

In a Supervisor station, for some history reports, an expanded **Purge Config** window displays with additional properties.

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

Figure 74 Purge Config window, Supervisor, History reports including Auto Purge



This window opens in a Supervisor station when you click **Reports**, click one of the history reports, and click the Purge Config button (.

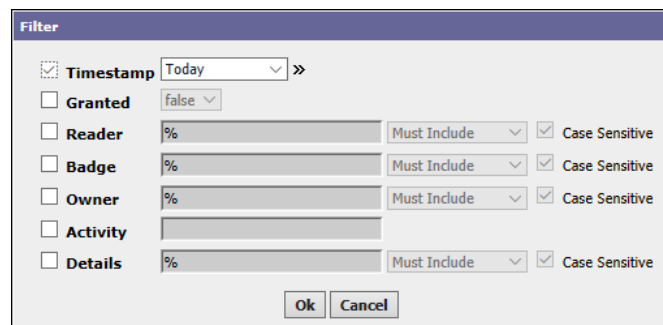
This purge window presents in a Supervisor station for the following reports: Access History, Alarm History, Intrusion History, Audit History, and Log History.

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 Auto Purge , 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 75 Access History Filter window



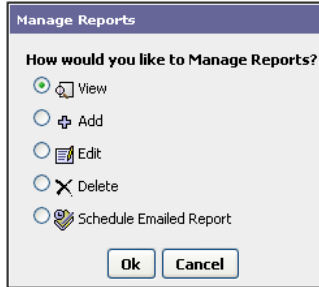
This window opens when you click **Reports**→**Access History**, followed by clicking the Filter button (.


Criterion	Value	Description
Timestamp	drop-down list	Selects a period of time for displaying access history. To further 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 76 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 many 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).

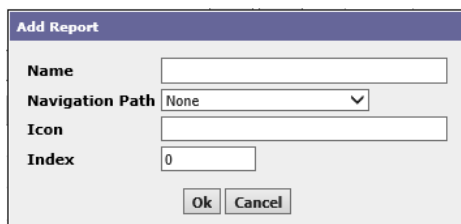
Selecting the *View*, *Edit*, and *Delete* options open a window that lists the custom reports. You choose the report to view, edit, or delete from this list.

NOTE: You cannot delete the pre-configured reports.

Add (or edit) Report window

This window sets up custom reports.

Figure 77 Add/Edit Report window



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

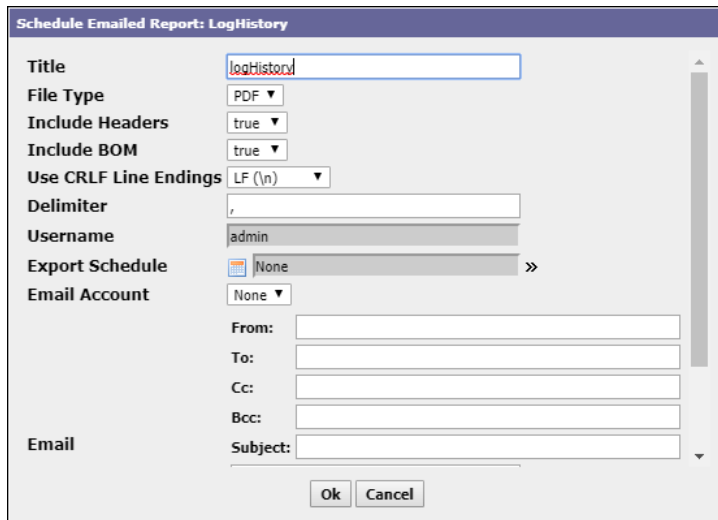
Property	Value	Description
Name	text	Defines a unique name for the report.
Navigation Path	hierarchy (defaults to None)	Selects where in the station hierarchy to store the new report. The default allows access to the report from the Manage Reports window even though the report does not appear in the menu hierarchy.

Property	Value	Description
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 78 Schedule Emailed Report window



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

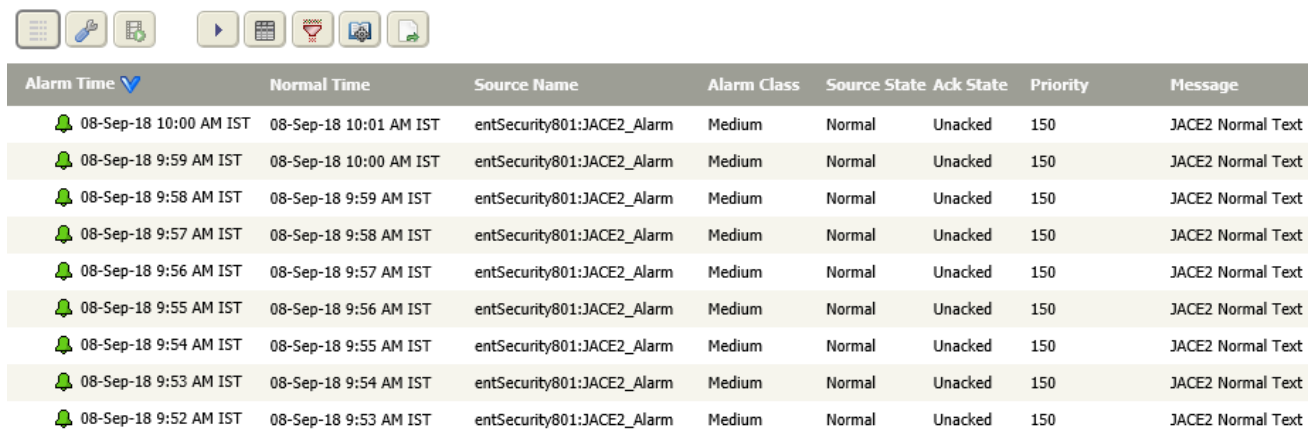
Property	Value	Description
Title	text	Creates a title for the email.
File Type	drop-down list (defaults to PDF)	PDF creates a PDF file.CSV creates a comma delimited file.
Include Headers	true (default) or false	Configures the inclusion of report headings.
Include BOM	true (default) or false	
Use CRLF Line Endings	drop-down list	Configures how to terminate each line of the report: LF = line feed, CRLF = carriage return, line feed.
Deliminator	character (defaults to comma (,))	Defines the character used to separate individual fields of inforamtion.
Username	read-only	Identifies the current user.
Export Schedule	Ref Chooser	Opens a list of schedules from which to choose an email schedule.

Property	Value	Description
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 79 Alarm History report







The screenshot shows a row of control buttons at the top: a list icon, a wrench icon, a refresh icon, a play icon, a calendar icon, a funnel icon, a video icon, and a document icon. Below these is a table with the following columns: Alarm Time, Normal Time, Source Name, Alarm Class, Source State, Ack State, Priority, and Message. The table contains ten rows of alarm records, all with a priority of 150 and a message of 'JACE2 Normal Text'.

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 Text
08-Sep-18 9:59 AM IST	08-Sep-18 10:00 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Text
08-Sep-18 9:58 AM IST	08-Sep-18 9:59 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Text
08-Sep-18 9:57 AM IST	08-Sep-18 9:58 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Text
08-Sep-18 9:56 AM IST	08-Sep-18 9:57 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Text
08-Sep-18 9:55 AM IST	08-Sep-18 9:56 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Text
08-Sep-18 9:54 AM IST	08-Sep-18 9:55 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Text
08-Sep-18 9:53 AM IST	08-Sep-18 9:54 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Text
08-Sep-18 9:52 AM IST	08-Sep-18 9:53 AM IST	entSecurity801:JACE2_Alarm	Medium	Normal	Unacked	150	JACE2 Normal Text

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	Reports when the alarm condition returned to normal.
Source Name	Reports the location that caused the alarm.

Column	Description
Alarm Class	Reports the Alarm Class, which identifies alarm routing, for the alarm.
Source State	Reports the current condition of the alarm (in alarm, acknowledged, normal, in alert).
Ack State	Reports if the alarm is unacknowledged or acknowledged.
Priority	Reports the alarm's priority number. The lower the number, the higher the priority.
Message	Reports any message associated with the alarm.
Badge	If the alarm was triggered by an access control violation, identifies the responsible badge.
User	Identifies the user who was logged in when the system generated the alarm.

Alarm history Summary window

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

Figure 80 Alarm History Summary window

The screenshot shows the 'Alarm Details' window with the following information:

- 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/Doors\$204\$20\$2d\$20ICE\$20South\$20Shop\$20Entry\$20Doors\$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
- Alarm Data:**
 - escalated:** true
 - 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

An 'Ok' button is visible at the bottom right of the window.

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 transition from normal occurred, triggering the alarm.
Uuid	Reports the Universally Unique Identifier.
Source State	Reports the alarm's component state transition (normal to offnormal, fault or alert).
Ack State	Reports if the alarm has been acknowledged or is yet unacknowledged.
Ack Required	Indicates if an acknowledgment is required: true means it is required; false means an acknowledgment is not required.
Source	Reports the ORD that created the alarm.

Property	Description
Alarm Class	Reports the routing information for the alarm.
Priority	Reports alarm priority from 1 to 150, where 1 is the highest priority.
Normal Time	Indicates when the alarm condition returned to normal.
Ack Time	Reports when the alarm was acknowledged.
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	Repeats the source state.
Last Update	Reports the last time the system updated this alarm information.

Review Video view

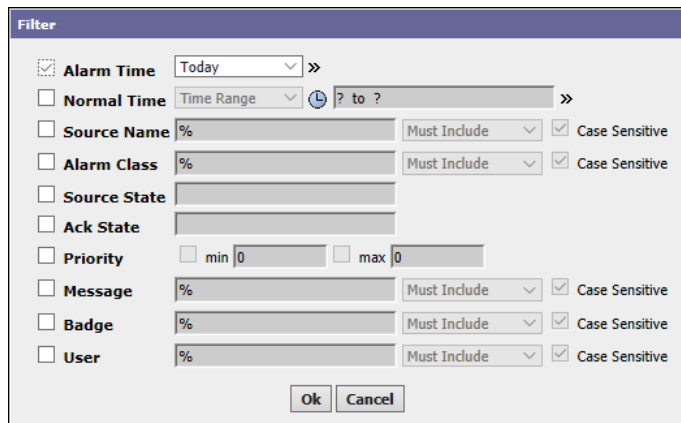
This view plays back the video associated with an alarm.

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 81 Alarm History Filter window



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 ()

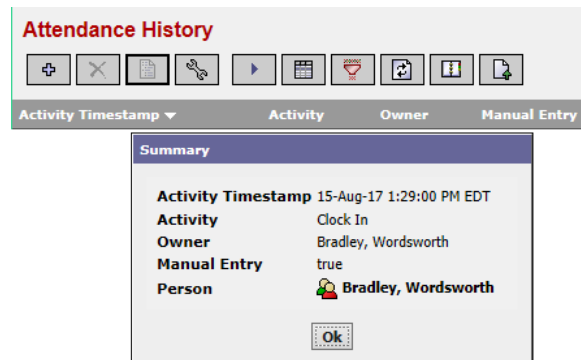
Criterion	Value	Description
Alarm Time	drop-down list	Selects the period of time to include in the report. To further filter report records based on alarm time, refer to a topic titled "Advanced Time Range Options window."
Normal Time	drop-down list and Ref Chooser	Selects a time range for reporting alarms that returned to normal. To further filter report records based on normal time, refer to a topic titled "Advanced Time Range Options window."


Criterion	Value	Description
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 (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 82 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

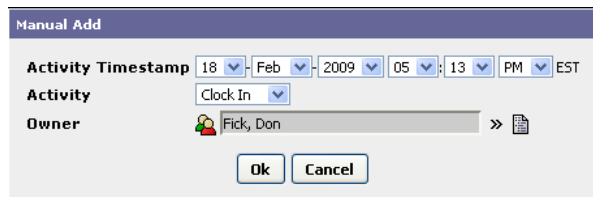
Table 23 Attendance History columns and Summary window properties

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 83 Manual Add window



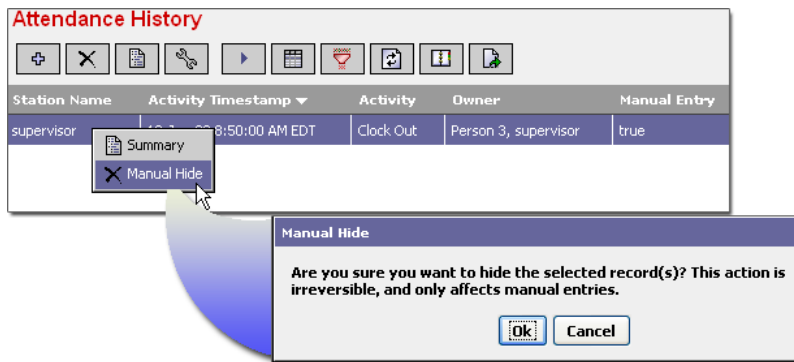
To open this window click **Reports**→**Attendance History** followed by clicking the Add button (.

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

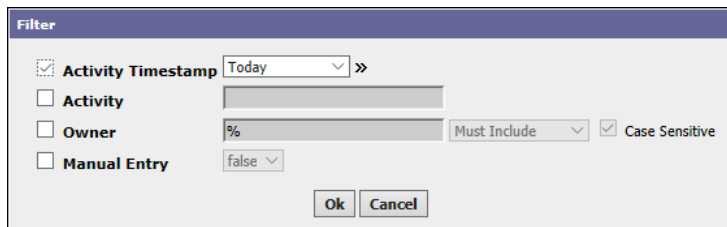
Figure 84 Manual Hide confirmation window (opened using the right-click menu)




Attendance History Filter window

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

Figure 85 Attendance History Filter window



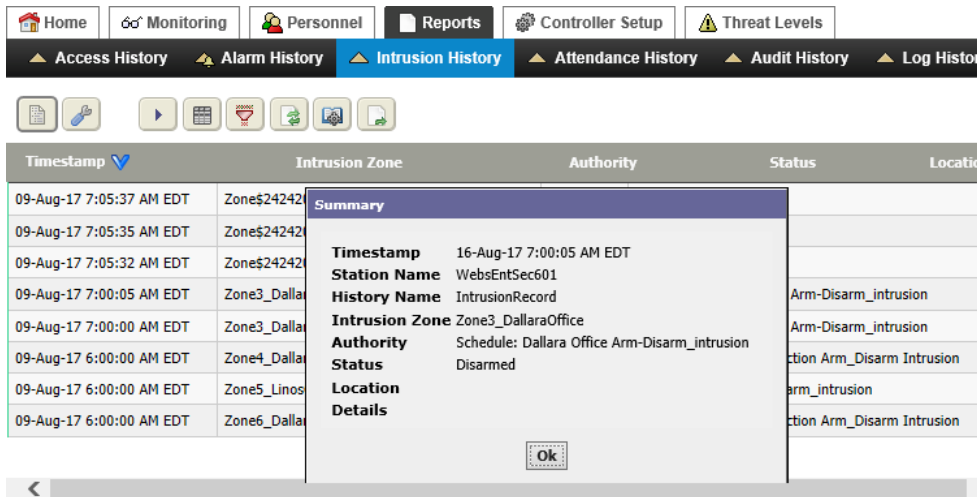
You access this window from the main menu by clicking **Reports**→**Attendance History**, followed by selecting an alarm history record and clicking the Filter button ()

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 86 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

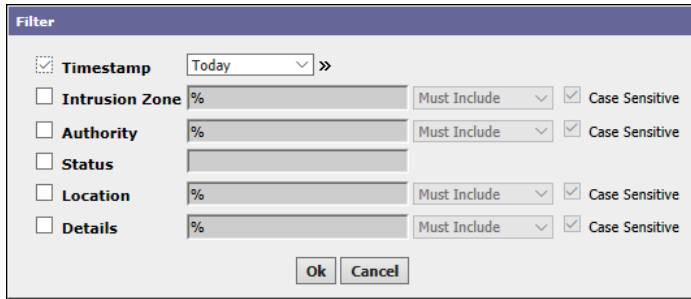
Table 24 Intrusion Zone Report columns and Summary window properties

Column	Description
Timestamp	Reports when the record was written to the database.
Station Name	Reports the station monitoring the intrusion zone.
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}
Location	Reports where the event occurred.
Details	Reports additional information.

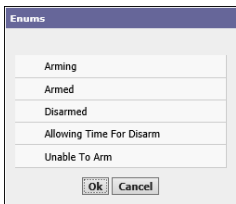
Intrusion History Filter window

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

Figure 87 Intrusion History Filter window



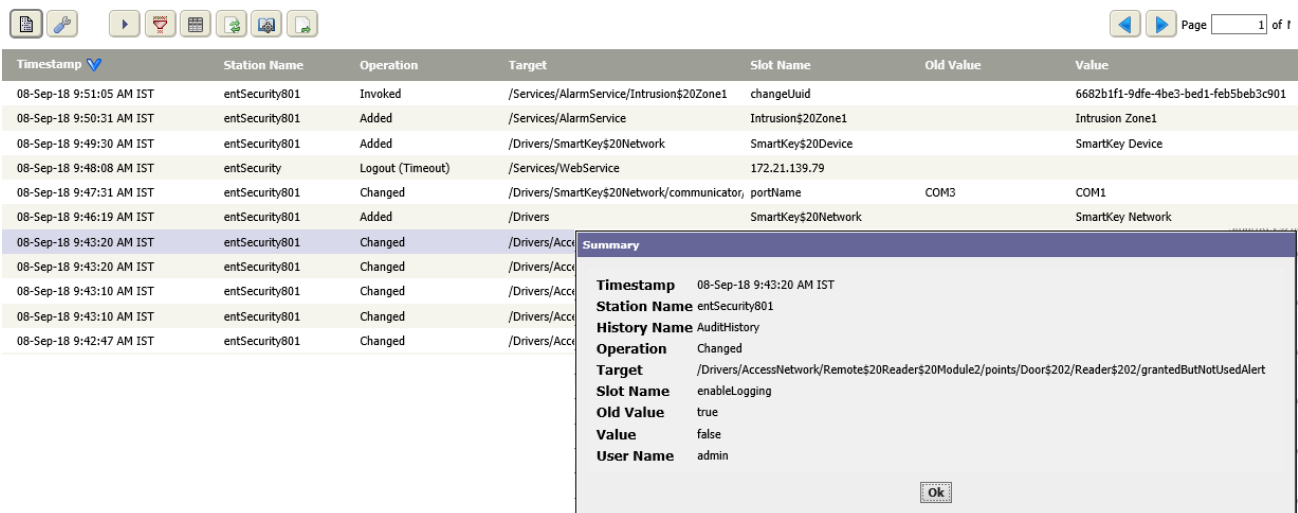
This window opens from the main menu when you click **Reports→Intrusion History**, followed by selecting an alarm history record and clicking the Filter button ()

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: Arming selects event records that occurred when the zone was in the process of arming. Armed selects event records that occurred when the zone was armed. Disarmed selects event records that occurred when the zone was not armed. Allowing Time For Disarm selects event records that occurred when the zone was waiting to receive the code to disarm. Unable to Arm selects event records that occurred when the door was open or some other condition was preventing the zone from arming.
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 88 Audit History report and Summary window



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

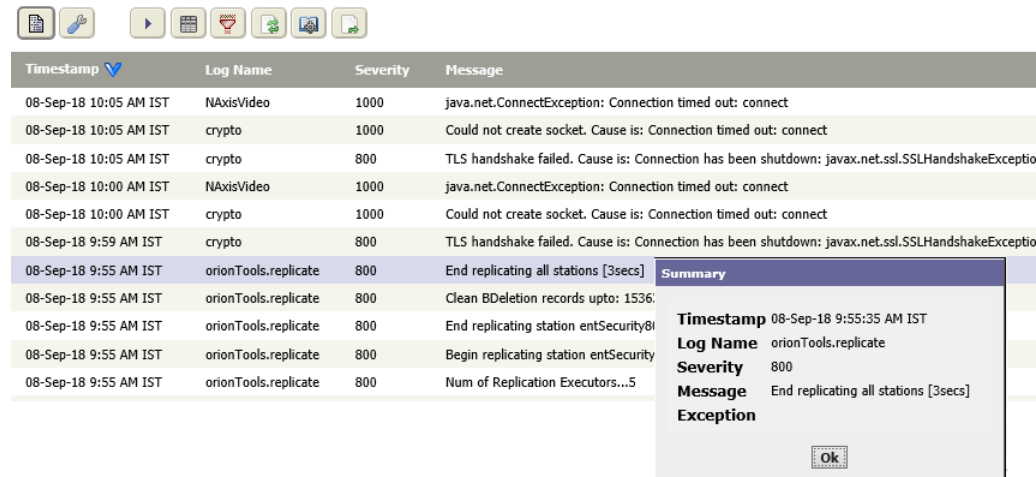
Column/Property	Description
Timestamp	Reports when the record was written to the database.
Station Name	Reports the name of the station that recorded the event.
Operation	Reports a single word to explain the activity: Changed, Invoked, Login, Logout, Removed.
Target	Reports the service to which the history 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 89 Log History report and Summary window





Timestamp	Log Name	Severity	Message
08-Sep-18 10:05 AM IST	NAxisVideo	1000	java.net.ConnectException: Connection timed out: connect
08-Sep-18 10:05 AM IST	crypto	1000	Could not create socket. Cause is: Connection timed out: connect
08-Sep-18 10:05 AM IST	crypto	800	TLS handshake failed. Cause is: Connection has been shutdown: javax.net.ssl.SSLHandshakeException
08-Sep-18 10:00 AM IST	NAxisVideo	1000	java.net.ConnectException: Connection timed out: connect
08-Sep-18 10:00 AM IST	crypto	1000	Could not create socket. Cause is: Connection timed out: connect
08-Sep-18 9:59 AM IST	crypto	800	TLS handshake failed. Cause is: Connection has been shutdown: javax.net.ssl.SSLHandshakeException
08-Sep-18 9:55 AM IST	orionTools.replicate	800	End replicating all stations [3secs]
08-Sep-18 9:55 AM IST	orionTools.replicate	800	Clean BDeletion records upto: 1536:
08-Sep-18 9:55 AM IST	orionTools.replicate	800	End replicating station entSecurity8
08-Sep-18 9:55 AM IST	orionTools.replicate	800	Begin replicating station entSecurity8
08-Sep-18 9:55 AM IST	orionTools.replicate	800	Num of Replication Executors...5

Summary	
Timestamp	08-Sep-18 9:55:35 AM IST
Log Name	orionTools.replicate
Severity	800
Message	End replicating all stations [3secs]
Exception	

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

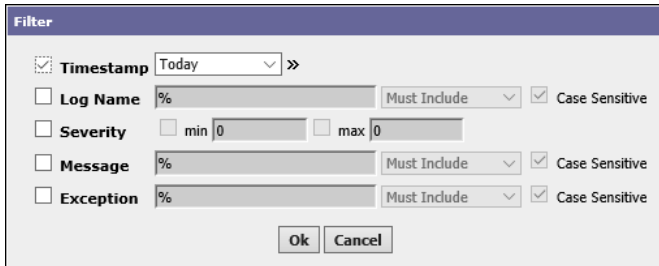
Table 26 Log History columns and Summary window properties


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	Reports any descriptive message associated with the event.
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 90 Log History Filter window






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.
Exception	wild card (%)	Selects based on the exception stack trace, which is available if Severity 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.

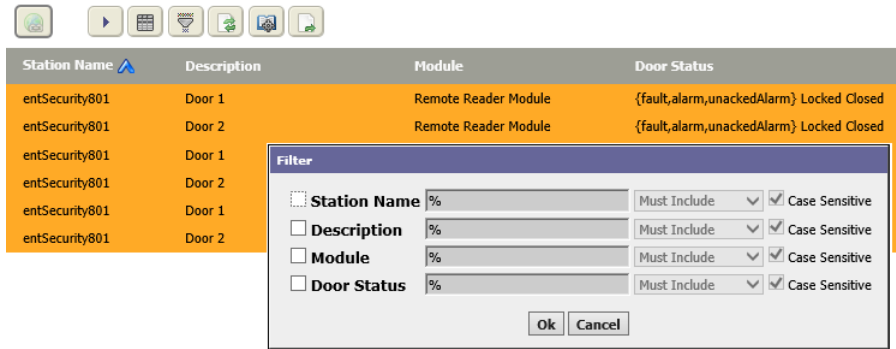
Each hardware report provides the same set of control buttons. In addition to the standard control buttons (Auto Refresh, Column Chooser, Manage Reports and Export), these control buttons provide varying results:

-  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 91 Doors report and Filter window



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

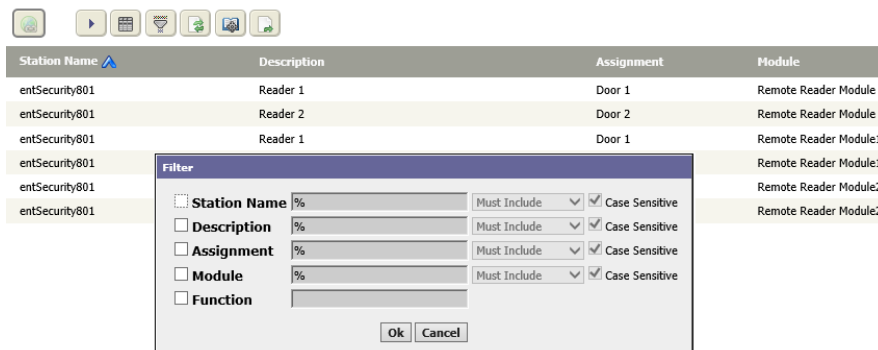
Table 27 Doors report columns and search criteria

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 92 Readers report and Filter window



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

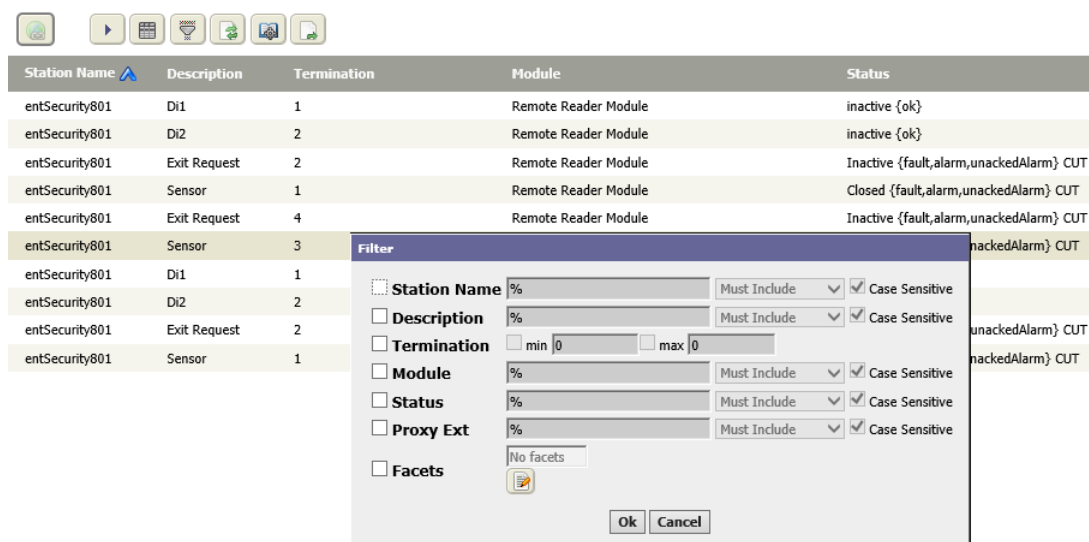
Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the reader.

Column/criterion	Description
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 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 93 Inputs report and Filter window



This report opens when you click **Reports→Hardware→Inputs**. The **Filter** window opens when you click the Filter button (🔍).

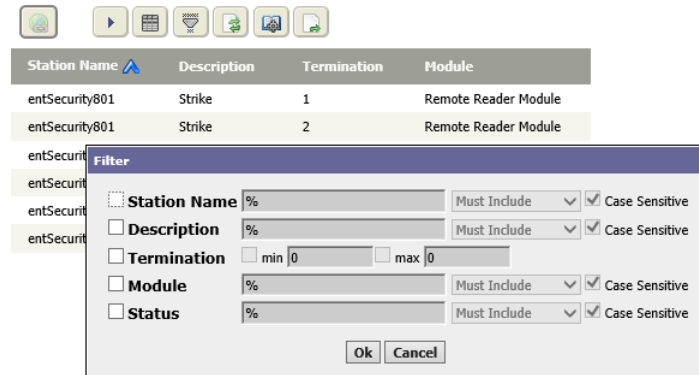
Table 29 Inputs report columns and search criteria

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 94 Outputs report



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

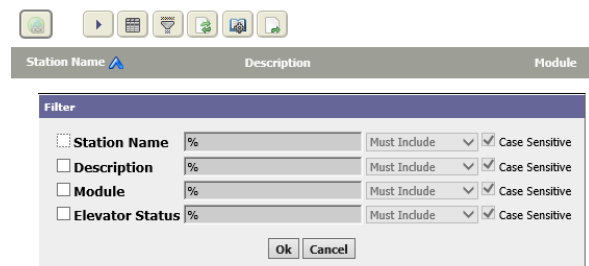
Table 30 Outputs report columns

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 95 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.

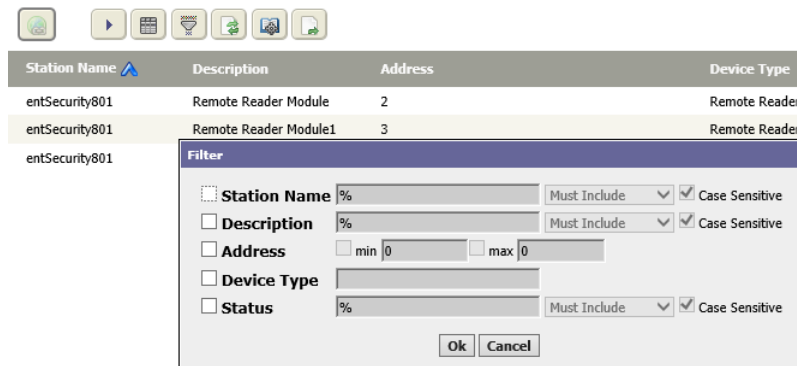
Remote Modules Report and Filter window

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 96 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

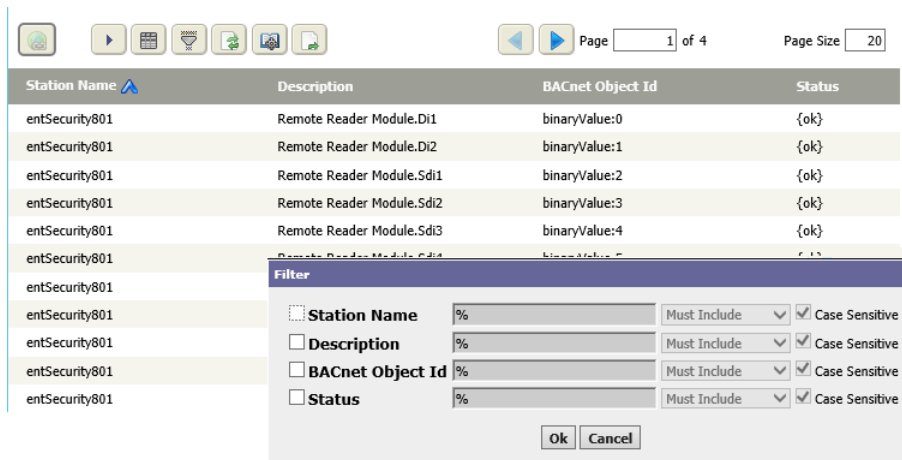
Column/criterion	Description
Station Name	Displays data, and selects data to view based on the name of the managing station.
Description	Displays data, and selects data to view based on any description associated with the module.
Address	Displays data, and selects data to view based on the random integer value assigned to the reader. Each reader has a different integer, which may start from one (1).

Column/criterion	Description
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 Io34 Io34sec
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 97 BACnet Points report and Filter window



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.

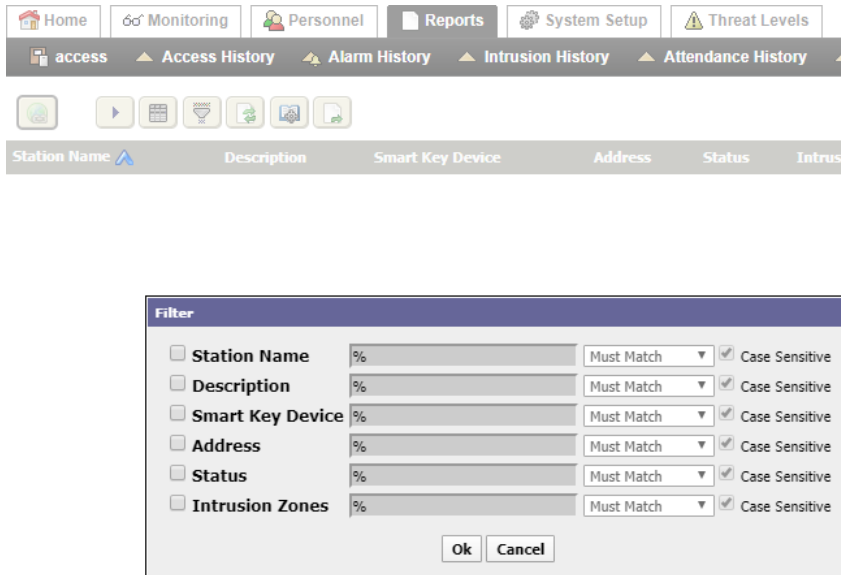
Intrusion Displays Report and Filter


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 98 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.

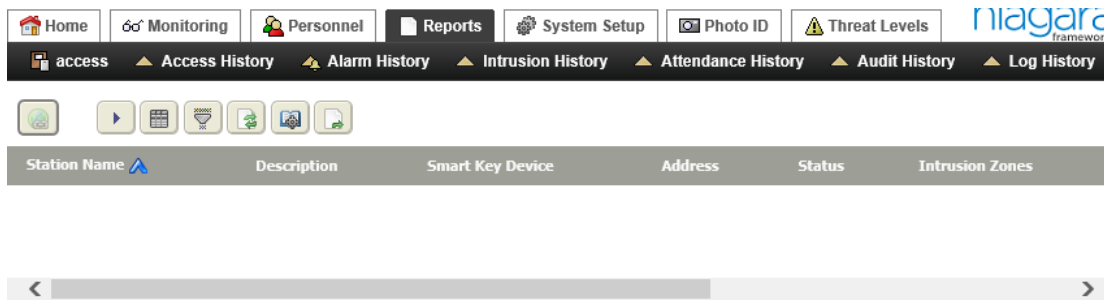
Table 34 Intrusion Displays report columns and search criteria

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



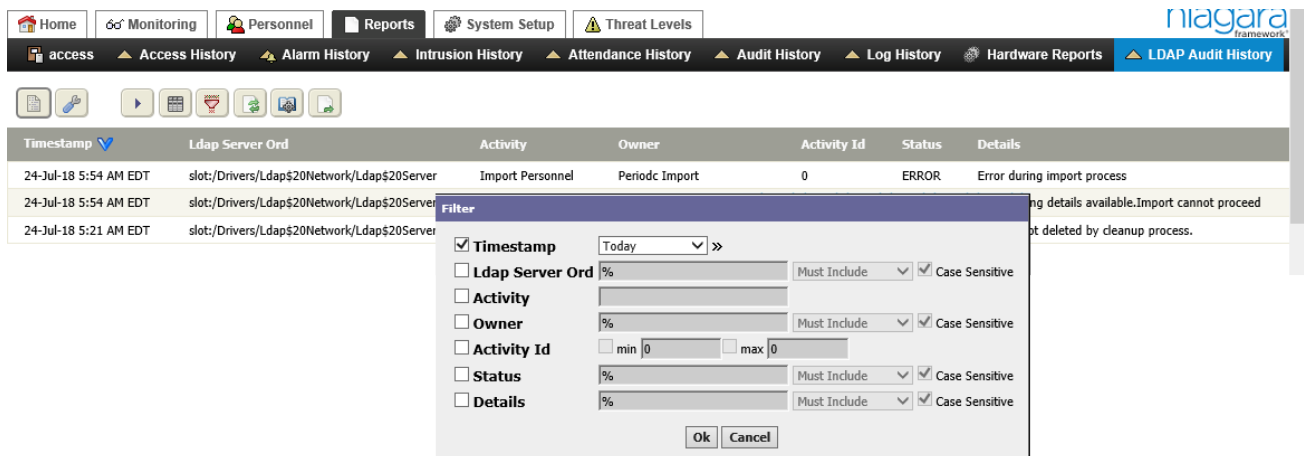
The Consolidated Intrusion Displays report view is available on a Supervisor when you click the **Intrusion Displays** menu item under the **Intrusion Setup** menu or when you select **Reports→Hardware Reports→Intrusion Displays**.

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 100 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.

Column/criterion	Description
Status	Indicates server status when the audit record was created.
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 101 Person Access Right Report and Filter

The screenshot shows a web application interface for the Person Access Right Report. At the top, there are several icons for navigation and actions, and a page indicator showing 'Page 1 of Many'. Below this is a table with the following columns: Person, Access Right Name, Start Date, End Date, and Tenant. The table contains 11 rows of data, all with 'honeywell' as the Access Right Name and 'null' for Start and End Dates. A 'Filter' dialog box is open in the foreground, allowing users to filter the data by Person, Access Right Name, Start Date, End Date, and Tenant. The 'Person' field is currently set to 'None', and the 'Access Right Name' field is set to '%'. There are checkboxes for 'Must Include' and 'Case Sensitive', and 'Time Range' dropdowns for Start and End Dates.

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			

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	Reports the access right associated with the person.
Start Date	Reports when the access right first took effect.
End Date	Reports when this access right will no longer apply to the person.
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 102 Person Reader Report and Filter

The screenshot shows the Person Reader Report interface. At the top, there are several icons for navigation and actions, followed by a pagination control showing 'Page 1 of Many' and 'Page Size 20'. Below this is a table with the following columns: Person, Access Right Name, Reader, and Tenant. The table contains 10 rows of data. A 'Filter' dialog box is open over the table, showing the following fields:




- Person**: None
- Access Right Name**: % Must Include Case Sensitive
- Reader**: None
- Tenant**: None

Buttons for 'Ok' and 'Cancel' are visible at the bottom of the filter dialog.

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

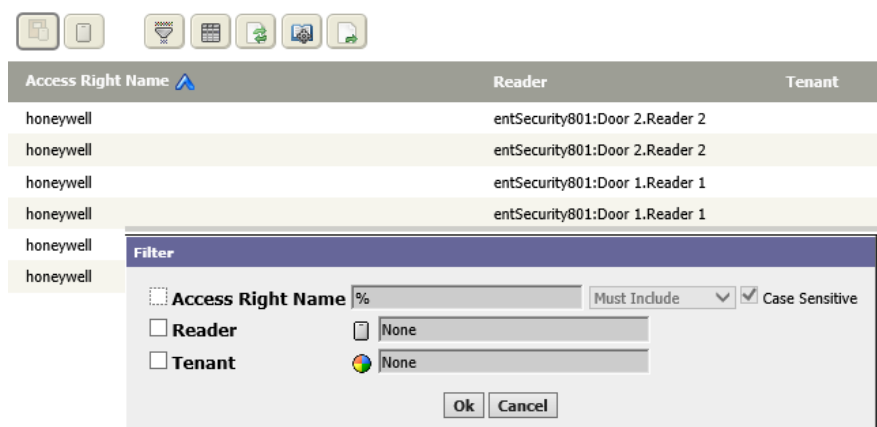
Table 37 Person Reader Report columns

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 103 Access Right Reader Report and Filter



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 104 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

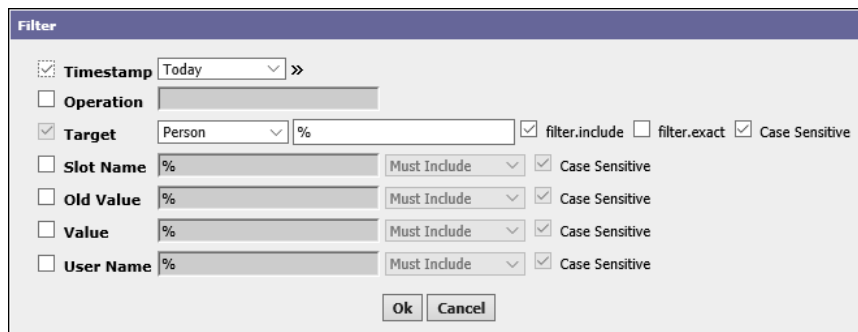
Column/Property	Description
Timestamp	Reports when the record was written to the database.
Operation	Indicates what happened to the record: Added, Changed or Removed.
Target	Identifies the database and person's name.
Slot Name	Identifies what changed.

Column/Property	Description
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 105 Personnel changes Filter window



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 (%)	Defines the records to view: Person selects changes made to specific people. Badge selects changes made to selected badges. Access Right selects changes made to specific access rights. Tenant selects changes made to tenant records. Person Acc Join selects changes made to a person’s access right. The access right is associated with a person or badge.
Slot Name	wild card (%)	Defines what changed.
Old Value	wild card (%)	Defines the value before the change.
Value	wild card (%)	Defines the value after the change.
User Name	wild card (%)	Defines the type of user, such as admin, operator etc.

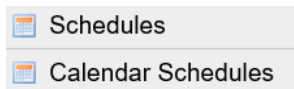
Chapter 5 Controller (System) Setup–Schedules

Topics covered in this chapter

- ◆ Schedules view
- ◆ Add New (edit or duplicate) Schedule view
- ◆ Calendar Schedules view
- ◆ Add New (or edit) Calendar Schedule view

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

Figure 106 Schedules menu



Schedules view








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

Figure 107 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.

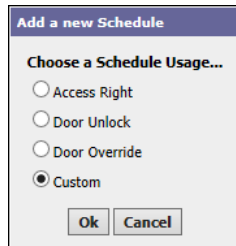
Table 40 Schedules view table default columns

Column	Description
Schedule Name	Identifies the name of the schedule.
Usage	Helps to identify the schedule and provide filtering options when choosing a schedule from a list.
Access Right Name	Identifies the name of the related access right.
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 108 Add a New Schedule window



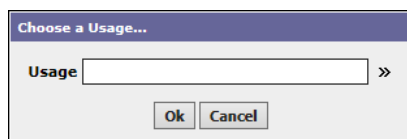
To access this window from the main menu, click **Controller (System) Setup→Schedules**, followed by clicking the Add control button (🟢).

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 109 Choose a Usage... window



This window opens a string chooser.

Schedules Quick Edit window

This window edits schedule properties.

Figure 110 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.
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 111 Schedule Filter window

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.

Summary Scheduler Schedule Setup Special Events Access Rights Intrusion Pins

Start: 09:00 AM EDT
 Finish: 05:00 PM EDT
 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	Reports the name of the schedule.
Usage	Identifies the type of schedule: access right, door unlock, door override, and custom.
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.
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.

Scheduler 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 112 Scheduler tab

Summary Scheduler Schedule Setup Special Events Access Rights Intrusion Pins

12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM

Sun Mon Tue Wed Thu Fri Sat

Access Access Access Access Access Access

Start: 08:00 AM IST
 Finish: 06:00 PM IST
 Output: null Access

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

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.

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	The system routes this value to the access device at the schedule 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
Default Output	Access {ok} »				
Cleanup Expired Events	true ▾				
Scan Limit	090 d 00 h 00 m [1day - +inf]				
Last Modified	21-Jun-18 5:01 PM IST				
Out Source	Default Output				
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"/> Access »				
False Text	<input type="text"/> 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 or false	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 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.

Property	Value	Description
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	read-only	Reports the current out value.
In	read-only	Reports the current input value.
Next Time	read-only	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. When you change an output time or value in the Scheduler tab, the value takes effect immediately, however, Next Time may not update for several minutes. Refreshing the browser view may help.
Next Value	read-only	Reports the next scheduled out value (true or false) to occur at Next Time. This value is meaningless if Next Time is null.
Usage	String Chooser	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 Filter window's Usage property to show only access right schedules.
True Text	String Chooser	Defines the text to display when the current time is within the range defined by the schedule. For example, "Unlocked"
False Text	String Chooser	Defines the text to display when the current time is outside of the range defined by the schedule. For example, "Locked"

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.

Figure 113 Special Events editor

The screenshot shows the 'Special Events' editor interface. At the top, there is a navigation bar with tabs for 'Schedules', 'User Management', 'Backups', 'Remote Devices', 'Access Setup', 'Intrusion Setup', 'Alarm Setup', and 'Miscellaneous'. Below this is a 'Save' button and a 'Schedules' dropdown menu. The main interface has several tabs: 'Summary', 'Scheduler', 'Schedule Setup', 'Special Events', 'Access Rights', and 'Intrusion Pins'. The 'Special Events' tab is selected, displaying a table with the following data:

Name	Summary
HappyBirthday	Date: 17 Sep

To the right of the table is a 24-hour time pane. The time slots are listed from 12:00 AM to 12:00 AM. A blue bar labeled 'Access' is shown between 9:00 AM and 3:00 PM. Below the time pane are fields for 'Start', 'Finish', and 'Output':

Start: 09:00 AM IST
 Finish: 03:00 PM IST
 Output: null Access

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.

Buttons above the table

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

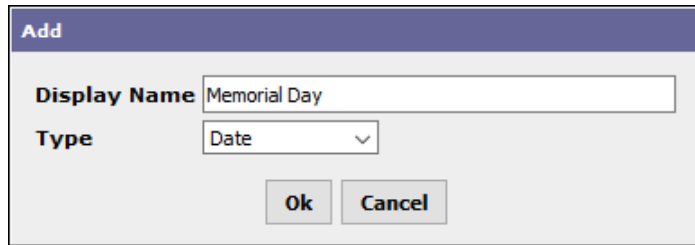
Property	Description
Name	Reports the name that describes the event or function.
Summary	Summarizes the event configuration, for example: Week and Day: Sun Every Week Every Month


Special Events properties

Column	Value	Description
Start	hour:minutes, 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:minutes, AM, PM	Fine tunes the end time.
Output	drop-down list	The system routes this value to the access device at the schedule times.

Add event window

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



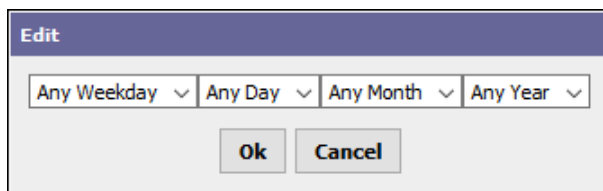
This window opens when you click the Add button () to create a new special event.

Property	Value	Description
Display Name	text	Defines a name that describes the event or function.
Type	drop-down list	<p>Determines the selection criteria for day or days, with the following choices: <i>Date</i>:(default) defines type by various combinations of weekday, numerical date, month or month combinations, and year.</p> <p>Refer to .</p> <p>Refer to Add (or edit) date range window, page 128 <i>Week And Day</i> defines the type by By combination of day of week, week in month, month.</p> <p>Refer to Add (or edit) week and day window, page 128. <i>Date Range</i> defines the type by start and end range, using for each a combination of day, month, year. <i>Custom</i> defines type by various combinations of day, month, weekdays, and year.</p> <p>Refer to Add (or edit) custom window, page 129. <i>Reference</i> adds a pre-defined Calendar Schedule to your calendar if you have one already setup. Selecting Reference 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.</p> <p>Refer to Add (or edit) reference window, page 129</p>

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 114 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.

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

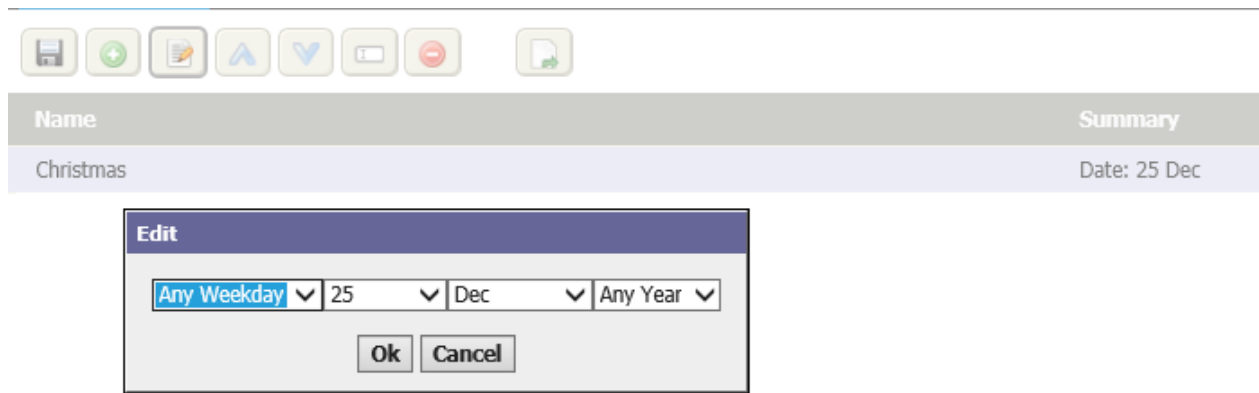
Property	Value	Description
Day of the month	drop-down list, default: Any Day	Identifies the day of the month: 1, 2, ... 31.
Month of the year	drop-down list, default: Any Month	Identifies the month of the year: Jan, Feb, etc.
Day of the week	drop-down list, default: Any Weekday	Identifies the day of 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 115 Example of a referenced calendar schedule



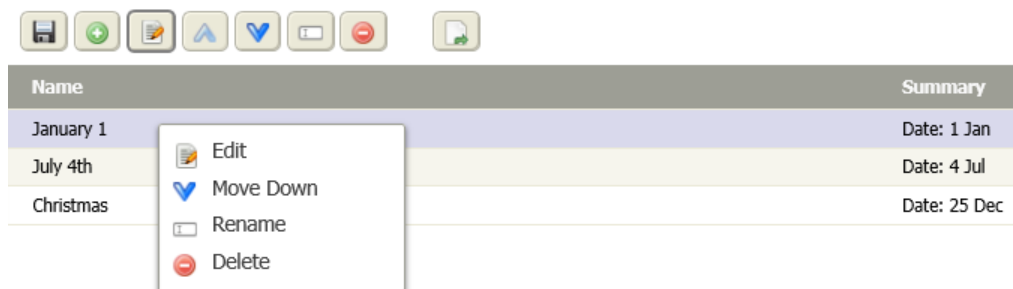
The figure above shows a portion of its **Special Events** tab, listing a single special event that references a calendar schedule. This indicates that the special event (a holiday calendar day) is defined remotely in the configuration of the referenced calendar schedule.

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 116 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 117 Access Rights tab

Newly Assigned

Access Right Name Schedule Name Integration Name Tenant Name Threat Level Group Name





Unassigned

Access Right Name Schedule Name Integration Name Tenant Name Threat Level Group 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 **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 118 Intrusion Pins tab






Summary Scheduler Schedule Setup Special Events Access Rights **Intrusion 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.

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.

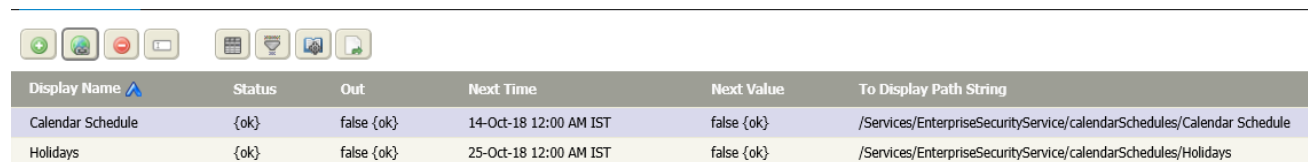
Calendar Schedules view

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 119 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

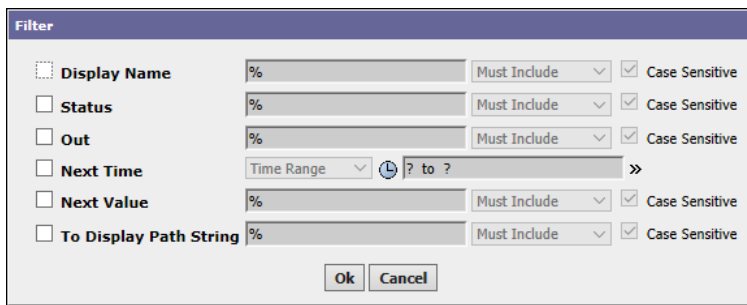
Table 44 Calendar Schedules columns

Column	Description
Display Name	Identifies the schedule name.
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	Reports the display path.

Calendar Schedules Filter window

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

Figure 120 Calendar Schedules Filter window



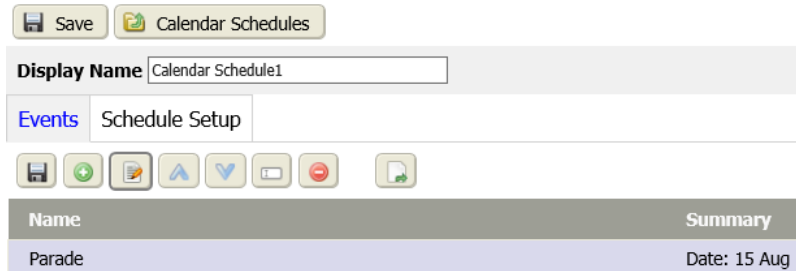
This window opens when you click the Filter button () on the Calendar Schedules view.

Property	Value	Description
Display Name	wild card (%)	Searches for calendar schedule records by name.
Status	wild card (%)	Searches for calendar schedule 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 121 Calendar Schedules view



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:

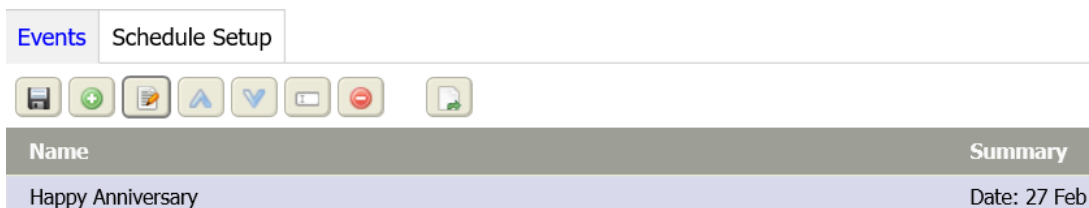
- **Save** stores the schedule in the database.
- **Calendar Schedules** returns to the menu page.

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 122 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

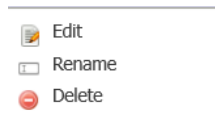
Table 45 Events tab table

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 123 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 124 Schedule Setup tab

Summary	Scheduler	Schedule Setup	Special Events	Access Rights	Intrusion Pins
Default Output		Access {ok} »			
Cleanup Expired Events		true ▾			
Scan Limit		090 d 00 h 00 m [1day - +inf]			
Last Modified		21-Jun-18 5:01 PM IST			
Out Source		Default Output			
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"/> Access »			
False Text		<input type="text"/> 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	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. false configures the system to retain one-time events even though they will not occur again.
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	read-only	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. When you change an output time or value in the Scheduler tab, the value takes effect immediately, however, Next Time may not update for several minutes. Refreshing the browser view may help.
Next Value	read-only	Reports the next scheduled out value (true or false) to occur at Next Time. This value is meaningless if Next Time is null.
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 Controller (System) Setup- User Management

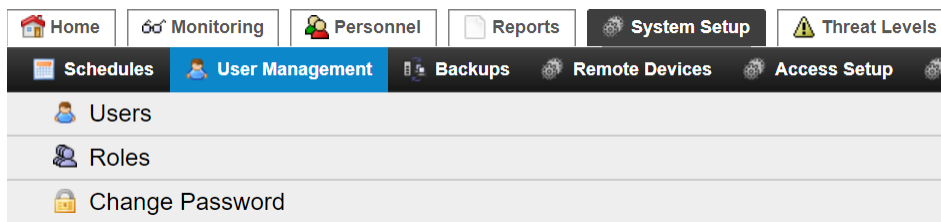
Topics covered in this chapter

- ◆ Users view
- ◆ Add New (and edit) User view
- ◆ Roles view
- ◆ Add New (or edit) Role tab
- ◆ Change Password view

User management includes working with individual user credentials, assigning roles and managing passwords.

A user is a set of properties associated with each person whose responsibility it is to manage the system. User properties include credentials and roles based on which the system grants the associated person the right to log in and use system features. Users are personnel, but not all personnel are users.

User Management views



Users view

This view opens a table that lists the people and software functions authorized to manage the system.

Figure 125 Users view



The screenshot shows the Users view table with the following data:



User Name	Full Name	Roles	Tenants
Engineer		Maintenance	
Personnel Manager		admin	
admin		admin	

This is the default when you click **System Setup**→ **User Management**→ **Users** from the main menu. The table lists all existing user types.

Control buttons

In addition to the standard control buttons (Delete, Rename, Column Chooser, Filter, Manage Reports, and Export), The following control buttons manage this view:

-  Add creates a new user record in the station database.
-  Hyperlink opens an existing user record for editing.

-  Configure opens the Configure window for setting up lockout properties, defining password strength and password configuration.
-  Quick Edit changes a limited set of properties.

NOTE: Button availability is based on the role assigned to the currently-logged in user. For example if the role supports read-only permissions, the Add button is grayed out.

Columns

The table contains the following columns.

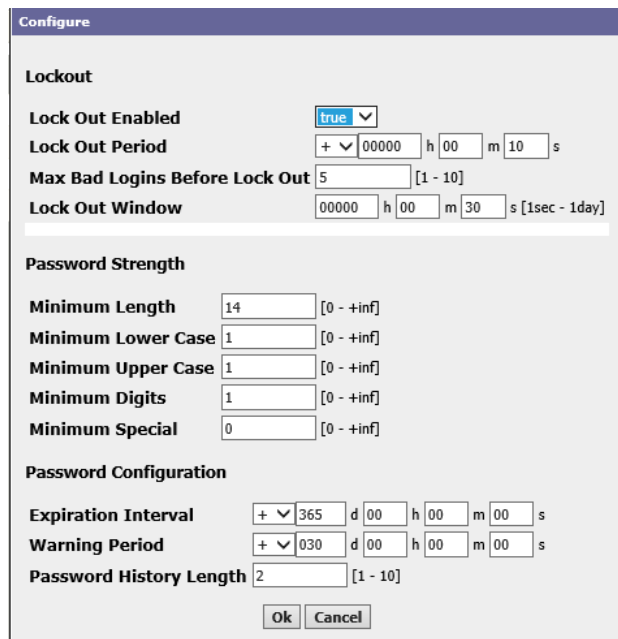
Table 46 Users view columns

Column	Description
User Name	Displays the user name associated with the person, role or machine-to-machine user.
Full Name	Reports a longer name. This could be the first and last name of the person who authorized to use the system or a longer name for a machine-to-machine user.
Roles	Displays the role assigned to this user.
Tenants	Reports the tenant associated with this user.

Configure window

This window configures lock out options and the definition of strong passwords. These requirements apply to all users. You can quickly set password and Lock Out options for one or more users using this view.


Figure 126 Configure window (global password properties)



The screenshot shows the 'Configure' window with the following settings:

- Lockout:**
 - Lock Out Enabled: true
 - Lock Out Period: 00000 h 00 m 10 s
 - Max Bad Logins Before Lock Out: 5 [1 - 10]
 - Lock Out Window: 00000 h 00 m 30 s [1sec - 1day]
- Password Strength:**
 - Minimum Length: 14 [0 - +inf]
 - Minimum Lower Case: 1 [0 - +inf]
 - Minimum Upper Case: 1 [0 - +inf]
 - Minimum Digits: 1 [0 - +inf]
 - Minimum Special: 0 [0 - +inf]
- Password Configuration:**
 - Expiration Interval: 365 d 00 h 00 m 00 s
 - Warning Period: 030 d 00 h 00 m 00 s
 - Password History Length: 2 [1 - 10]

Buttons: Ok, Cancel

You access this window from the main menu by clicking **Controller (System) Setup→User Management→Users**, followed by clicking the Configure button ().

Lockout properties

Property	Value	Description
Lockout Enabled	true (default) or false	true temporarily prevents a user from logging in to a user account after a number of consecutive authentication failures. The user is locked out for the duration of the lock out period (next property). This feature makes it difficult to automate the guessing of passwords. Changing this property opens a second Configure window that allows you to individually set Require Strong Passwords and Lock Out Enabled . The Clear Lock Out button on the Edit User view terminates the locked-out state.
Lockout Period	hours, minutes, seconds (defaults to 10 seconds)	If lock out is enabled, this defines the period of time a user account is locked out before being reset. While locked out, any login attempt (even a valid one) is unsuccessful.
Max Bad Logins Before Lockout	number from 1 to 10 (defaults to 5)	In conjunction with Lock Out Window , specifies the number of consecutive failed login attempts that trigger a user lockout. The system enforces lockout changes on the next login attempt. For example, suppose that Max Bad Logins . . . is set to 5, and a user has failed to log in four times within the Lock Out Window . At that moment, suppose an admin-level user changes Max Bad Logins . . . to 3. The change does not lock out the user who still has one more chance to log in. If the fifth login attempt fails, the user is locked out, since five failed attempts is greater than or equal to the Max Bad Logins . . . setting of 3.
Lock Out Window	hours, minutes, seconds, up to one day (defaults to 30 seconds)	If lock out is enabled, and the number of Max Bad Logins Before Lock Out occurs within this window of time, the user is locked out for the Lock Out Period duration.

Password Strength properties

Property	Value	Description
Minimum Length	number from zero to infinity (defaults to 10)	Defines the fewest number of letters a user can configure.
Minimum Lower Case	number from zero to infinity (defaults to 1)	Defines the fewest number of lower-case letters required.
Minimum Upper Case	number from zero to infinity (defaults to 1)	Defines the fewest number of upper-case letters required.
Minimum Digits	number from zero to infinity (defaults to 1)	Defines the fewest number of numeric digits required.
Minimum Special	number	Defines the fewest number of special characters required.

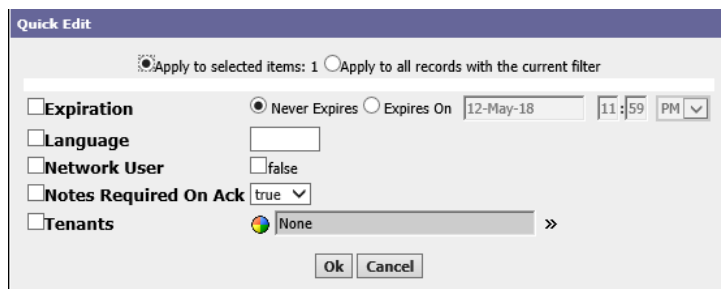
Password Configuration properties

Property	Value	Description
Expiration Interval	days, hours, minutes, seconds	Defines a date in the future when the password expires.
Warning Period	days, hours, minutes, seconds	Defines when the warning period begins before the password expires.
Password History Length	number from zero (0) to 10 (defaults to 0)	Defines how many previous passwords cannot be used. The system stores the history of each user’s passwords and does not allow reuse of the same password up to 10 passwords ago. For example, if this value is two (2), a user could create the same password they had three-times ago, but they could not reuse their password from two times ago.

Quick Edit window

This window presents user properties for quick editing.

Figure 127 Users Quick Edit window



You open this window from the main menu by clicking **Controller (System) Setup→User Management→Users**, selecting a user type row in the table, and clicking the Quick Edit button (📄).

Property	Value	Description
Apply	two radio buttons	Determines to which records the changes apply.
Expiration	radio button and drop-down lists for configuring the date	Sets a predetermined expiration date for a user. <i>never</i> configures the user to never expire. Date option properties—Activates the six date option properties. Edit the Month, Day and Year to set a user expiration date. Edit the hour, minutes, and AM/PM properties set an expiration time.
Language	list of two-character language codes, defaults to the language used by the browser	Specifies a lexicon (for example: <i>fr</i> or <i>de</i>), which identifies language support or other customizing, if available in the current system.
Network User	<i>true</i> or <i>false</i> (default)	Defines if this user definition can be used in other stations. <i>false</i> defines a user that is local to this particular station only. <i>true</i> automatically replicates (or propagates) the user to subordinate stations that are joined under a Supervisor station.

Property	Value	Description
Notes Required on Ack	true (default) or false	Defines if a note is required. true requires a user to enter a note when acknowledging an alarm. true requires a user to enter a note when acknowledging an alarm false disables this requirement.
Tenants	Ref Chooser	Identifies the associated tenant.

Filter window

This window sets up search criteria for users. It is available on the User view.

Figure 128 Users Filter window

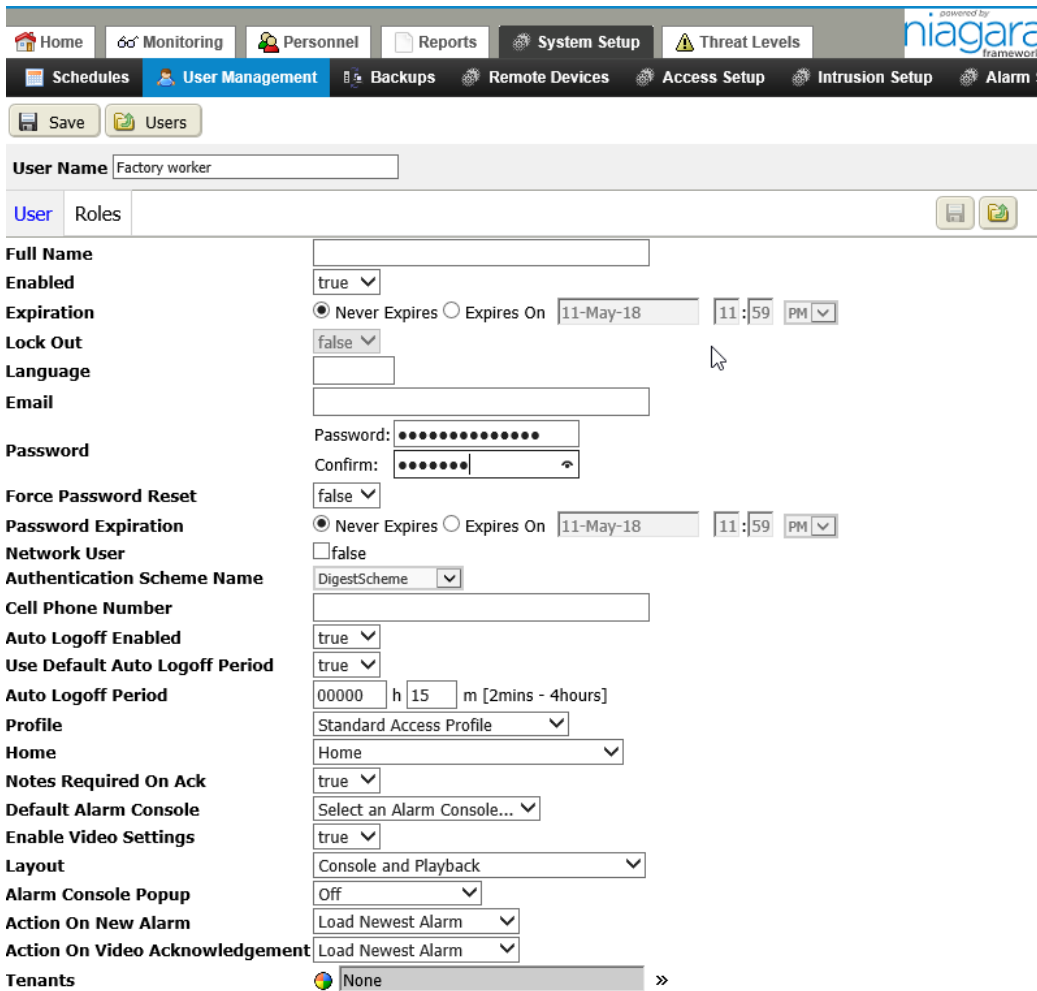
You open this window from the main menu by clicking **Controller (System) Setup→User Management→Users**, followed by clicking the Filter button (🔍).



Criterion	Value	Description
User Name	wild card (%)	Selects a user name (admin, operator, etc.) as a criterion.
Full Name	wild card (%)	Selects the associated person's first and last name as a criterion.
Roles	wild card (%)	Selects a role as a criterion.
Tenants	wild card (%)	Selects a tenant as a criterion.

Add New (and edit) User view

The **New User** view creates and configures system users. These can be people, operational roles, or machine-to-machine users.

Figure 129 Add New User view



To open this view from the main menu, click **Controller (System) Setup**→**User Management**→**Users** and click the Add button (). To open the Edit view, select the user in the table and click the Hyperlink button ().

The **User Name** property appears above the tabbed area. Use it to assign a unique name to the user type.

If an existing user type is in a locked-out state, a **Clear Lockout** button displays at the top of the view. Click this button to immediately clear a user from a locked out state.

The tabs configure user types and the associated role(s).

NOTE: A new user type is not created until you click the **Save** button.

Properties

Property	Value	Description
User Name	text	This can be the name of a person authorized to manage the system, the name of a person type, such as "operator," "administrator," or the name of a machine-to-machine user, such as "obix."
Full Name	text, optional	Assigns a longer name for the user type.

Property	Value	Description
Enabled	true or false	Turns the use of a user type on (<code>true</code>) and off (<code>false</code>). You can enter and maintain user information in the system without having to enable the user type. However, user log-on credentials are not valid unless and until the user type is enabled.
Expiration	radio button and drop-down lists	Sets a predetermined expiration date for a user. <code>never</code> configures the user to never expire. Date option properties—Activates the six date option properties. Edit the Month, Day and Year to set a user expiration date. Edit the hour, minutes, and AM/PM properties set an expiration time.
Lock Out	read-only true or false (available when the Lockout Enabled property is set to <code>true</code>)	Displays <code>true</code> if a user is in a locked-out state. This happens when a user exceeds a maximum number of failed log-in attempts within the defined log-in window of time.
Language	list of two-character language codes, defaults to the language used by the browser	Specifies a lexicon (for example: <code>fr</code> or <code>de</code>), which identifies language support or other customizing, if available in the current system.
Email	email syntax	Specifies a single email address each user logged in to the system with the user type.
Password and Password Confirm	two properties	Specifies and confirms the desired user password.
Force Password Reset	true or false (default)	<code>true</code> requires the user to reset the password at the next login.
Password Expiration	two options with date	Configures password changes. This is a system feature.
Network User	true or false (default)	Defines if this user definition can be used in other stations. <code>false</code> defines a user that is local to this particular station only. <code>true</code> automatically replicates (or propagates) the user to subordinate stations that are joined under a Supervisor station.
Authentication Scheme Name	drop-down list	Selects the scheme for verifying username and password.
Cell Phone Number	telephone number	Provides a place to associate a cell phone number with the user.
Auto Logoff Enabled	true (default) or false	Turns on (<code>true</code>) and off (<code>false</code>) the use of an auto log-off time. If set to <code>true</code> , an Auto Logoff Time is required.
Use Default Auto Logoff Period	true (default) or false	<code>true</code> configures the system to use the default auto logoff period. <code>false</code> requires the configuration of the logoff period.
Auto Logoff Period	Hours, minutes and seconds	Defines the maximum time a user may remain inactive before the system logs the user off. This security measure takes effect when Auto Logoff Enabled set to <code>true</code> .

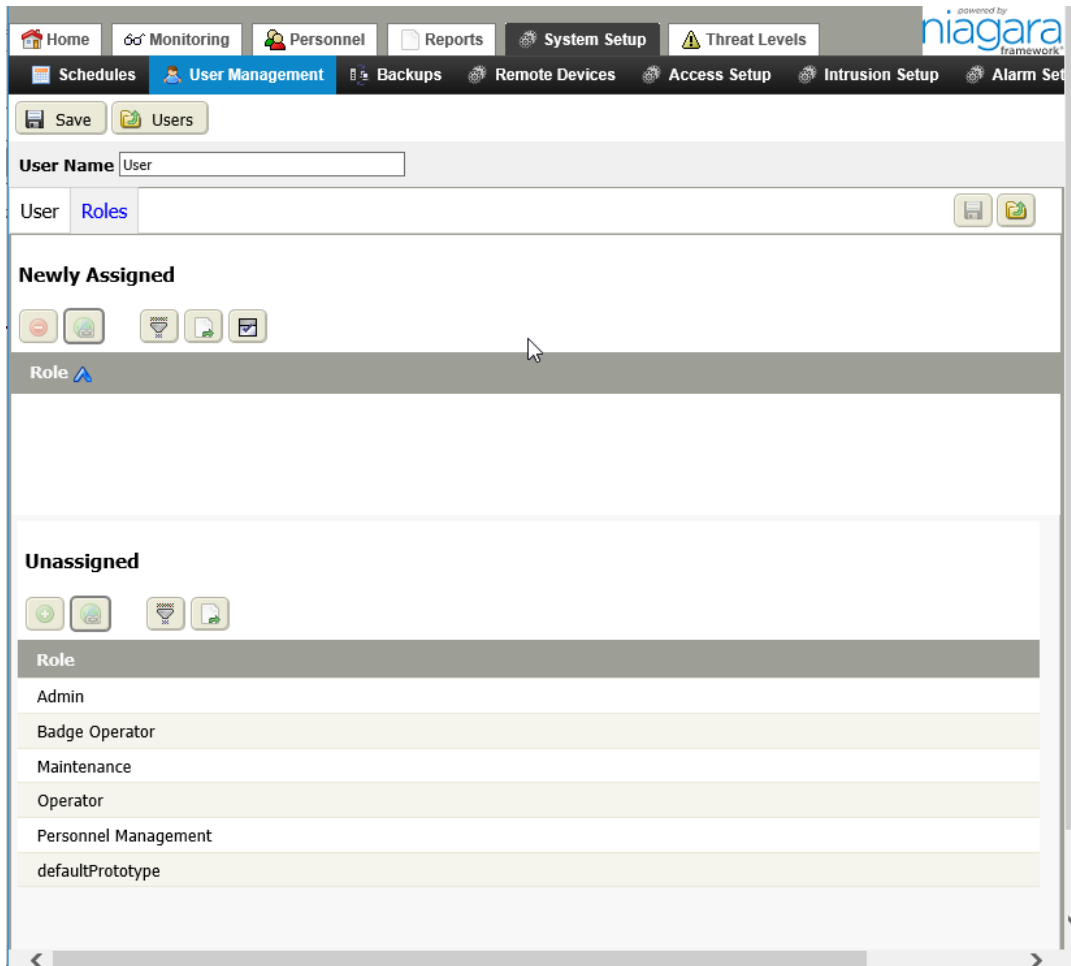
Property	Value	Description
Profile	drop-down list	Selects one of the available user profiles. For most users, the default <code>Standard Access Profile</code> option is used. Select the <code>Personnel Entry Access Profile</code> to provide <code>Personnel Entry Management</code> users a more limited set of views and menu options.
Home	name	Provides a home page you can configure and assign to individual users. The value selected here determines the initial logon page that displays when the user logs on to the application. NOTE: This setting only affects the user's initial logon page and does not change the top-level navigation page that displays when a user clicks the Home link from the main menu.
Notes Required on Ack	true (default) or false	Defines if a note is required. true requires a user to enter a note when acknowledging an alarm. true requires a user to enter a note when acknowledging an alarm false disables this requirement.
Default Alarm Console	text	In cases where you have more than one Alarm Console, this property selects the console that displays initially when an alarm console view opens.
Enable Video Settings	true (default) or false	Displays and hides the video setting properties. When set to false, the following properties do not display in the view: Layout , Alarm Console Popup , Action on New Alarm , and Action On Video Acknowledgment .
Layout	drop-down list	Lists the display options that are available for the Alarm Console - Live view. The options determine what information the live console view displays. Some layouts include one or more video feeds.
Alarm Console Popup	on or off (default)	Enables and disables the alarm console popup feature. When enabled (on), new alarms open an alarm popup window.
Action on New Alarm	drop-down list (defaults to Load Newest Alarm)	For video alarms, determines alarm console behavior when a new alarm (with video) occurs. Load Newest Alarm automatically displays video associated with the latest alarm. Manual Alarm Selection displays no video until you select an alarm in the console.
Action on Video Acknowledgment	drop-down list (defaults to Load Newest Alarm)	Determines the video alarm console behavior when a video alarm is acknowledged from the video alarm controls. Load Newest Alarm automatically displays the video associated with the acknowledged alarm. Manual Alarm Selection displays no video until you select the alarm in the console.
Tenants	Ref Chooser	Opens a list of tenants from which to choose the associated tenant.


Roles tab

This tab manually assigns or unassigns roles to users.

NOTE: Each user must have one or more roles assigned to them. You can create a user of a level equal to or lower than your level. For example, if you logged in as an operator, you cannot add roles of any type.

Figure 130 Add New User Roles tab



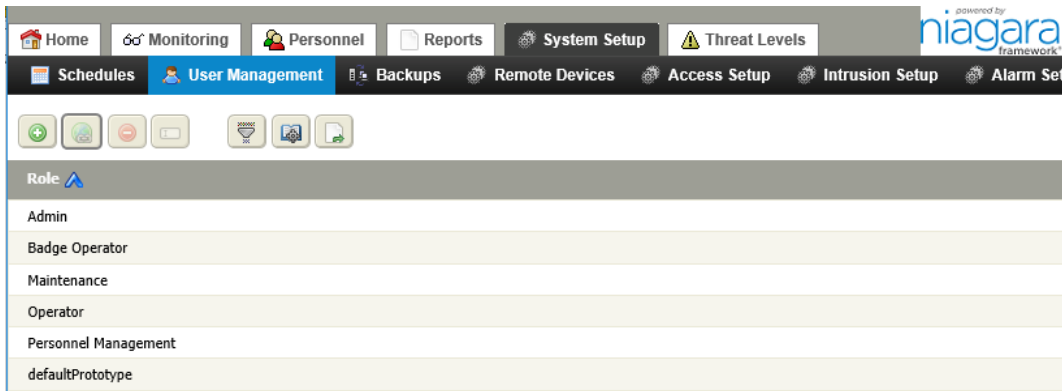
You access this view from the main menu by clicking **System Setup**→**User Management**→**Users**, followed by clicking the Add button (), and clicking the **Roles** tab.

NOTE: You cannot assign a role to the current user. To assign a role, the current user should be the admin or super user.

Roles view

Roles configure a permissions map for each user type that, when assigned to a user, permits the user to make authorized changes to database records.

Figure 131 Roles view



You access this view from the main menu by selecting **System Setup**→**User Management**→**Roles**.

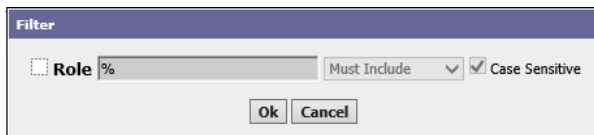
The control buttons (Hyperlink, Delete, Rename, Column Chooser, Filter, Manage Reports, and Export) provide standard functions. The Add button (🟢) opens the **Add New Role** view.

NOTE: Button availability is based on the role assigned to the currently-logged in user. If the role supports read-only permissions, the Add button is grayed out.

Filter window

This window reduces the number of roles listed in the Add New User Roles view. It has the same properties as the Users view **Filter** window.

Figure 132 Roles Filter window



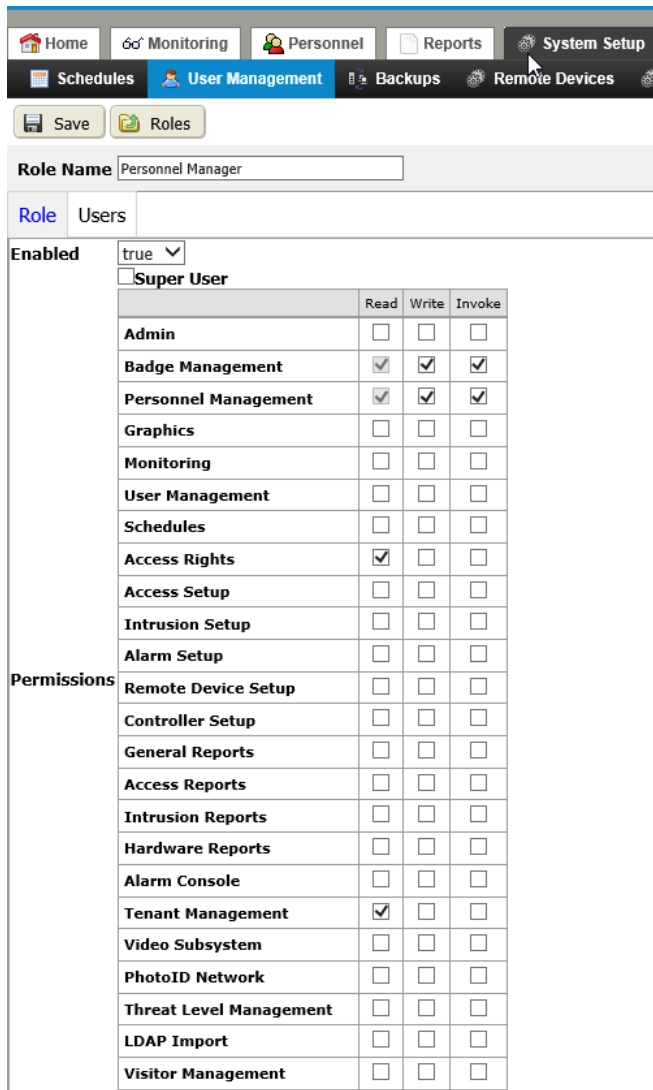
You open this window from the main menu by clicking **Controller (System) Setup**→**User Management**→**Roles**, followed by clicking the Filter button (🔍).

This window has a single property (**Role**) used to limit the table view.

Add New (or edit) Role tab

This view creates and edit roles and provides access to one or more user types that are associated with this role.

Figure 133 Add New Role view



You access this view/tab from the main menu by selecting **System Setup**→**User Management**→**Roles**, followed by clicking the Add button (🟢).

You open this view to edit an existing role by selecting the role from the **Role Manager** view and clicking on the Hyperlink button (🔗).

The number of permissions available in this view is based on the role assigned to the current user. You can create new roles and assign only the permissions that your role allows you to read, write, and invoke.

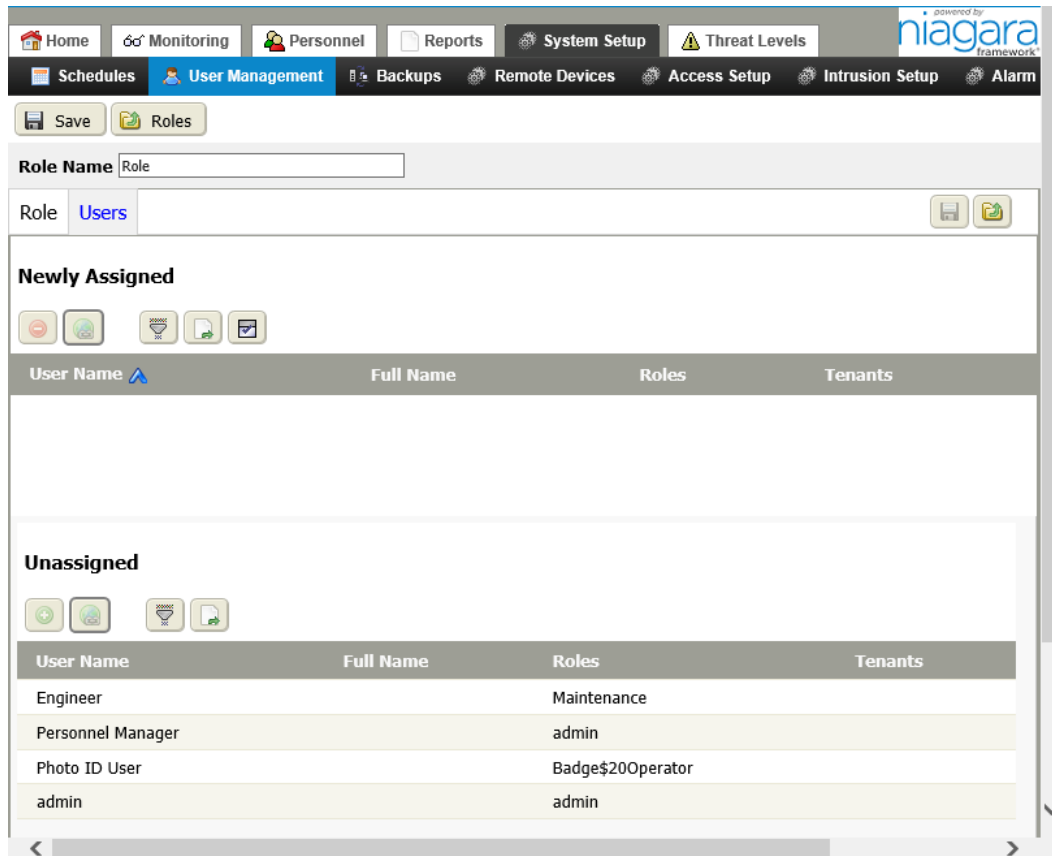
Property	Value	Description
Role Name	text	Provides a name for the role
Enabled	true (default) or false	true assigns the role automatically to user. false requires manual assignment.

Property	Value	Description
Super User	check box	Assigns to the user all permissions (read, write, and invoke) for all available categories, overrides any selections in the Permissions Map and removes the Permissions Map from view.
Permissions map	table of option boxes	Enables and disables individual Read, Write, and Invoke permissions for a list of categories. Selecting a Write level permission automatically sets the corresponding Read level permission for that category. The categories in the table depend on the categories.xml, which you may edit to customize it for individual stations. The default Categories.xml file restores default categories.

Users tab

This tab provides a way to manually assign a role to a user. When the learn mode is selected, all available users display and may be assigned to the currently-displayed role.



Figure 134 Users tab



User types can have more than one role assigned to them. Also, you can only create a user of a level equal to or lower than the level that you are logged in as. For example, if you are logged on as with operator-level privileges, you cannot add roles of any type.

Buttons

In addition to the standard control buttons (Hyperlink, Filter, and Export, these control buttons have special meaning:

-  Unassign removes the selected role from the user.
-  Assign mode opens the **Unassigned Pane** from which to choose roles.

Columns

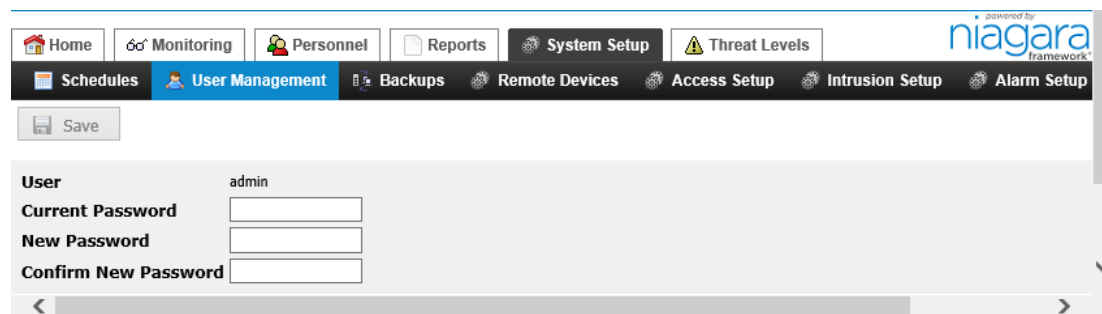
Table 47 New Users columns

Column	Description
User Name	Reports the user name (admin, operator, etc) assigned to the person.
Full Name	Reports the full name of the associated person.
Roles	Reports each role assigned to the user.
Tenants	Reports the tenant, if any, associated with the user.

Change Password view

This view sets a new password for the current user.

Figure 135 Change password view



You access this view from the main menu by clicking **System Setup**→**User Management**→**Change Password**.

Property	Value	Description
User	read-only	Identifies the user name for the user who is currently logged in.
Current Password	text	Prompts you to enter the user's existing password.
New Password	text	Defines the new password.
Confirm New Password	text	Defines the new password again. This property must match the New Password property.

Chapter 7 Controller (System) Setup–Backup views

Topics covered in this chapter

- ◆ Backups view
- ◆ Restore from Backup Distribution File or System Backup File 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

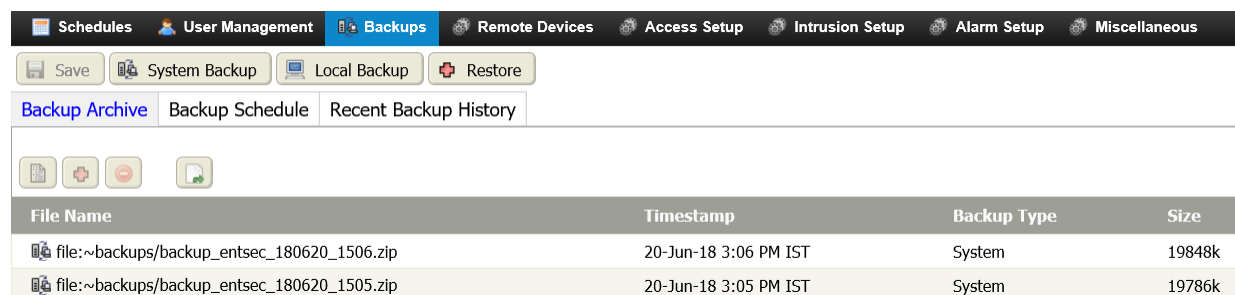
Another difference between Supervisor and controller backups involves the archive that results from making a backup. Archive files made from a Supervisor and subordinate stations have a *.zip file extension. Local archives made from a single controller station have a .dist extension.

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.

Supervisor Backups


Figure 136 Supervisor Backups view



This view opens when you select **System Setup**→**Backups** from the main menu of a Supervisor station.

The primary buttons are located below the view title at the top of the view. They include the following:

- **Save** is dimmed until you make a change in an editable property on the **Backup Schedule** tab.
- **System Backup** initiates a manual backup by of the Supervisor station and all subordinate stations. This button is not available when accessing the Backups view in a controller station.
- **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.

The four control buttons above the table provide standard functions. The unique function for this view is provided by the Restore button ().

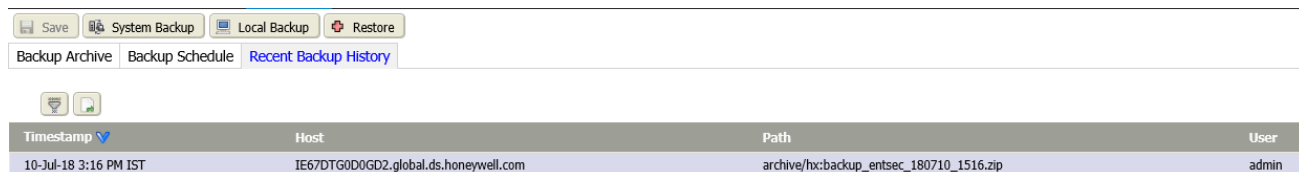
Backup Archive columns

Table 48 Backup Archive columns

Column	Description
File Name	Displays the archived file name and path location. NOTE: 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"> • Local: includes a Supervisor station only • System: includes a Supervisor and its subordinate stations
Size	Indicates the backup file size.

Controller backups

Figure 137 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 49 Backup Archive columns

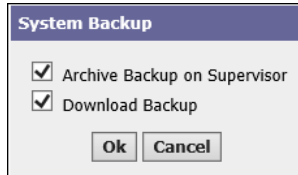
Column	Description
Timestamp	Displays the date and time that the backup was saved.
Host	Reports the host's IP address.

Column	Description
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 138 Example of a System Backup window



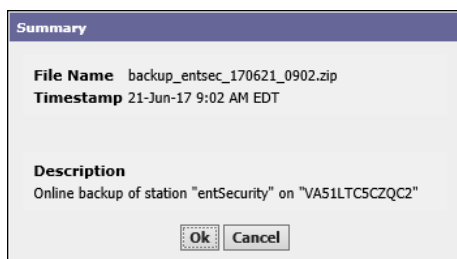
This window opens when you click the **System Setup**→**Backups**, followed by clicking the **System Backup** or **Local Backup** button. The only difference between the **System Backup** and **Local Backup** windows is the window title.

Property	Value	Description
Archive Backup on Supervisor	check box	Saves the backup file to a <code>backups</code> 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 139 Supervisor backups Summary window




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

Table 50 Summary properties

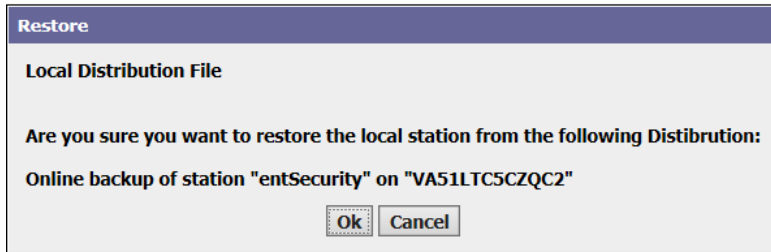
Property	Description
File Name	Identifies the backup file name.
Timestamp	Reports when the backup was created.
Description	Provides additional information.


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 140 Restore window

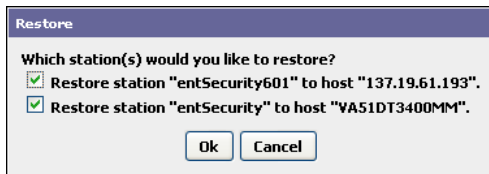



This window opens when you navigate to **System Setup→Backups**, select a Supervisor station backup and click the Restore button (). It asks you to confirm the restoration to the local Supervisor station.

Restore window — remote host

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

Figure 141 Restore window



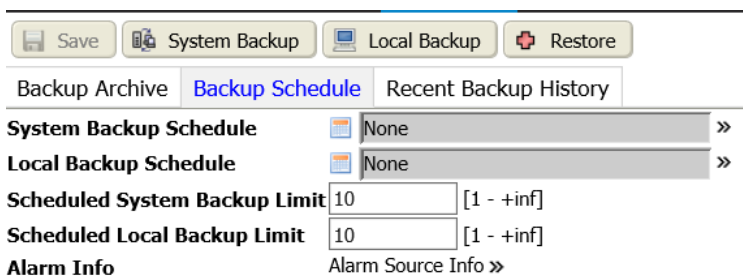
This window opens when you navigate to **System Setup→Backups**, select a host station backup and click the Restore button (). It lists all the available backup files from which you may choose the file to restore to the remote host station. These files are stored in the Supervisor PC’s !backups folder.

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 142 Backup Schedule tab



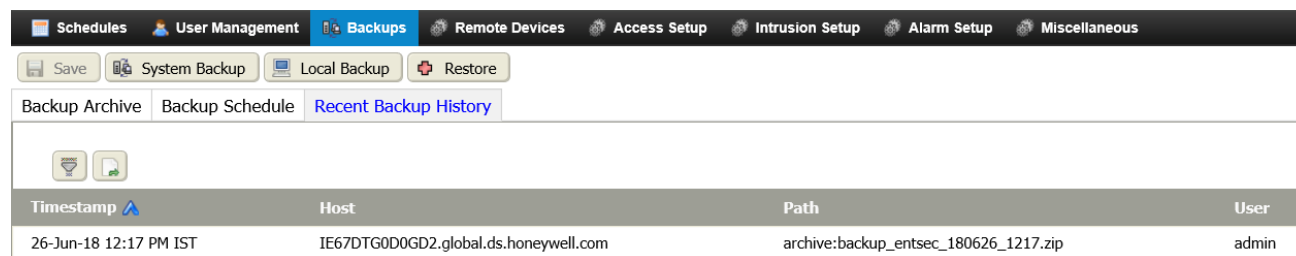
You access this tab by clicking **System Setup→Backups**, followed by clicking the **Backup Schedule** tab.

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	Contains a set of properties for configuring and routing alarms when this component is the alarm source.

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 143 Recent Backup History tab



Timestamp	Host	Path	User
26-Jun-18 12:17 PM IST	IE67DTG0D0GD2.global.ds.honeywell.com	archive:backup_entsec_180626_1217.zip	admin

This view opens when you click the **Recent Backup History** tab on the **Backups** view.

Standard Filter () and Export () control buttons are provided.

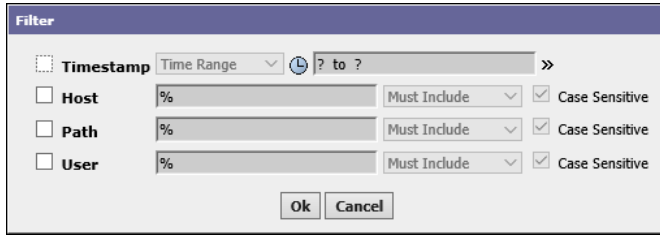
Columns


Table 51 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.



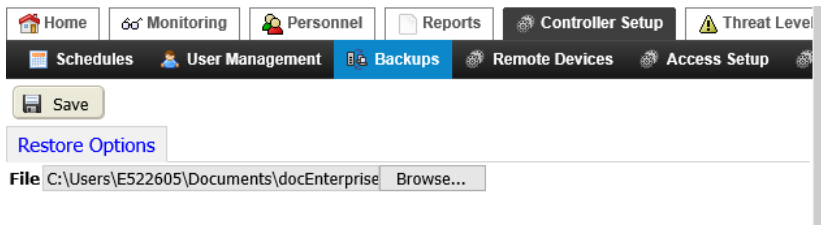
This window opens when you click the Filter button () on the **Recent Backup History** tab of the **Backups** view.

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 144 Supervisor Restore window



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).

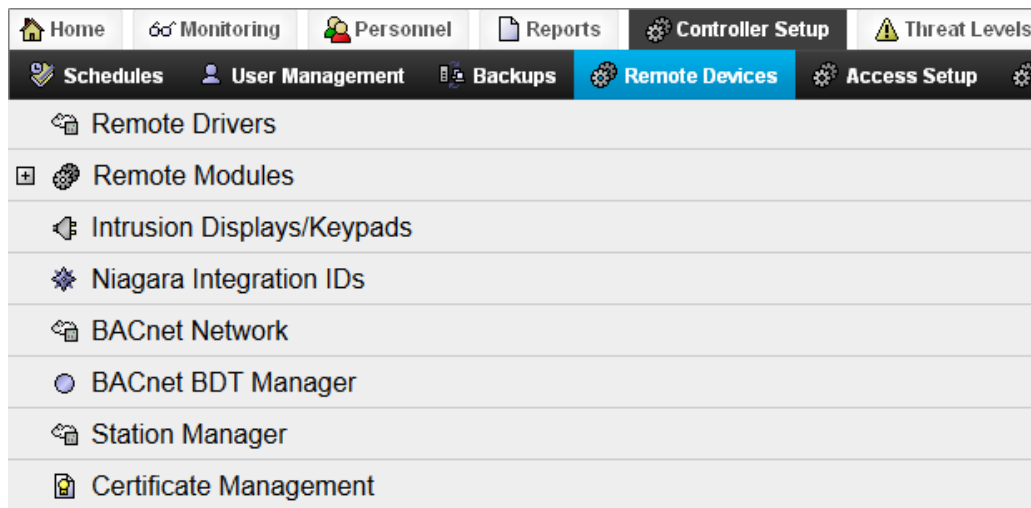
Chapter 8 Controller (System) Setup– Remote Devices

Topics covered in this chapter

- ◆ Remote Drivers view
- ◆ Remote Modules menu
- ◆ Access Device Manager – Database (Remote Module Setup) view
- ◆ Device modules views
- ◆ Door Setup view, Readers tab
- ◆ Reader configuration options
- ◆ Elevators Setup view, Elevator tab
- ◆ Burglar Panel view
- ◆ Edit Unlock Input view
- ◆ Edit Power Monitor view
- ◆ Remote Module Network Identification view
- ◆ Access Network view and tab
- ◆ Niagara Integration IDs view
- ◆ Add New (or edit) Niagara Integration ID view and tab
- ◆ BACnet Network view, BacNet Network tab
- ◆ BACnet BDT Manager (Broadcast Distribution Table) view
- ◆ New (or edit) Entry views
- ◆ Station Manager - Database view
- ◆ Join (Add) Station view
- ◆ Distributed Schedule Manager - Database view
- ◆ Recover Station view
- ◆ Station Device Properties view
- ◆ Certificate Management view
- ◆ Video Network views
- ◆ DVR and NVR views
- ◆ Video camera views
- ◆ Edit Point view, Configuration tab
- ◆ SmartKey Discovery view
- ◆ SmartKey Device Manager - Database view

These views, tabs and windows configure network communication among controllers, their modules, and devices. Several use the network discovery and learn modes to find, add, and configure devices.

Figure 145 Remote Devices view



You access this list of views by clicking **Controller (System) Setup→Remote Devices**.

These views include views that involve network communications between controllers and their modules and devices. Several of these views use the network discovery and learn modes to find, add, and configure devices across the system network.

Remote devices include these views:

- Remote Drivers view
- Remote Modules view
- Module Setup view (edit module configuration)
- Door Setup view
- Reader Setup view
- Elevator Setup view
- Edit Points view
- Edit Burglar Panel view
- Alarm Source Exts view
- Edit Alarm Source Ext Properties
- Network Identification view (Remote Module Identification)
- Access network view
- SmartKey Device Manager - Database view
- SmartKey Device view
- Niagara Integration ID view
- Edit BACnet Network view
- BDT Manager view
- New Entry view and Edit Entry view
- Station Manager - Database view
- Distributed Schedule Manager - Database view
- Add Station view

- Certificate Management view

Remote Drivers view

This view and the views, tabs and windows that open from it manage the network drivers and devices that connect to them.

Figure 146 Remote Drivers view

Name	Status	Enabled	Fault Cause
Axis Video Network	{ok}	true	
Ldap Network	{ok}	true	
Obix Network	{ok}	true	
Photo ID Network	{ok}	true	





You access this view by clicking **Controller (System) Setup→Remote Devices→Remote Drivers**.

These network drivers work with the system:

- Access Network
- Axis Video Network
- Milestone Network
- Obix Network
- Nrio Network
- SmartKey Network

Buttons

In addition to the standard controls, (Filter, Manage Reports and Export), these control buttons provide driver control features:

-  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.
-  Delete removes the selected record (row) from the database table. This button is available when you select an item.
-  Enable/Disable Networks activates and deactivates the selected network.
-  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.

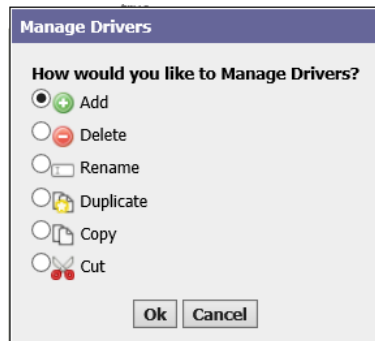
Columns

Column	Description
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}
Enabled	Reports if the function is turned on (true) or off (false).
Fault Cause	Reports the reason for an undesirable status.

Manage Drivers window

This window provides options for managing network drivers.

Figure 147 Manage Drivers window



You access this window from the main menu by clicking **Controller (System) Setup→Remote Devices→Remote Drivers**, followed by clicking the Manage Drivers button ().

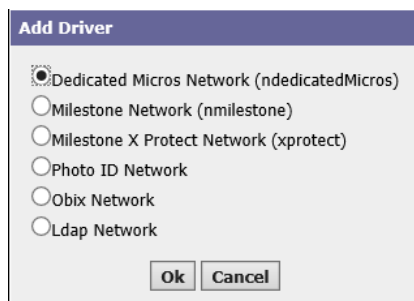
This window provides these options:

- Add opens the **Add Driver** window.
- Delete removes the selected driver from the database.
- Rename asks you to confirm the operation, then opens a window with a text field.
- Duplicate opens the **Add Driver** window with the properties populated by the selected driver.
- Creates a copy of the device, which you can rename.
- Cuts the device, saving a copy in memory. When you select **Manage Devices** again you can create a new device by pasting the cut device into the new record.

Add Driver windows

This window lists all the drivers for which a driver module is available to the controller.

Figure 148 First Add Driver window

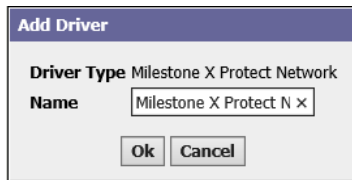


This window opens when you click **Controller (System) Setup→Remote Devices→Remote Drivers**, followed by clicking the **Manage Drivers** button, and selecting the **Add** option in the **Manage Drivers** window and clicking **Ok**.

The drivers listed in this window depend upon your unique software installation. Once you select a driver it no longer appears in this list.

After selecting the driver, another **Add Driver** window opens.

Figure 149 Next Add Driver window



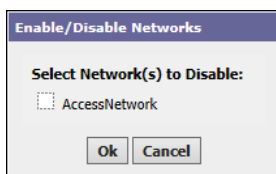
This window opens after you select the type of driver and click **OK**.


You use the **Name** property to provide a customized name for the driver in your system.

Enable/Disable Networks window

This window activates the selected driver.

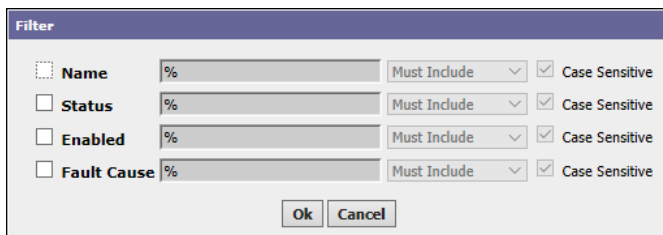
Figure 150 Enable/Disable Networks window




This window opens when you click **Controller (System) Setup→Remote Devices→Remote Drivers**, followed by selecting one or more driver rows in the table and clicking the Enable/Disable Networks button ().

Filter window

This window defines search criteria for limiting the number of records in the table.



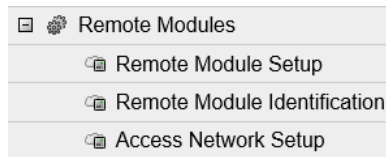
This window opens when you click **Controller (System) Setup→Remote Devices→Remote Drivers**, followed by clicking the Filter button ().

Property	Value	Description
Name	wild card (%)	Searches based on the name of the driver.
Status	wild card (%)	Searches based on current driver status.
Enabled	wild card (%)	Searches for drivers that are currently enabled (<code>true</code>) or disabled (<code>false</code>).
Fault Cause	wild card (%)	Searches for drivers based on the reason they are in fault.

Remote Modules menu

These sub-menu options manage hardware option modules added to the remote controller.

Figure 151 Remote modules

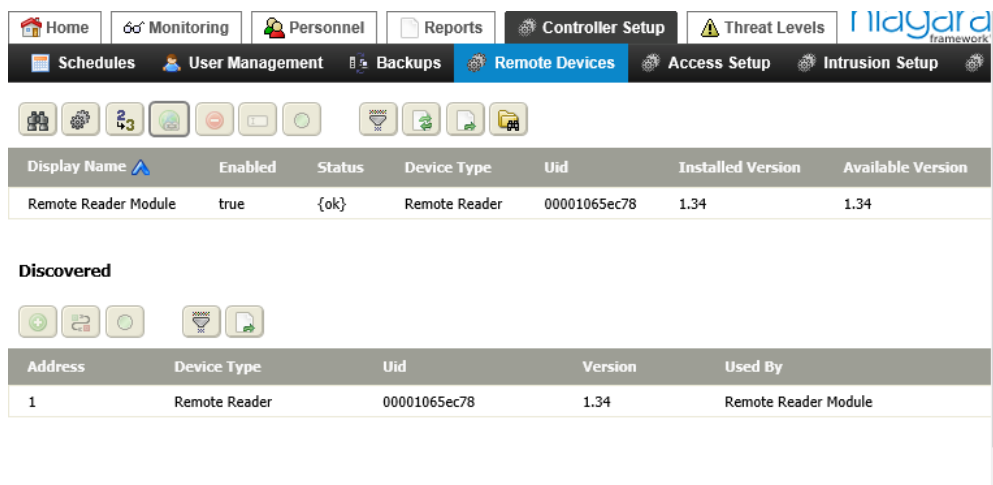


You access these options by clicking **Controller (System) Setup**→**Remote Devices** followed by expanding the **Remote Modules** node in the menu tree.

Access Device Manager – Database (Remote Module Setup) view

This view manages the devices (modules) connected to a remote host controller. It is available only using a controller station.

Figure 152 Access Device Manager - Database view



You access this view in at least one of two ways:

- By clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**.
- Or by double-clicking the **AccessNetwork** row on the **Remote Devices**→**Remote Drivers** view.

Database pane

In addition to the standard control buttons (Discover, Hyperlink, Delete, Rename, Filter, Refresh and Export), the **Database** pane provides these database-related controls:

- 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. The duplicate option provides the ability to quickly create multiple copies of a pre-configured device that is in your database.
- Upgrade Firmware initiates an upgrade of a selected module.
- 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).
- Learn Mode opens and closes the **Discovered** pane to show and hide discovered devices.

Table 52 Database pane columns

Column	Description
Display Name	Names the device.
Enabled	Indicates if the device is on or off.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}
Device Type	Identifies the type of device.
Uid	Universal Identification number
Installed Version	Reports the current version of the driver.
Available Version	Indicates if a more recent version is available.

Discovered pane

This pane opens when you click the Discover button ()

In addition to the standard control buttons (Filter and Export), the **Discovered** pane provides these data-base-related controls:





-  Add button adds the discovered and selected module to the station database.
-  Match associates a reader record that is already in the system database with the actual reader. It is available only when you select the reader in both the **Database** pane and the **Discovered** pane of a manager view. This is usually an item you previously added off line. The added item assumes the properties defined for it in the database. You can edit these properties after matching the item.
-  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 the reader record to the database off line and are using the match function).

Table 53 Discovered pane columns

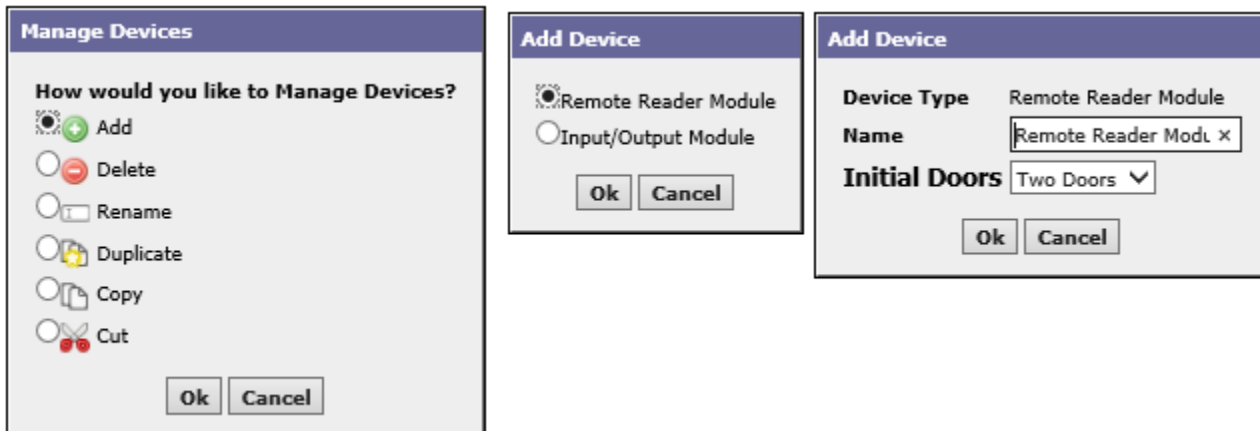
Column	Description
Address	Indicates in what order the system discovered the modules. It does not correlate to how the modules are wired or their physical location.
Device Type	Identifies the type of device.
Uid	Universal Identification number
Version	Identifies the software version of the module.
Used By	Identifies the module that uses this device.

Add Device windows

The manage devices button () appears in several device-related views. When clicked, this button initiates a series of windows used to add, delete, rename, duplicate, copy, and cut and paste devices that are related to a module, door, elevator, or reader. You can use the duplicate, copy and paste options to quickly add new devices.

This window appears in the **Configure Database** view and has analogous options for adding, deleting, renaming and duplicated databases.

Figure 153 Example using Manage Devices windows to add a door



You access these windows by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**, followed by clicking the Manage Devices button (⚙️).

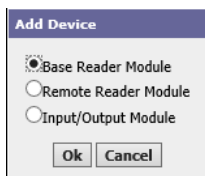
All options work similarly by opening windows to allow you to perform the desired operation. The actions available in this view provide standard features.

Manage Devices window

- **Add** creates a new device record in the database.
- **Delete** removes the device record from the database.
- **Rename** changes the name of the currently-selected device record in the database.
- **Duplicate** creates a new record with the same properties as an existing record. This feature speeds configuring multiple similar devices.
- **Copy** saves the selected record in memory.
- **Cut** deletes the selected record while saving a copy of it in memory.
- **Paste** appears only after you have copied or cut a device.

First Add Device window

Figure 154 First Add Device (modules) window



The screen capture illustrates the addition of three devices (hardware modules):

- **Base Reader Module** is built into the controller base. It supports two readers.
- **Remote Reader Module** connects to a controller base extension. It supports two readers.
- **Input/Output Module** is an interface that receives and sends electrical signals. It supports a wide variety of devices, such as billing controls, window control, etc.

Second Add Device window

This is followed by another **Add Device** window.

Figure 155 Second Add Device (modules) window

Properties

Property	Value	Description
Device Type	read-only	Identifies the type of module.
Name	text	Customizes the device name.
Initial Doors	drop-down list	Defines the number of doors.

Add device window, discovered reader

This window configures a discovered device, such as a card reader.

Figure 156 Add device window

This window opens from the main menu when you click **Controller Setup→Remote Devices→Remote Modules→Remote Module Setup**, discover devices, select a reader device in the **Discovered** pane and click the Add button (🟢).

Property	Value	Description
Device Type	read-only	Displays the type of device you are adding.
Device Name	text	Assigns a unique name to the device.
Device Type	drop-down list	Changes the type of device. Device types include: None Base Board Reader Remote Reader Remote Input Output Io16 Io16 V1 Io34 Io34sec
Enabled	true or false	Turns the feature on (true) and off (false).
Address	number	Identifies a number by which the system accesses the device.

Property	Value	Description
Uid	text	Reports a six-byte number that is globally unique to this specific I/O hardware device. Discovery automatically obtains this Unique ID (Uid) from each device.
Initial Doors	drop-down list (defaults to Two Doors)	Defines the number of doors. No Doors One Door Two Doors

Add device window, discovered Asure ID Client Device

This window configures a discovered Asure ID Client Device.

Figure 157 Add device window

This window opens from the main menu when you click **Photo ID** followed by clicking the Manage Devices button (), clicking **Add**, selecting `Asure ID Client Device` and clicking **Ok**.

Property	Value	Description
Device Type	read-only	Identifies the object to add.
Name	text (defaults to Asure Id Client Device)	Provides a name.
Host Name	text	Identifies the computer on which Asure ID is running.
Entsec AsureID Port	number	Identifies the computer port used to communication with the client device.

Device modules views

Any number of device (hardware) modules can be connected to a remote controller. Most are reader modules.

The view that opens depends on the module you add:

- Input/Output Module

The tabs and options available for each module vary depending on the module.

Links

The links that appear under the module name vary depending on the module. This list includes all the possible links:

- **Save** activates when there are unsaved changes in the view. Click the button to save changes.

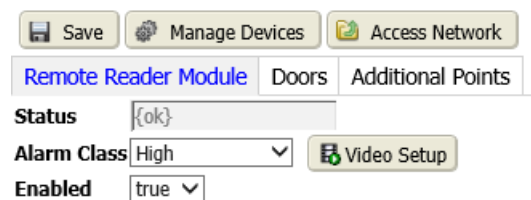
- **Manage Devices** opens the **Manage Devices** window, which adds, removes, duplicates, or renames extensions (such as an access alarm source extension) on the currently selected point.
- **Elevators** links to the **Elevator** tab on the parent device.
- **Schedule Floors** opens the **Schedule Floors** window. You use this window to assign schedules to individual floors.
- **Access Network** links to the **Access Device Manager – Database** view.
- **Manual Override** opens the **Manual Override** window, which configures override properties.

Modules tab

The device modules tabs include the Base Reader Module, Remote Reader Module, and Input/Output Module tabs. These configure components added to a controller for the purpose of connecting card readers and other input and output modules.

Each module has a setup view for listing and editing the configuration of the hardware modules.

Figure 158 Remote Reader Module tab



You access a module tab from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup** followed by creating a new device or double-clicking a selected row in the table. Double-clicking a module row opens a slightly different set of tabs for each module:

- A Base Reader Module opens these tabs: Base Reader Module, Doors, Elevators, Additional Points and Burglar Panels.
- A Remote Reader Module opens these tabs: Remote Reader Module, Doors and Additional Points
- An Input/Output Module opens these tabs: Input/Output Module and Additional Points.

Properties

In addition to the standard properties (Status, and Enabled) this property and button supports a remote reader module.

Property	Value	Description
Alarm Class	drop-down list	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.
Video Setup button	additional properties	Opens the Video Setup window, which selects, enables and configures a video camera to associate with the alarm point or device.

Video Setup window

This window configures video properties.

Figure 159 Video Setup window



You open this window by clicking the Video Setup button on a Modules tab (Remote Reader Module, Base Reader Module).

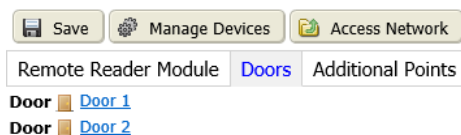
Properties

Property	Value	Description
Video Enabled	true or false (default)	Turns the use of video on (<code>true</code>) and off (<code>false</code>).
Camera	drop-down list	Selects the video camera.
Go to Preset	true or false (default)	Triggers the execution (<code>true</code>) of a preset.
Camera Preset	drop-down list	Selects the camera preset to execute. A preset positions the camera.
Send Alarm To Display	true or false (default)	Turns on (<code>true</code>) and off (<code>false</code>) the display of an associated alarm.

Doors tab

This tab provides hyperlinks to the door configuration view. The view defaults to two doors, but more may be configured if you added them when you created the reader module record.

Figure 160 Doors tab

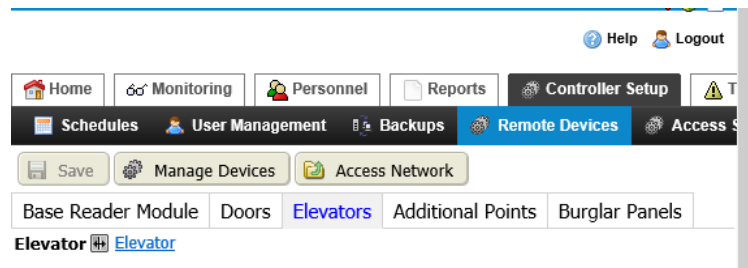


You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**, then either creating a new device or double-clicking a selected row in the table, and clicking the **Doors** tab. What happens when you click one of the door hyperlinks is documented in the topics that begin with “Door view.”

Elevators tab

This tab provides access to one or more elevators.

Figure 161 Elevators tab



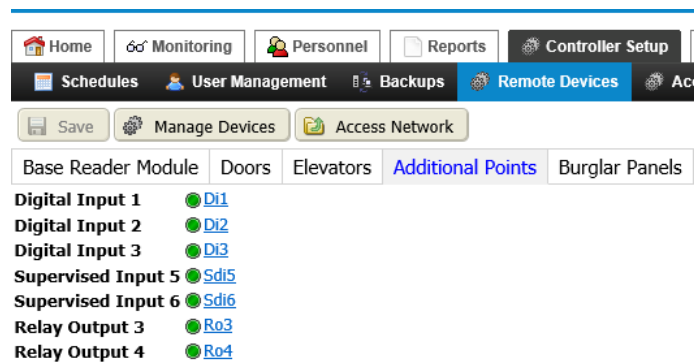
You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**, creating a new device or double-clicking a selected row in the table, and clicking the **Elevators** tab.

What happens when you click one of the elevator hyperlinks is documented in the topic that begins with “Elevator view.”

Additional Points tab

This tab lists additional points associated with the module. Each point links to a tab, which configures the properties for the specific point.

Figure 162 Additional Points tab

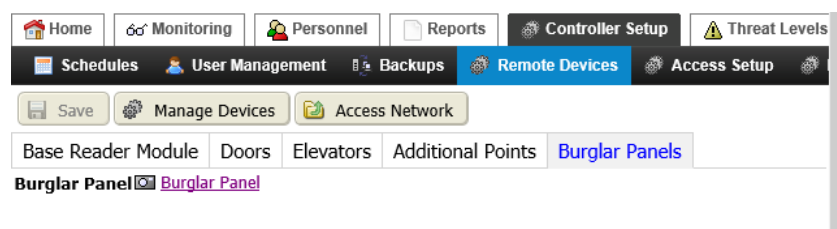


You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**, creating a new device or double-clicking a selected row in the table, and clicking the **Additional Points** tab.

Reader Modules view, Burglar Panels tab

This tab lists one or more burglar panels associated with the reader.

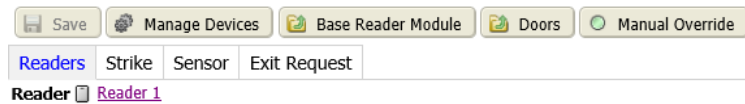
Figure 163 Burglar Panels tab



Door Setup view, Readers tab

This view manages the reader(s), strike, sensor and exit request properties for a specific door. The door view defaults to the **Readers** tab, which links to the reader view associated with this door. The standard is one card reader per door.

Figure 164 Door view with Readers tab selected.



You access this view by clicking **Controller Setup→Remote Devices→Remote Modules→Remote Module Setup**, followed by double-clicking the base reader module row in the table, clicking the **Doors** tab, and clicking the link to a specific door.

Links

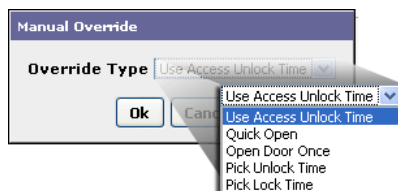
These links under the name of the door provide these functions on all door tabs:

- **Save** activates when there are unsaved changes in the view. Click the button to save changes.
- **Manage Devices** opens the Manage Devices window from which you can add, delete, rename, duplicate, copy, and cut devices.
- **Base Reader Module** returns to the **Base Reader Module** view.
- **Doors** returns to the **Doors** tab.
- **Manual Override** opens the **Manual Override** window from which you can specify lock and unlock options.

Door view, Manual Override window

This window initiates an action to override the system.

Figure 165 Manual Override window



This window opens from the main menu when you click **Controller Setup→Remote Devices→Remote Modules→Remote Module Setup**, add or double-click a remote reader module, click the **Doors** tab, click a door, and click the **Manual Override** button.

The **Override Types** are these:

- **Use Access Unlock Time** configures the door to open as defined by the **Access Unlock Time**, which is defined on the **Strike** tab.
- **Quick Open** unlocks the door momentarily and re-locks it, allowing just enough time for someone standing at the door to open it.
- **Pick Time** specifies a time for the door to remain unlocked.
- **Open Door Once** unlocks the door and leaves it unlocked until you click the **Manual Override** button a second time and confirm to cancel the manual override.
- **Pick Lock Time** specifies a time (in minutes and seconds) to temporarily lock a door that is currently unlocked by an assigned schedule setting. when this override is invoked, the door remains locked until the

configured override time expires or until you click the **Manual Override** button a second time and confirm to cancel the manual override.

Strike tab

This tab configures the unlocking and locking of the door. Door options work in conjunction with the selected Unlock Schedule.

Figure 166 Strike tab

To access this tab, under the **Controller Setup** menu, select **Remote Devices**→**Remote Modules**→**Remote Module Setup** and double-click the door device (module), click the door name, and click the **Strike** tab.

Property	Value	Description
Locked State	Open or Closed	Defines the position of the lock associated with the Door Lock Output property.
Status	read-only	Indicates the current strike state (Locked, Unlocked, and status {ok}, or other possibilities.)
Auto Relock	drop-down list	Defines what should happen with a door that has just been unlocked. Unlock Time permits the door to remain unlocked for the amount of time defined by Access Unlock Time . Relock On Door Open locks the door as soon as it unlocks. Relock On Door Close locks the door either after the Access Unlock Time expires (if the door has been unlocked, but not opened) or when the door closes.
Schedule Operation	drop-down list	Specifies when to set the strike status. All options work with the selected unlock schedule. If no schedule is selected, (property set to none), none of the options are available for specifying how to set the strike status. Normal follows the schedule defined by the Unlock Schedule property. Unlock on first validation causes the strike to unlock (if access is granted) and remain unlocked after the first time access is granted within the scheduled open time. If access is granted outside of the scheduled open time, an unlock-on-first-validation is not performed. Unlock and Relock alternately unlocks and re-locks with each card swipe.

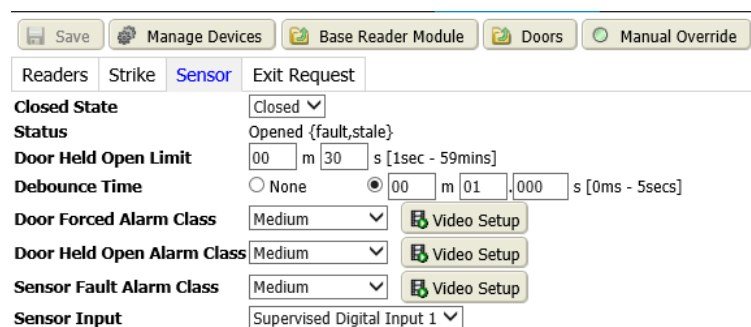
Property	Value	Description
		Follow <code>Another Strike</code> opens a Ref Chooser used to select a module and door strike to follow. Door status reflects the status of the strike to follow. Choosing this option, when the schedule is true, inhibits the door force alarm without waiting for the door to follow to have its strike enabled.
Unlock Schedule	Ref Chooser	Selects a schedule to indicate when a door should be unlocked. <code>None</code> disables all strike properties. If no schedules appear in the Ref Chooser, none may have been created yet. A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Override Schedule	Ref Chooser	Selects a schedule to temporarily unlock and lock the door using a higher priority level than the level assigned to the <code>Unlock Schedule</code> . This sets up an exception to the regular <code>Unlock Schedule</code> .
Access Unlock Time	minutes and seconds (1 second to 59 minutes)	Defines the length of time that a door may remain unlocked after access is granted. Values are only used when <code>Auto Re-lock</code> is set to <code>Unlock Time</code> .
Log Exit Requests	drop-down list (defaults to <code>None</code>)	Defines the conditions under which to initiate a log entry associated only with an exit request at the selected door. <code>None</code> disables exit request logging. <code>Unlocked</code> creates a record any time the door is unlocked. <code>Opened</code> creates a record any time that the door is opened. <code>Unlocked or Opened</code> creates a record any time the door is unlocked or opened.
Log Schedule Activity	<code>true</code> (default) or <code>false</code>	Manages the log for a scheduled activity. <code>true</code> creates a record any time a schedule controls activity at this door. The record may be displayed in the Access History report. <code>false</code> disables the recording of scheduled activity.
Threat Level Group	Ref Chooser	Assigns an optional Threat Level Group to the strike. When assigned, two additional properties display.
Schedule Lock-down Threat Level (Appears when you assign a Threat Level Group to the strike.)	drop-down list (defaults to <code>None</code>)	Specifies a threat level that keeps the door locked no matter what the state of the associated schedule is. The default sets the door to follow the associated schedule without regard to the active threat level. A value other than the default (<code>Low</code> , <code>Normal</code> or <code>High</code>) keeps the door locked as long as the active threat level is at or above that specified here. This value must be greater threat than the value specified in the <code>Unlock Threat Level</code> . If not, the system displays a warning message next to the property when you try to save.

Property	Value	Description
Unlock Threat Level (Appears when you assign a Threat Level Group to the strike.)	drop-down list (defaults to <code>None</code>)	Specifies a threat level that keeps the door unlocked, no matter what the state of the associated schedule is. The default follows the associated schedule without regard to the active threat level. A value other than the default (that is, <code>Low</code> , <code>Normal</code> or <code>High</code>) keeps the door unlocked as long as the active threat level is at or below the level specified here. The value of the Schedule Lockdown Threat Level must be a greater threat level than the value specified by this property, otherwise, a warning message displays when you try to save changes.
Door Lock Output (Appears when you assign a Threat Level Group to the strike.)	drop-down list	Defines the relay output control the strike lock action.

Sensor tab

The properties on this tab configure the door sensor.

Figure 167 Sensor tab



To access this tab, under the **Controller Setup** menu, select **Remote Devices** → **Remote Modules** → **Remote Module Setup** and double-click the door device (module), click the door name, and click the **Sensor** tab.

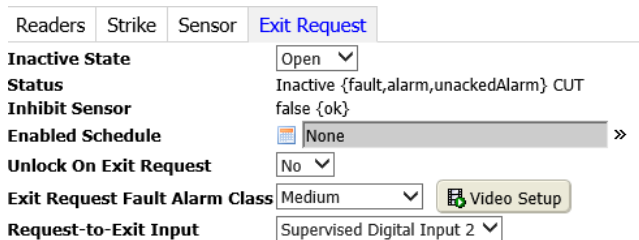
Property	Value	Description
Closed State	<code>open</code> or <code>closed</code>	Defines the normal state of the designated input to match the requirements of the sensor device.
Status	<code>read-only</code>	Indicates the current state of the sensor (<code>Locked</code> or <code>Unlocked</code>), and its status <code>{ok}</code> , or other possibilities.
Door Held Open Limit	minutes and seconds	Defines the length of time that the door is allowed to be held open before the system generates an alarm.
Debounce Time	None (no debounce time used), minutes and seconds (0 minutes to 59 minutes); defaults to 1 second	Minimizes Door Forced alarms around the time of a validation, exit request activation, or manual door override. The intent is to prevent unwanted Door Forced alarms caused by a door bouncing open momentarily just after or just prior to an authorized entry. Two scenarios use this property. In the first scenario, a bounce after open or close occurs when a legitimate open or close is followed by slamming the door, which bounces it open momentarily causing a forced-door alarm. Setting a

Property	Value	Description
		debounce time allows time for a bounce to occur without creating an alarm. In the second scenario, a bounced door can be quickly followed by a legitimate opening when a person attempts to open a door and the door slips out and closes momentarily before the person opens it fully. A bounce closed is not counted if it is less than the debounce time.
Door Forced Alarm Class	drop-down list: Low, Medium, High, or Off.	Sets the priority for a forced door alarm by choosing an appropriate alarm class. <i>Off</i> cancels alarm generation.
Door Held Open Alarm Class	drop-down list: Low, Medium, High, or Off.	Sets the priority by choosing an appropriate alarm class. <i>Off</i> cancels alarm generation.
Sensor Fault Alarm Class	drop-down list: Low, Medium, High, or Off.	Sets the priority for a sensor fault alarm by choosing the appropriate alarm class. <i>Off</i> cancels alarm generation.
Sensor Input	drop-down list	Designates the supervised input to use for the door sensor. Select the associated check box to <i>enable</i> or <i>deselect</i> to <i>disable</i> the selected input.

Exit Request tab

This tab configures exit requests.

Figure 168 Exit Request tab



Property	Value	Description
Inactive State	Open or Closed	Defines the normal inactive state for the designated input to match the exit request device that you are using. This setting matches the normally inactive state of the exit request device.
Status	read-only	Indicates the current state of the sensor (<i>Active</i> or <i>Inactive</i>), and its status { <i>ok</i> }, or other possibilities.
Inhibit Sensor	read-only <i>true</i> or <i>false</i>	Indicates what happens to a door-forced-open alarm during an exit request. <i>true</i> indicates that the door-forced-open alarm stays inhibited during an exit request. This is only possible if Status is <i>Active</i> and Enabled Schedule is <i>true</i> . If either changes, Inhibit Sensor changes from <i>true</i> to <i>false</i> after a time that is equal to the Access Unlock Time . <i>false</i> indicates the door-forced-open alarm manifests during an exit request.

Property	Value	Description
Enabled Schedule	Ref Chooser	Selects the schedule to control the time of day when an Exit Request is enabled and (if Unlock on Exit Request is set to <code>true</code>) unlocks the door on exit. If no enabled schedule is selected (the Enabled Schedule property is set to <code>None</code>), the exit request is always enabled. Choose a schedule from the drop-down list to assign the schedule value to the input.
Unlock on Exit Request	yes or no (default)	Allows an exit request to unlock a door.
Exit Request Fault Alert Class	drop-down list: Low, Medium, High, or Off.	Sets the desired priority for an exit request fault alert by choosing the appropriate alarm class: Low, Medium, High, or Off. The Off setting cancels any alarm generation.
Request-To-Exit Input	check box	Designates the supervised input used for the request to exit sensor. Select the associated check box to <code>enable</code> or <code>deselect</code> to <code>disable</code> the selected input.

Alarm Relay tab

Each door may have one or more alarm relay devices assigned to it. This allows you to choose an alarm extension assignment on a door rather than a control point, as you would do with a Relay Out. The properties for this device are the same as the Relay Out.

Override Input

Each door may have one or more additional override inputs assigned. A separate tab opens for each override input that is added.

Property	Value	Description
Status	read-only	Reports the status of the override input.
Relay In	Ref Chooser	Assigns the relay input source. The system automatically populates the Ref Chooser.

Property	Value	Description
Owner	text	Provides a unique name for the source of the override.
Override Type	drop-down list	<p>Defines the type of override.</p> <p><code>Use Access Unlock Time</code> causes the manual override to use the time defined by <code>Access Unlock Time</code>, under the Reader Setup section of the Hardware Module Setup view.</p> <p><code>Quick Open</code> unlocks the door momentarily and relocks it, allowing just enough time for someone standing at the door to open it.</p> <p><code>Pick Time</code> provides minute and second properties to specify a time for the door to remain unlocked.</p> <p><code>Open Door Once</code> unlocks the door and leaves it unlocked until you click the Manual Override button a second time and confirm that you want to cancel the manual override.</p> <p><code>Pick Lock Time</code> specifies a time (in minutes and seconds) to temporarily lock a door that is currently unlocked by an assigned schedule setting. When this override option is invoked, the door remains locked until the configured override time expires or until you click the Manual Override button a second time and confirm that you want to cancel the manual override.</p>

ADA tab

If a door has an ADA (Americans with Disabilities Act) component, then an **ADA** tab is provided.

This tab provides these configurable or display-only properties.

Property	Value	Description
Inactive State	Open or Closed	Match the normally inactive state of the ADA device.
Status	read-only	Indicates the current state of the ADA component.
Inhibit Sensor	read-only true or false	Indicates if the door-forced-open alarm stays inhibited during an exit request. This property value can be <code>true</code> only if the Status is active and Enabled Schedule is set to <code>true</code> . If either of these values changes, Inhibit Sensor changes from <code>true</code> to <code>false</code> after a time that is equal to the Access Unlock Time .
Unlock on Exit Request	true or false	Configures an exit request to unlock a door. <code>true</code> unlocks the door and powers the ADA output for the ADA Output time. <code>false</code> , configures the ADA device to work only when the door is already unlocked.
Enabled Schedule	drop-down list (defaults to None)	<p>Configures the time of day to enable the ADA functionality. For this to work, the door strike must be unlocked and the schedule must be <code>true</code>. You assign a schedule to the input from the drop-down list.</p> <p>When set to <code>None</code>, ADA functionality is enabled when the door strike is unlocked either by access card swipe or an unlock schedule assigned to the strike. When selected, this schedule adds additional control.</p>
ADA Output	drop-down lists	Defines the relay output to control the ADA device.

Property	Value	Description
ADA Output Time	minutes and seconds)	Defines the length of time that the ADA output signal remains active (to power the ADA device). Values are only used when Auto ReLock option is set to Unlock Time .
Exit Request Fault Alarm Class	drop-down list	Sets the desired priority for an exit request fault by choosing an appropriate alarm class: Low , Medium , High , or Off (cancels any alarm generation).
ADA Input	check box	Uses an option list to designate the supervised input that is used for the activated the ADA device. Select the associated check box to enable or deselect it to disable the selected input.

Relay Out tab

Each door may have one or more additional output relay devices assigned. This tab opens for each output relay device that is added.

Property	Value	Description
Status	read-only	Reports the status of the relay out.
Relay Out	Ref Chooser	Defines which output this relay is connected to by choosing an output (for example, a Strike) from the Ref Chooser window. The system automatically populates this window with the available inputs.
Assignment	Ref Chooser	Defines which input this relay is connected to by choosing an input from the window. This window is automatically populated with the available inputs.
Relay Type	drop-down list	Defines how the relay out behaves relative to the assigned input. You can toggle relay settings on and off or the relay may be out of phase (inverse) with the assigned input. Follow matches the state of the assigned input. Inverse selects the relay out status that is the opposite of the assigned input state. Toggle on active changes the relay from its current state when the assigned input state changes to active. Toggle on inactive changes the relay from its current state when the assigned input state changes to inactive.

Reader configuration options

The **Reader Config** property has five options. This table lists the options and describes how they may be used, depending on whether the reader is assigned to an intrusion zone or to an access device, such as a door, elevator, or floor.

Table 54 Reader configuration options

Option:	Assigned to:	What you do:	What the system does:
Reader Only	Access Point	Enter Credential by card swipe for badge validation.	Checks credential number to authorize or deny access.

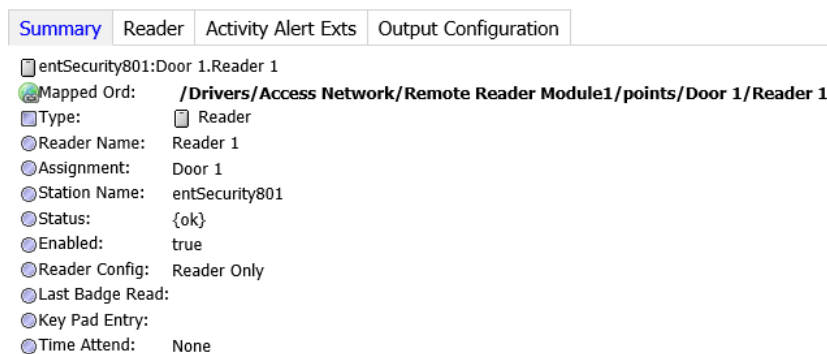
Option:	Assigned to:	What you do:	What the system does:
	Intrusion Zone	Enter Credential by card swipe for badge validation.	Checks credential number to authorize or deny arm or disarm of intrusion zone.
Reader Plus Keypad	Access Point	Enter Credential by card swipe and PIN by keypad for badge and PIN validation.	Checks both the credential number and the Person PIN to authorize or deny access.
	Intrusion Zone	Enter Credential by card swipe AND Person PIN by keypad for badge and PIN validation.	Checks both the credential number and the Person PIN to authorize or deny arm or disarm of the intrusion zone.
Reader or Keypad	Access Point	Enter Credential by card swipe or by keypad entry. Complete credential number is required, including any leading zeros. You may create a custom format to use a shorter, more user-friendly credential here.	Checks credential number to authorize or deny access. Personnel PINs are not UNIQUE, therefore are not used here for authorization. You must enter a complete credential number if you are using a Keypad option.
	Intrusion Zone	Enter Credential by card swipe or keypad entry. Complete credential number is required, including any leading zeros. You may create a custom format to use a shorter, more user-friendly credential here.	Checks credential number to authorize arm or disarm of the intrusion zone. Personnel PINs are not UNIQUE, therefore are not used here for authorization. You must enter a complete credential number if you are using a Keypad option.
Reader or Intrusion Keypad	Access Point	Enter Credential by card swipe	Checks credential number to authorize access
	Intrusion Zone	Enter Credential by card swipe or enter Intrusion PIN at Intrusion Keypad	- If card swipe is used, it checks the credential number to authorize or deny access. - If keypad is used, it checks the Intrusion PIN to authorize arm or disarm of intrusion zone.
Intrusion Keypad	Access Point	No access granted with this option	N/A
	Intrusion Zone	Enter Intrusion PIN at Intrusion Keypad.	Checks Intrusion PIN for validation of arm or disarm.

If you use a 16-bit Wiegand format, and want to allow access using only an entry (not intrusion) keypad, assign a more convenient credential number. You can then create a badge with this format and assign the badge to the person. You can assign more than one badge to a person.

Reader view, Summary tab

This view manages the reader associated with a specific door.

Figure 169 Reader view, summary tab



You access this tab from the main menu by clicking **Controller (System) Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**, followed by double-clicking a module row in the table, clicking the **Doors** tab, clicking the hyperlink for a door, and clicking the hyperlink for the door’s reader.

The **Summary** tab opens by default for this view. It displays a read-only list of all properties, including a link to the **Edit Access Rights** view for any associated access rights listed at the bottom of the summary.

The standard control buttons (**Save** and **Door**) are located under the view title.

NOTE: The reader input and output properties relate to the hardware wiring described in the appropriate *Hardware Mounting and Wiring Guides*.

Table 55 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	Indicates if the reader provides a keypad.
Time Attend	Indicates when the last badge swipe at the reader occurred.

Reader Setup view, Reader tab

This tab provides reader properties.

Figure 170 Reader tab

Summary | **Reader** | Activity Alert Exts | Output Configuration

Status {ok}

Enabled true

Reader Config Reader Only

Time Attend None

Assignment Door 1

Last Badge Read

Key Pad Entry

Threat Level Group ⚠ Threat Level Group1 » 📄 ✕

Elevated Threat Level None

Elevated Threat Reader Config Reader Only

To access this view from the main menu click **Controller (System) Setup→Remote Devices→Remote Modules→Remote Module Setup**, followed by double-clicking a module row in the table, clicking the **Doors** tab, clicking the hyperlink for a door, clicking the hyperlink for the door’s reader, and clicking the **Reader** tab.

Property	Value	Description
Status	read-only	<p>Reports the condition of the entity or process at last polling.</p> <p>{ok} indicates that the entity is licensed and polling successfully.</p> <p>{down} indicates that the last poll was unsuccessful, perhaps because of an incorrect property.</p> <p>{disabled} indicates that the Enable property is set to false.</p> <p>{fault} indicates another problem.</p> <p>Depending on conditions, multiple status flags may be set including {fault} and {disabled}, combined with {down}, {alarm}, {stale}, and {unackedAlarm}.</p>
Enabled	drop-down list; true or false	Turns the reader on and off.
Reader Config	drop-down list	Sets up the required hardware to validate an entry request, as well as a request to arm or disarm an intrusion zone.
Reader model (appears if Reader Config is set up for anything other than Reader Only).	drop-down list	Specifies the reader model: HID5355 or GE T-525/Essex KPT
Time Attend	drop-down list	Sets up the reader to provide a clock in or a clock out message at the time of a badge swipe. If the reader is not used for time and attendance records, choose the None option.
Assignment	read-only	Identifies the name of the door to which the reader is assigned.
Last Badge Read	read-only	Displays badge (credential) number of the last badge swiped at this if reader.
Key Pad Entry	hidden, read-only	<p>Displays the most recent PIN entered at the reader key pad. For security reasons, the value of this property is hidden (blank).</p> <p>While testing during reader configuration, an admin user can view this PIN by disabling the reader (badge validation ceases), and disabling the hide attribute (exposing) this property on the Workbench slot sheet.</p> <p>After reader configuration is complete, the admin user must hide this property again and enable the reader. Otherwise, it will not scan badges.</p>
Threat Level Group	Ref Chooser	Assigns a threat level group to the reader.

Property	Value	Description
Elevated Threat Level (appears when you assign a Threat Level Group to the reader.)	drop-down list (defaults to None)	Defines a threat level for changing the reader configuration. The default ignores any active threat level changes.
Elevated Threat Reader Config (appears when you assign a Threat Level Group to the reader.)	drop-down list	Specifies a reader configuration to enable when the active threat level matches or exceeds the Elevated Threat Level .

Activity Alert Exts tab

This tab provides a set of properties for configuring alarm priority. You can also setup video and enable or disable logging for these alarms.

Figure 171 Activity Alert Exts tab

Summary	Reader	Activity Alert Exts	Output Configuration
Badge Does Not Exist Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Badge Is Lost Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Badge Is Disabled Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Badge Not Assigned Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
No Active Schedule Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
No Access Right Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Granted But Not Used Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Invalid Pin Number Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Connection Problem Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Granted But Connection Problem Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Validation Timeout Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Trace Card Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Inactive Threat Level Group Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging

To access this view from the main menu click **Controller (System) Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**, followed by double-clicking a module row in the table, clicking the **Doors** tab, clicking the hyperlink for a door, clicking the hyperlink for the door's reader, and clicking the **Activity Alert Exts** tab.

The properties you can configure are documented in the topic titled *Add New Access Zone view*.

Output Configuration tab

The contents of this tab depends on the actual outputs that are physically connected to the reader.

Figure 172 Example of an Output Configuration tab

Summary Reader Activity Alert Exts **Output Configuration**

Green

Valid Green

Green Inactive State

Red

Invalid Red

Red Inactive State

Beeper

Valid Beeper

Invalid Beeper

Beeper Inactive State

Beeper on Door Held Open Alarm

To access this view from the main menu click **Controller (System) Setup→Remote Devices→Remote Modules→Remote Module Setup**, followed by double-clicking a module row in the table, clicking the **Doors** tab, clicking the hyperlink for a door, clicking the hyperlink for the door’s reader, and clicking the **Output Configuration** tab.

In the example the red LED, green LED, and beeper are connected to the reader interface. The hyperlinked headings open additional views.

Best Practice: Configure all readers in the building to function in exactly the same way regardless of the type of door lock. Otherwise, occupants will always be trying to figure out what the lights mean.

Property	Value	Description
Valid Green	drop-down list	Specifies how the green LED displays when an access granted signal is received. Inactive leaves the current state of the green LED unchanged when the reader receives an access granted input. Unlock Time activates the reader's green LED for the amount of time defined by the Unlock Time. Follow Strike State changes the state of the reader's green LED based upon the state (locked or unlocked) of the designated door strike. This is not a good choice for an invalid condition because nothing changes state when a request is invalid. Custom Time activates the reader's green LED for the amount of time you designate in the associated Seconds property. Burst activates the reader's green LED in a pattern you define using the associated On, Off, and Burst properties.
Green Inactive State	open or closed	Defines what an inactive green LED means in relationship to the state of the door strike. Use this property to configure this inactive state to match your actual hardware requirements. open configures what inactive means when the door strike is open. closed configures what inactive means when the door strike is closed.
Invalid Red	drop-down list	Specifies how the red LED displays when an access denied signal is received.

Property	Value	Description
		<p><code>Inactive</code> leaves the current state of the red LED unchanged when the reader receives an access granted input.</p> <p><code>Unlock Time</code> activates the reader's red LED for the amount of time defined by the <code>Unlock Time</code>.</p> <p><code>Follow Strike State</code> changes the state of the reader's red LED based upon the state (locked or unlocked) of the designated door strike. This is not a good choice for an invalid condition because nothing changes state when a request is invalid.</p> <p><code>Custom Time</code> activates the reader's red LED for the amount of time you designate in the associated <code>Seconds</code> property.</p> <p><code>Burst</code> activates the reader's red LED in a pattern you define using the associated <code>On</code>, <code>Off</code>, and <code>Burst</code> properties.</p> <p>The <code>Follow Strike State</code> option is not a valid choice for the <code>Invalid Red</code> property because the Strike does not change state for an invalid credential.</p>
Red Inactive State	open or closed	<p>Defines what an inactive red LED means in relationship to the state of the door strike. Use this property to configure this inactive state to match your actual hardware requirements.</p> <p><code>open</code> configures what inactive means when the door strike is open.</p> <p><code>closed</code> configures what inactive means when the door strike is closed.</p>
Valid Beeper	drop-down list	<p>A valid beeper is a sound that provides an audible signal when an access granted message is received. This option list specifies how the beeper sounds when an access granted signal is received.</p> <p><code>Inactive</code> leaves the current state of the beeper unchanged when the reader receives an access granted input.</p> <p><code>Unlock Time</code> sounds the reader's beeper for the amount of time defined by the <code>Unlock Time</code>.</p> <p><code>Follow Strike State</code> changes the state of the reader's beeper based upon the state (locked or unlocked) of the designated door strike. This is not a good choice for an invalid condition because nothing changes state when a request is invalid.</p> <p><code>Custom Time</code> sounds the reader's beeper for the amount of time you designate in the associated <code>Seconds</code> property.</p> <p><code>Burst</code> sounds the reader's beeper in a pattern you define using the associated <code>On</code>, <code>Off</code>, and <code>Burst</code> properties.</p>
Invalid Beep	drop-down list	<p>An invalid beeper is a sound that provides an audible signal when an access denied message is received. This option list specifies how the beeper sounds when an access denied signal is received.</p> <p><code>Inactive</code> leaves the current state of the beeper unchanged when the reader receives an access granted input.</p>

Property	Value	Description
		<p>Unlock Time sounds the reader's beeper for the amount of time defined by the Unlock Time.</p> <p>Follow Strike State changes the state of the reader's beeper based upon the state (locked or unlocked) of the designated door strike. This is not a good choice for an invalid condition because nothing changes state when a request is invalid.</p> <p>Custom Time sounds the reader's beeper for the amount of time you designate in the associated Seconds property.</p> <p>Burst sounds the reader's beeper in a pattern you define using the associated On, Off, and Burst properties.</p>
Beeper Inactive State	open or closed	<p>Identifies the state of the output that does not activate the beeper.</p> <p>open configures what inactive means when the door strike is open.</p> <p>closed configures what inactive means when the door strike is closed.</p>
Beeper on Door Held Open Alarm	drop-down list	<p>Activates and configures the beep sound associated with a door-held-open alarm.</p> <p>Inactive disables the beep sound.</p> <p>Warning only provides a beep that precedes the actual alarm condition by the number of seconds specified by Warning Time. 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.</p> <p>Continuous provides a warning-time beep, however, at the end of the Warning Time, the beep continues to sound until either the door closes or the Maximum Continuation Time is reached. You specify this time in minutes and seconds using the Max Continuation text box.</p>
Intrusion Beep (visible only when the reader is assigned to an intrusion zone)	true or false	<p>Provides an intrusion zone beep.</p> <p>This property replaces Beeper on Door Held Open Alarm when a reader is assigned to an intrusion zone. Also, some properties are not available for editing and appear dimmed (read-only).</p> <p>true enables the intrusion beep.</p> <p>false disables the intrusion beep.</p>

Alarm Relay tab

Each input may have one or more alarm relay devices assigned to it. This allows you to choose an alarm extension assignment on an input, as you would do with a Relay Out.

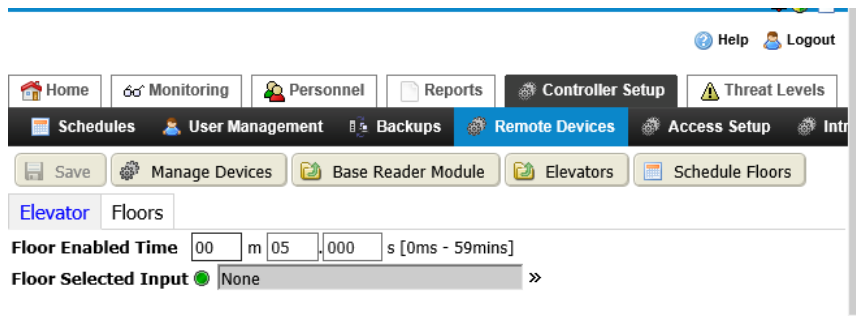
Properties

Property	Value	Description
Status	read-only	<p>Reports the condition of the entity or process at last polling.</p> <p>{ok} indicates that the entity is licensed and polling successfully.</p> <p>{down} indicates that the last poll was unsuccessful, perhaps because of an incorrect property.</p> <p>{disabled} indicates that the Enable property is set to false.</p> <p>{fault} indicates another problem.</p> <p>Depending on conditions, multiple status flags may be set including {fault} and {disabled}, combined with {down}, {alarm}, {stale}, and {unackedAlarm}.</p>
Relay Out	Ref Chooser	Defines which output this relay is connected to. The system automatically populates the Ref Chooser with the available outputs.
Assignment	Ref Chooser	Defines which input this relay is connected to. The system automatically populates the Ref Chooser with the available inputs.
Relay Type	drop-down list	<p>Defines how the relay out behaves relative to the assigned input. You can toggle relay settings on and off or the relay may be out of phase (inverse) with the assigned input.</p> <p>Follow matches the state of the assigned input.</p> <p>Inverse selects the relay out status that is the opposite of the assigned input state.</p> <p>Toggle on active changes the relay from its current state when the assigned input state changes to active.</p> <p>Toggle on inactive changes the relay from its current state when the assigned input state changes to inactive.</p>
Inverse		Sets the relay out state to the opposite of the assigned input state.
Toggle On Active		Changes the relay out status from its current state when the assigned input state changes to inactive.

Elevators Setup view, Elevator tab

For an elevator, you configure one relay output for each floor. This relay is typically in the elevator control room (use an RIO module) and is wired in series with the floor buttons in the elevator car. When the elevator reader is assigned to an access right, you select the floors associated with that access right. The person with that access right presents a badge. The relays for the floor(s) they can access come on for a few seconds so they can make their selection. You may assign a schedule to individual floors such that during daytime hours, the floor can be enabled automatically.

Figure 173 Elevator tab



The **Elevator Setup** view opens when you click on a listed elevator link on the **Elevators** tab under the **Module Setup** view. The elevator name appears in the view title, above the control buttons.

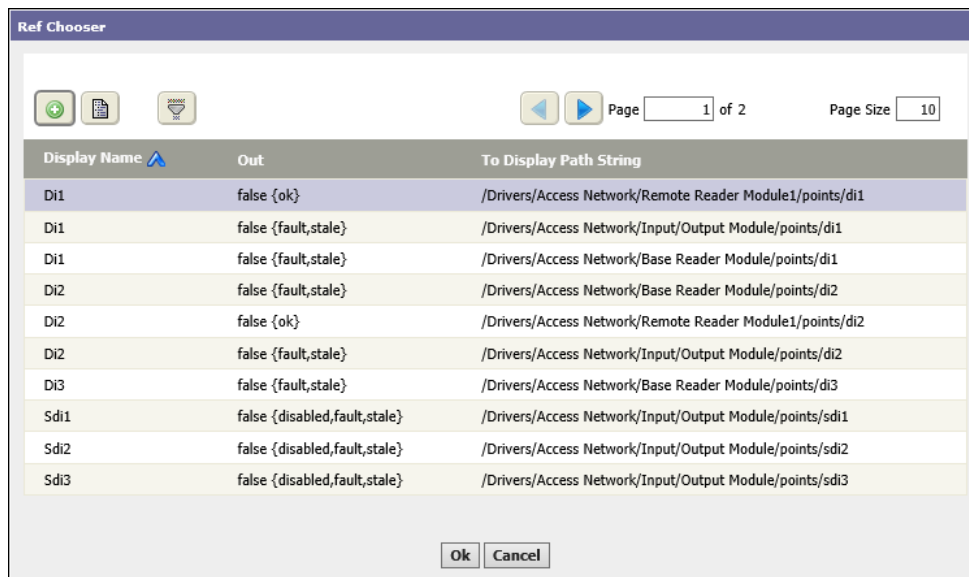
Properties

Property	Value	Description
Floor Enabled Time	minutes, milliseconds	Sets the amount of time that the elevator floor button is active after access is granted to the floor.
Floor Selected Input	additional properties	If the elevator system provides a floor-selected feedback, these properties activate and specify a module and an input for receiving that data. Refer to Buttons, page 188 (the next section).

Elevator Ref Chooser

This window lists the available input points. Using it you select a point to associate with the elevator and click **Ok**.

Figure 174 Elevator Ref Chooser



Buttons

In addition to the standard Export, Filter and page navigation buttons, the Assign button (Assign icon) associates the input point with the elevator.

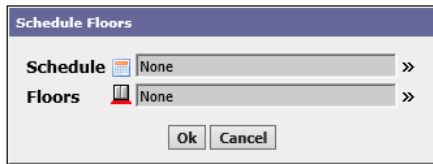
Columns

Column	Description
Display Name	Reports the name of the input point.
Out	Indicates true if the associated output point is enabled, and indicates in parentheses the current state of the input point.
To Display Path String	Reports the path to the location of the point in the station.

Schedule Floors window

This window

Figure 175 Schedule Floors window



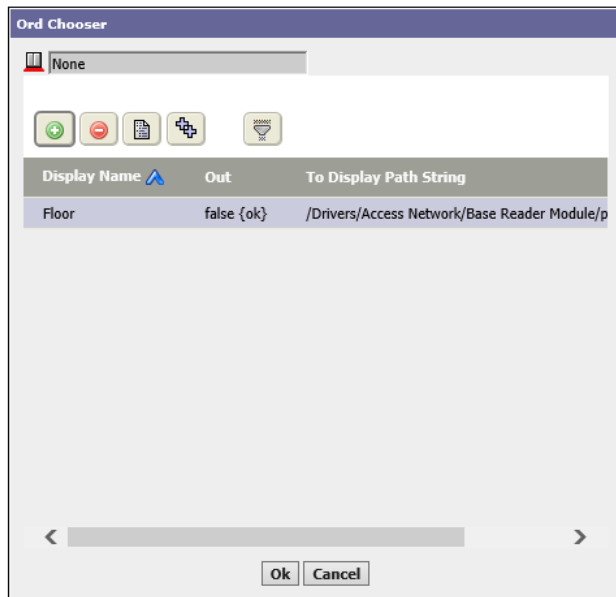
You access this view from the main menu by clicking **Controller Setup→Remote Devices→Remote Modules→Remote Module Setup**, creating a new device or double-clicking the base reader module in the table, clicking the **Elevators** tab, clicking the Elevator link, and clicking the **Schedule Floors** link.

Property	Value	Description
Schedule	Ref Chooser	Opens the Schedule Ref Chooser.
Floors	Ord Chooser	Opens the Floors Ord Chooser. Refer to the next topic.

Floor Ord Chooser

This window configures the floor associated with the current elevator.




Figure 176 Floor Ord Chooser



You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**, creating a new device or double-clicking the base reader module in the table, clicking the **Elevators** tab, clicking the Elevator link, clicking the **Schedule Floors** link, and clicking the chevron to the right of the **Floors** property.

Buttons

In addition to the standard buttons, Summary and Filter, this window provides these specific buttons:

-  Assign associates the floor ORD with the current elevator.
-  Unassign disassociates the ORD with the current elevator.
-  Assign All associates all selected floors with the currently elevator.

Floors tab

This tab lists all the floors that are assigned to the elevator, with each floor having scheduling-related properties. Use the **Manage Devices** button and the associated window to add floors to the Elevator device in this view. The fields next to each floor allow you to assign a schedule to the floor and link a floor to a relay output using the Ref Chooser window. Click the >> icon to open the Ref Chooser window to add a relay. You can also remove a floor device by clicking the Delete icon (⊖).

Figure 177 Floors tab



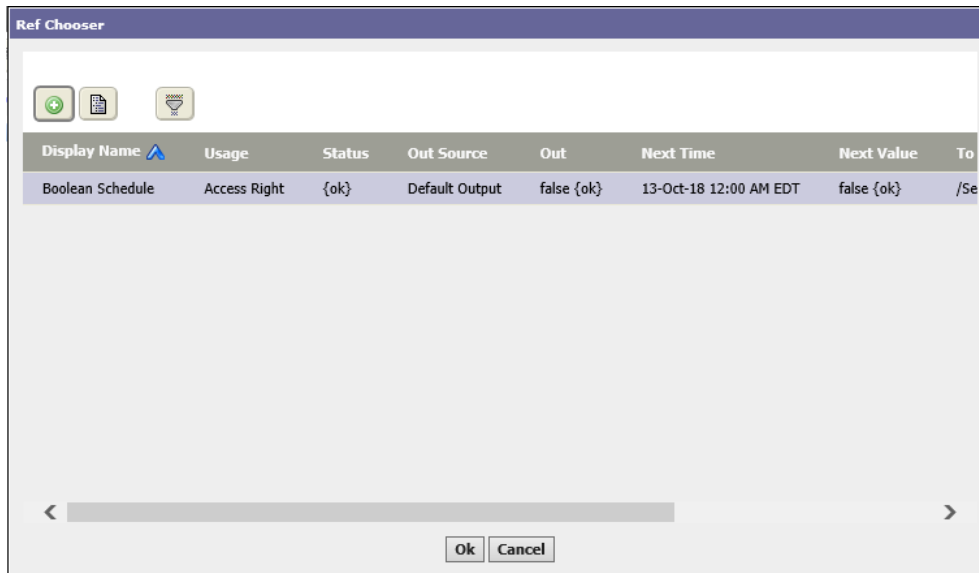
NOTE: Floors are elevator devices.

Property	Value	Description
Floor	read-only, false or true	Reports if a floor associated with this elevator is enabled, and the current status of the controlling point.
Schedule	Ref Chooser	Opens a list of schedules for managing floor access. Refer to Buttons, page 190 .
Log Schedule Activity	checkbox (default is not selected)	Sets up the creation of a record any time a schedule controls activity at this elevator. When selected, any schedule control occurring at this elevator is recorded and may be displayed in the Access History report. When cleared, schedule activity is not recorded.
Schedule	Ref Chooser	Opens a list of log schedules. Refer to Columns, page 192 .
Floor Selected Input	text	If the elevator system provides floor-selected feedback, this property activates and specifies a module and an input for receiving that data.


Schedule floors Ref Chooser

This Ref chooser opens on the Floors tab when you click the chevron to the right of the **Floor** property, and when you click the **Schedule Floors** link.

Figure 178 Schedule Ref Chooser



Buttons

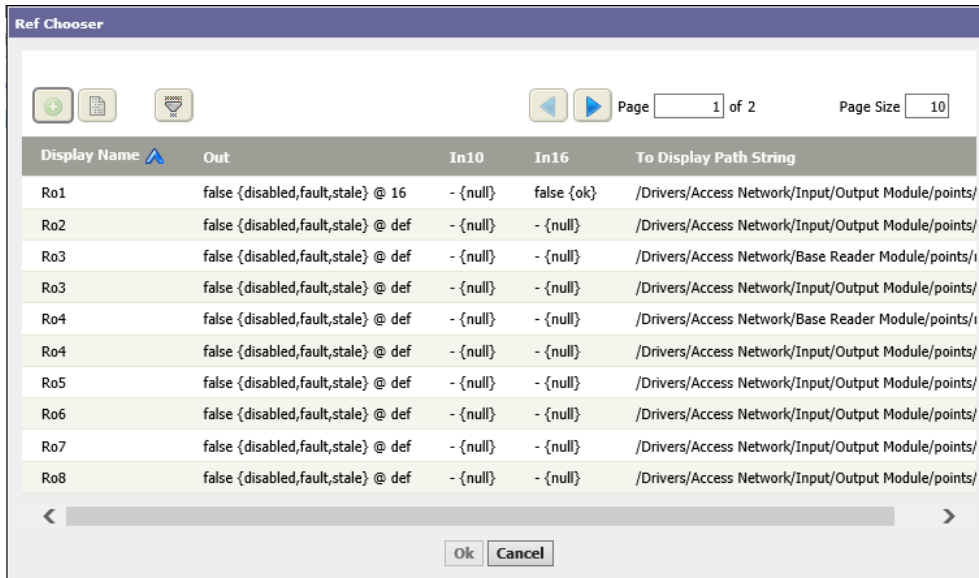
In addition to the standard Export, Filter and page navigation buttons, the Assign button () associates the schedule with the elevator.

Columns


Column	Description
Display Name	Reports the name of the schedule.
Usage	Reports the purpose of the schedule.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}
Out Source	Identifies the source of the output.
Out	Reports if the output source is ok or in fault.
Next Time	Indicates when the next event is scheduled.
Next Value	Reports a true or false value.
To Display Path String	Identifies where in the station the schedule is located.

Schedule log Ref Chooser

Figure 179 Schedule log Ref Chooser



Buttons

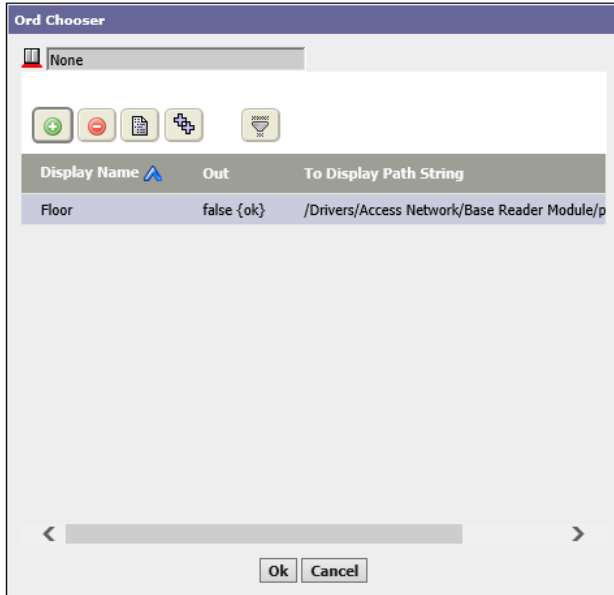
In addition to the standard Export, Filter and page navigation buttons, the Assign button () associates the log schedule with the elevator.

Columns

Column	Description
Display Name	Reports the name of the schedule.
Out	Reports if the output source is ok or in fault.
In10	Reports if the first input point is ok or in fault.
In16	Reports if the last input point is ok or in fault.
To Display Path String	Identifies where in the station the schedule is located.

Floor Ord Chooser

Figure 180 Floor Ord Chooser



This chooser defines the path to the floor in the database.

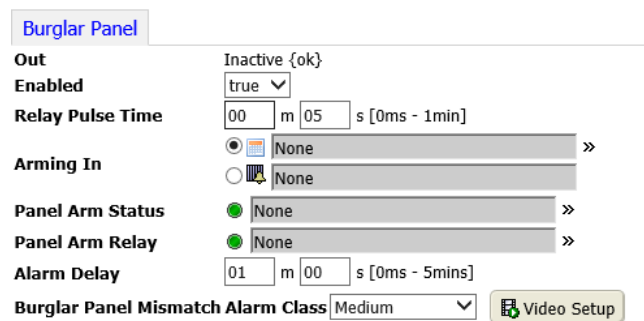
Readers tab


This tab lists all the readers that are assigned to the elevator. Use the **Manage Devices** button and the associated window to add readers to the Elevator.

Burglar Panel view

Arms and disarms a third-party burglar alarm panel.

Figure 181 Burglar Panel view



To access this view, click on a burglar panel link  that is listed in the **Burglar Panels** tab under the **Module Setup** view. The burglar panel display name appears at the top of the view. The following control buttons display above the **Burglar Panel** tab.

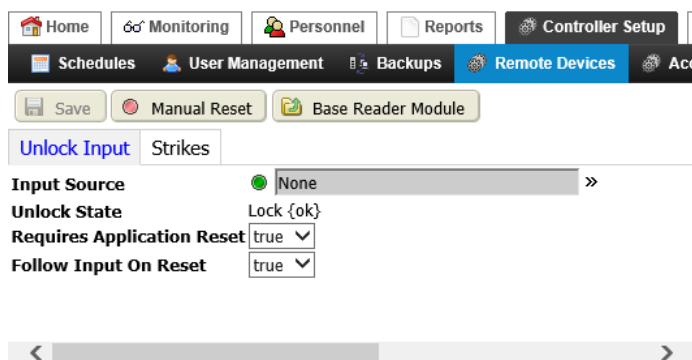
- **Save** is available when there are unsaved changes in the view. Click the button to save changes.
- **Base Reader Module** button links to the **Module Setup** view.

Property	Value	Description
Out	read-only	Reports the current Panel Arm Relay Out state and status. The Arming In property controls the state, which is triggered only when the Arming In property value changes and the new value does not match the Panel Arm Status value.
Enabled	true and false	Turns the feature on (true) and off (false).
Relay Pulse Time	up to 1 minute maximum	Sets the time for the assigned relay output pulse to attempt to change the burglar alarm panel status.
Arming In	Ref Chooser (defaults to none)	Defines how to arm the panel. 🗓️ Schedule arming arms the burglar panel by assigning a schedule using this property. 🚪 Intrusion Zone arming arms the burglar panel by assigning an access zone to the property.
Panel Arm Status	Ref Chooser	Assigns the status input for the burglar panel. The value of this input indicates the actual status of the burglar alarm. the system compares it to the Arming In property value to detect a match or mismatch condition.
Panel Arm Relay	Ref Chooser	Assigns the arming relay for the burglar panel. This relay momentarily energizes (for the Relay Pulse Time) the panel in an attempt to change the burglar alarm status to match the Arming In value.
Alarm Delay	minutes and seconds (defaults to one minute)	Defines a minimum amount of time to wait if a mismatch exists between the Arming In and Panel Arm Status . For example, when a Arming In value changes and a mismatch is detected, an alarm is generated only after the Alarm Delay time is exceeded.
Burglar panel Mismatch Alarm Class	drop-down list	Defines the alarm class to use for alarms generated as the result of a mismatch between Arming In and Panel Arm Status .

Edit Unlock Input view

Unlock Input is a device option that uses an input (DI or SDI) to override a locked state on a door strike. When active, the door remains unlocked and the system inhibits door forced alarms until the input returns to an inactive state.

Figure 182 Unlock Input view



You access this view by clicking **Controller Setup→Remote Devices→Remote Drivers**, double-clicking the **Access Network** row in the table, double-clicking a base or remote reader row, clicking the **Manage Devices** link, followed by clicking **Add**, selecting **Unlock Input**, clicking **Ok** twice, clicking the **Unlock Inputs** tab, and clicking an **Unlock Input** hyperlink.

When you add this option to your base or remote reader module, using the **Manage Devices** window, the **Unlock Inputs** tab appears in the **Modules** view. You can have one or more **Unlock Inputs** listed on the **Unlock Inputs** tab.

Property	Value	Description
Input Source	additional properties	Opens a Ref Chooser for identifying the input source. When this source is active, the lock state of the assigned strike is overridden.
Unlock State	read-only	Displays the current state of the assigned strike (Locked or Unlocked).
Requires Application Reset	true (default) or false	Determines how the unlock state responds to a change of state in the assigned input source. true prevents an unlock input override change until you click the Manual Reset button. false clears the unlock input override when the input source value changes to false or inactive. The Manual Reset and Follow Input on Reset buttons do not apply and do not appear in the view.
Follow Input On Reset	true (default) or false	If Requires Application Reset is true, this property is visible and causes the unlock input state to follow the unlock input as it transitions from one state to the other, for example: true to false, and back to true. When an application reset is not required, this property is not applicable.

Edit Power Monitor view

This view sets up an alarm notification to alert you when your controller has both a main power failure and low UPS battery power.

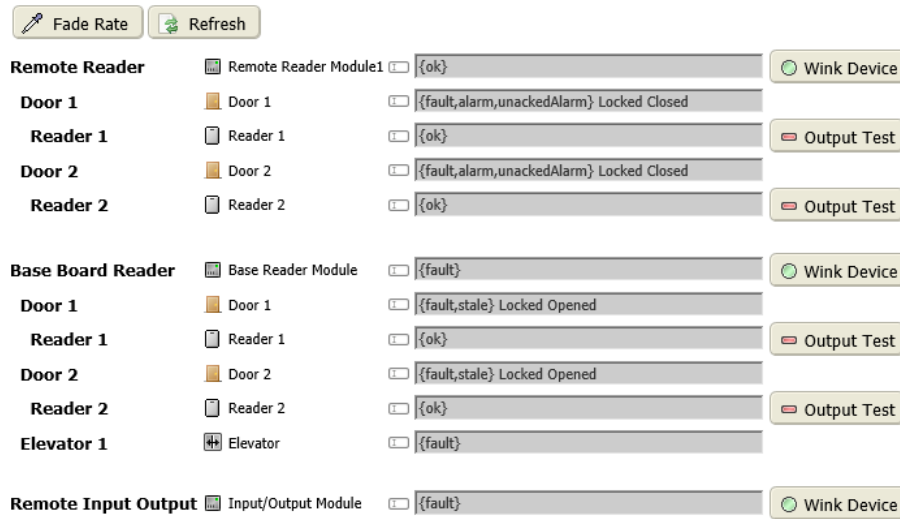
NOTE: To use this feature the configuration must meet these requirements: It must have a Boolean status output from a source that indicates primary power status, and a source that indicates UPS low-battery status. You may wire these outputs to a remote reader module's Di1 and Di2 inputs respectively. The system must discover and add the remote reader module to the station database using the **Access Device Manager - Database** (Remote Module Setup) view.

For this type of alarm to occur, these conditions must exist concurrently, although they do not need to be initiated simultaneously. For example, you may have a low power status on your UPS battery, but the system does not generate the power monitor alarm unless a primary power failure occurs at the same time. Similarly, the system does not generate an alarm if primary power fails as long as the UPS battery power is at a normal power state.

Remote Module Network Identification view

This view lists all the modules, doors, card readers (base board readers and remote readers) contained in the Network ID database, shows the current status of each, provides links to the views used to configure each device, and provides buttons with which to confirm the connection to each device.

Figure 183 Network Identification view



You access this view by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Identification**.

Buttons

At the top of the view, below the title, and to the right of the properties are these buttons:

The screen capture provides an example of one Base Board Reader module (with one reader (Reader 1), and two remote readers, one with a single reader and the other with two readers (Reader 1 and Reader 2). A Remote I/O module is listed at the bottom of the view.

- **Fade Rate** opens the Fade Rate window with which to define how quickly the color of each property in the status column changes when a device status changes.
- **Refresh** manually updates the data displayed in the table.
- **Wink Device** sends a message to the device.
- **Output Test**

Columns

Clicking any of the device icons opens the view for that specific device.

Table 56 Network Identification columns

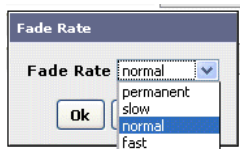
Column	Description
Device Type	The first column identifies the type of device (reader module, door or reader). A base reader module is connected to the local controller. A remote reader module is connected to a peer controller.
Icon: Base Reader Module (📡) Door (🚪) Reader (📱)	Next to the device type is an hyperlinked icon. Clicking this icon opens the device view for the selected device.
Device Description	The second column is an editable description you can customize for each device.
Rename icon (📱)	Provides a way to customize the device description.
Status column	This column displays information about the module, door and reader, including enabled/disabled status, strike position, alarm information, and more.

Column	Description
Wink Device button	This button opens the Wink Device window, which allows you to configure the length of the wink. The Wink Device button's color changes to red while winking is in progress, then back to blue when the wink completes.
Output Test button	This button activates a reader output (for example, a reader light or beep sound) and opens the Output Test window, which allows you to configure the type of output and the length of time for the test.

Fade Rate window

This window defines how quickly the color of each field in the status column changes when a device status changes.

Figure 184 Fade Rate window



You access this view by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Identification**, followed by clicking the **Fade Rate** button.

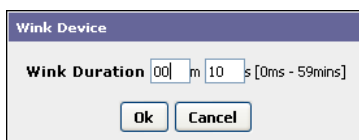
Table 57 Fade rate options

Option	Description
Permanent	Indicates that once the status changes, the color changes and never fades. You may use this to keep track of which points you have tested.
Slow	The color changes slowly.
Normal	The color changes at some medium speed.
Fast	The color changes quickly.

Wink Device window

This view configures how long a device wink lasts.

Figure 185 Wink Device window



You access this view by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Identification**, followed by clicking the **Wink Device** button.

The length of a wink is defined in minutes and seconds.

Output Test window

This window configures the output test.

Figure 186 Output Test window

You access this view by clicking **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Identification**, followed by clicking the **Output Test** button to the right of a device row.

Property	Value	Description
Output	drop-down list	Selects one of two colors to use or a beep.
Duration	minutes and seconds	Defines the meaning of each general duration term.

Access Network view and tab

This view displays values that apply to all devices assigned to the access network.

Figure 187 Access Network view

This view opens when you click **Controller Setup**→**Remote Devices**→**Remote Modules** the **Access Network Setup** menu item under the.

Clicking the **Save** button applies any changes.

Properties

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, and **Health**), these properties support access networks.

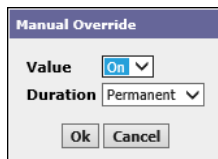
Property	Value	Description
Validation Timeout	minutes and seconds	Defines the maximum time allowed to receive a badge validation. If validation fails to occur within this time, the system may generate a validation-timeout-expired alarm. NOTE: A validation timeout alarm may be caused if a validation cache fault occurs, or if the cache is still initializing.
Show Results Time	minutes and seconds	Defines the time that the (normally <code>false</code>) valid or invalid status remains <code>true</code> after a card is swiped.

Property	Value	Description
Keypad Entry Time	minutes and seconds	Specifies a maximum amount of time after a badge swipe that is allowed before keypad entry must be completed.
Cut Value	voltage (V)	Defines a value for the <code>cut voltage</code> parameter on the network.
Open Value	voltage (V)	Defines a value for the <code>open voltage</code> parameter on the network.
Closed Value	voltage (V)	Defines a value for the <code>closed voltage</code> parameter on the network.
Alarm Source Info	Ref Chooser	Expands to display alarm class properties, which are documented in the “System Setup-Alarm Setup” chapter.

Manual Override window

This window configures manual override properties for alarms.

Figure 188 Manual Override window



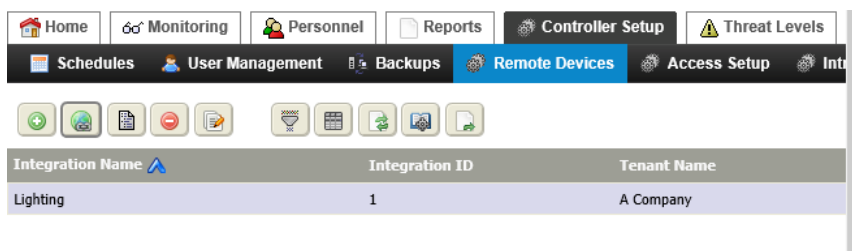
Property	Value	Description
Value	On (default) and Off	Enables and disables the ability to manually override an alarm.
Duration	drop-down list	Configures how long the <code>Value</code> property is in force.

Niagara Integration IDs view

This ID specifies a physically-defined space that indicates where a tenant cardholder resides in a facility. The ID may be passed to the building automation system by BACnet, for example, so that when the system grants access to the facility, it automatically adjusts the appropriate lighting, HVAC, and other controls for the specific person.

This view displays a tabular list of all existing Niagara Integration IDs.




Figure 189 Niagara Integration ID view



To access this view from the main menu of a remote station, click **Controller Setup**→**Remote Devices**→**Niagara Integration IDs**.

Buttons

In addition to the standard buttons (Summary, Delete, Filter, Column Chooser, Refresh, Manage Reports and Export), these buttons provide specific integration ID features:

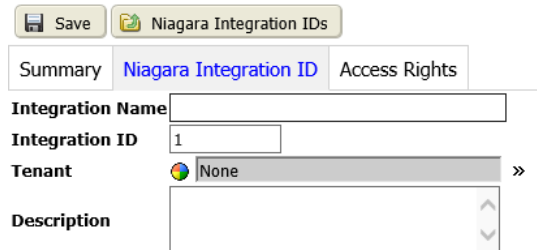
-  Add opens the **Add New Niagara Integration ID** view.
-  Hyperlink links to the edit view or window for the selected item. It is the same as double-clicking the table row. This button is available when a single record is selected.
-  Quick Edit opens the **Quick Edit** window for the selected item(s). This feature allows you to edit one or more records without having to leave the current view.


Property	Value	Description
Integration Name	text	Provides a descriptive title for the integration ID.
Integration ID	integer	Serves as the integration ID number.
Tenant Name	Ref Chooser	Assigns the tenant to the ID, who is considered to be the owner of the access right and is the only tenant that can edit the access right. NOTE: Only one tenant is assigned to a Niagara integration ID.

Add New (or edit) Niagara Integration ID view and tab

This tab adds a new integration ID.

Figure 190 Niagara Integration ID tab



This view opens from the main remote station menu when you click the **Controller Configuration→Remote Devices→Niagara Integration IDs**, followed by clicking the Add button () in the **Niagara Integration ID** view.

Links

A **Save** button and a link to the **Niagara Integration IDs** view are located just below the view title.

Properties

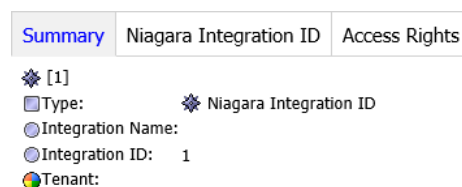
Property	Value	Description
Integration Name	text	Provides a descriptive title for the integration ID.
Niagara Integration ID	integer	Serves as the integration ID number.

Property	Value	Description
Tenant	Ref Chooser	Assigns the tenant to the ID. This tenant is considered to be the owner of the access right and is the only tenant that can edit the access right. NOTE: Only one tenant is assigned to a Niagara Integration ID.
Description	text	Provides general descriptive information about the ID.

Niagara Integration, Summary tab

This tab is displayed by default in this view. It displays a read-only list of all properties, including a link to the **Edit Access Rights** view for any associated access rights listed at the bottom of the tab.

Figure 191 Example of a Summary tab



This tab is present but does not display updated information until you create at least one Niagara Integration ID. For the selected Niagara Integration ID, this tab displays in the appropriate **Edit: Niagara Integration ID** view. The **Summary** tab may also include a list of associated access rights.

Access Rights tab

This tab configures the access rights associated with the Niagara Integration ID.

Figure 192 Access rights tab

Newly Assigned

Access Right Name	Schedule Name	Integration Name	Tenant Name	Threat Level Group Name
Daytime working hours	Boolean Schedule		B Company	Threat Level Group1

Unassigned

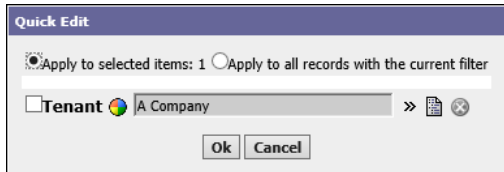
Access Right Name	Schedule Name	Integration Name	Tenant Name	Threat Level Group Name
Daytime working hours	Boolean Schedule		B Company	Threat Level Group1
Off hours	Boolean Schedule		B Company	Threat Level Group11


These panes provide standard Assign Mode functionality.

Quick Edit window

This window edits the Niagara Integration ID properties.

Figure 193 Niagara Integration ID Quick Edit window



To access this window from the main menu by clicking **Controller Setup**→**Remote Devices**→**Niagara Integration Ids**, followed by selecting an ID and clicking the Quick Edit button ().

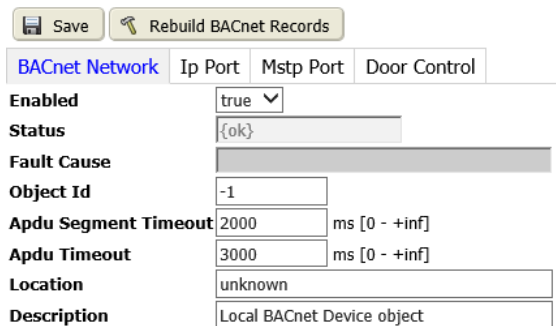
Properties

Property	Value	Description
Apply to selected items: n	radio button	Applies the updated tenant information to only the selected item(s).
Apply to all records with the current filter	radio button	Applies the updated tenant information to all visible records.
Tenant	ref chooser	Opens a ref chooser for selecting the tenant.

BACnet Network view, BacNet Network tab

This view configures BACnet network settings in the system.

Figure 194 BACnet Network view



To access this view, click **Controller Setup**→**Remote Devices**→**BACnetNetwork**.

The **Save** button saves configuration changes. The **Rebuild BACnet Records** button recreates all integrated BACnet records. This button is useful if you have a problem with BACnet point automation.

Properties

In addition to the standard properties (**Enabled**, **Status**, and **Fault Cause**), these properties support a BACnet network.

Property	Value	Description
Object Id	number with valid range from 0 to 4194302; defaults to -1 resulting in no device	Specifies a numerical device ID on the BACnet network (must be unique among all BACnet devices).
Apdu Segment Timeout	milliseconds; defaults to recommended value of 2000 ms	Defines the time to wait before retransmission of an APDU (application protocol data unit) segment.
Apdu Timeout	milliseconds; defaults to recommended 3000 ms	Defines the time to wait before retransmission of an APDU requiring acknowledgment, for which no acknowledgment has been received.
Location (optional)	text string, defaults to unknown	Describes the location of the BACnet device
Description (optional)	text	Describes the BACnet device object

IP Port tab

This tab configures the BACnet/IP link layer used by the controller, providing that the **Enabled** property (in **BACnet Network** tab) is set to `true`.

Figure 195 IP Port tab

The screenshot shows the 'IP Port' configuration tab within a software interface. At the top, there are four tabs: 'BACnet Network', 'Ip Port' (which is selected), 'Mstp Port', and 'Door Control'. Below the tabs, several properties are listed with their current values:

- Enabled:** false (dropdown menu)
- Status:** {disabled} (text field)
- Fault Cause:** (greyed out text field)
- Network Number:** 1 (text field)
- Adapter:** dm0 (dropdown menu)
- Udp Port:** 0xBAC0 (text field)
- Ip Device Type:** Standard (dropdown menu)
- Bbmd Address:** null (text field)

To access this view, click **Controller Setup**→**Remote Devices**→**BACnetNetwork**, followed by clicking the **IP Port** tab.

Properties

In addition to the standard properties (**Enabled**, **Status**, and **Fault Cause**) these properties support the BACnet IP Port.

Property	Value	Description
Network Number	number from 1 to 65534; default value is -1 (inoperative)	Specifies a unique network number across the entire BACnet internetwork for the BACnet/IP network.
Adapter	drop-down list (defaults to NET1)	Specifies which of the two physical Ethernet ports on the controller is used for BACnet/IP communications. NET1 or NET2

Property	Value	Description
UDP Port	port number (defaults to 0xBAC0, decimal 47808)	Specifies the UDP (user datagram protocol) port used by BACnet/IP. You can specify another port, if needed (say an existing BACnet/IP network is using another UDP software port).
IP Device Type	drop-down list: (defaults to BACnet device)	Defines the type of BACnet/IP device. Generally, the default Standard should be used. BACnet device BBMD (BACnet Broadcast Management Device) BACnet Foreign Device
Bbmd Address	number (defaults to null)	Sets the Bbmd (BACnet Broadcast Management Device) address. This address is only required when the system is being used as a BACnet Broadcast Management Device.

Mstp Port tab

These fields configure the BACnet/Mstp link layer used by the controller, providing that the `Enabled` property (in BACnet Network tab) is set to `true`.

Figure 196 Mstp Port tab

To access this view, click **Controller Setup**→**Remote Devices**→**BACnetNetwork**, followed by clicking the **Mstp Port** tab.

Properties

In addition to the standard properties (`Enabled`, `Status`, and `Fault Cause`) these properties support the BACnet Mstp Port.

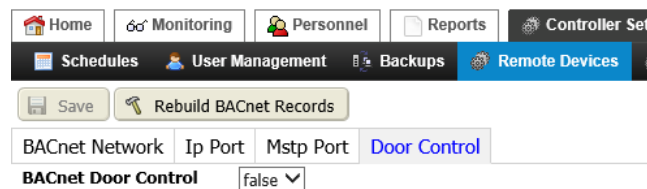
Property	Value	Description
Network Number	number from -1 to the BACnet network number for the network segment to which you are connecting	Sets the number of the network. If this is an existing BACnet installation, make sure to use the same network number already in use. If this is a new BACnet installation, choose this number (for example: 3)
Port Name	text	Typically, you leave the Mstp Address at 0 (the default), and verify that no other MS/TP device on the trunk is addressed the same. If there is ever a lost token, the device with the lowest MAC address regenerates the token (and, in this case, the station).

Property	Value	Description
Baud Rate	drop-down list	Selects the baud rate.
Mstp Address	number, in decimal, with a valid range from 0 (default) to 127	Sets the Mstp address to a unique BACnet MAC address on that MSTP trunk. Each BACnet device on the MS/TP network segment must have a unique MAC address.
Max Master	number, in decimal, with a valid range from 0 (default) to 127	Sets the maximum master device to the lowest known master device on the network, with possible room for expansion if needed.
Max Info Frames	number up to 100, defaults to 20	Specifies how many messages are sent before passing the token. Increasing this value to 100 improves performance in some cases.

Door Control tab

This tab configures door control.

Figure 197 Door Control tab



Properties

Property	Value	Description
BACnet Door Control	true or false (default)	Enables and disables control of a door that is a BACnet network device.

BACnet BDT Manager (Broadcast Distribution Table) view

This view is populated when the system is operating as a BACnet Broadcast Management Device (BBMD). This table lists all other participating BBMDs, including their IP address and broadcast distribution mask for each.



Figure 198 BACnet BDT Manager (Broadcast Distribution Table) view

Name	BACnet IP Address	Broadcast Distribution Mask
BdtEntry	test	test
localDevice	null	255.255.255.255

You access this view by selecting **Remote Devices**→**BACnet BDT Manager** from the main menu.

Buttons

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

-  Add opens a view for adding BBMD records to the database.
-  Edit opens a view for updating the selected existing BBMD record(s).

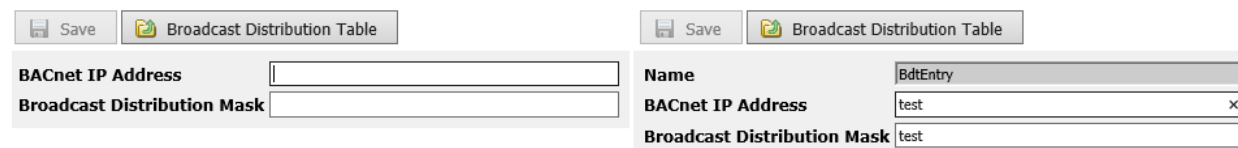
Columns

Column	Description
Name	Reports the name of the BBMD.
BACnet IP Address	Reports the IP Address of the BBMD.
Broadcast Distribution Mask	Reports either a subnet mask or all 1's. This mask indicates if a BBMD is to send a directed broadcast (retransmitted by appropriately configured IP routers) or a unicast message to the indicated BBMD, which then retransmits the forwarded broadcast message.

New (or edit) Entry views

These views configure a new BACnet (BBMD) entry in the database. The New and Edit views are identical except for the read-only Name in the Edit Entry view.

Figure 199 New Entry view and Edit Entry view



To access these views from the main menu, click **Controller Setup**→**Remote Devices**→**BACnet BDT Manager**, and click the Add button () or the Edit button ()

These views are identical except for the read-only **Name** property that displays in the **Edit Entry** view.

Under the title, both views provide a **Save** button and a link back to the **Broadcast Distribution Table** view.

Property	Value	Description
Name (Edit Entry view only)	read-only	Displays the name of the BDT entry that appears only in the Edit Entry view.
BACnet IP Address	6-octet B/IP address	Defines the address of a BBMD.
Broadcast Distribution Mask	4-octet field	Indicates how broadcast messages are to be distributed on the IP subnet served by the BBMD.

Station Manager - Database view

This view uses a typical two-pane set of tables to list stations that are already assigned to the database or that have been discovered on the network. While some features are available from both a remote station and a Supervisor station, the synchronize and join features are designed to be used in a Supervisor station.

Figure 200 Station Manager view (Supervisor station)

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

Discovered

Station Name	Host Name	Scheme	Fox Port	Already Exists
AGN_AMSTNLBW_3	172.31.66.214	fox	1911	false

This view opens from the main menu of a remote controller station when you select **Controller(System) Setup→Remote Devices→Station Manager**.

Database pane

The control buttons are located across the top of the pane. The unique station creation and management control buttons include:


- 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.
- New opens the **New Station** window in either a remote or Supervisor station. This view adds a station without using the discovery process.
- Edit opens the **Station** view in either a remote or Supervisor station. It has two tabs: **Niagara Station** and **Device exts.**
- Sync Time opens the **Remote Sync Time** window in a Supervisor station.
- Replicate opens a confirmation window in a Supervisor station.
- Set Auto Replicate enables (*true*) and disables (*false*) automatic replication from a Supervisor station.
- Join opens the **Join (Add) Station** view in a Supervisor station.
- Recovery opens the **Recover Station** view in a Supervisor station.
- Settings opens the **Settings** window in either a remote or a Supervisor station. This view configures the Fox Port and TimeSync properties. For example, a stand-alone controller that has never been joined to a supervisor only has the Fox Port field available, since no time sync is necessary.
- Learn Mode buttons open and close the **Discovered** pane in a remote or Supervisor station. These buttons show or hide the control buttons and any discovered items (devices, points, database properties, etc.).

Table 58 Database columns

Column	Description
Station Name	Identifies the station, by name. Station names should be unique in a Station Manager Database.
Host Name	Identifies the host by IP address.
Scheme	Reports if you are using fox or foxs for communication. Foxs uses TLS encryption and server authentication and is more secure than fox communication.
Fox Port	Identifies the host port number that the station is communicating on.

Column	Description
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}
Actual Role	Describes the relationship between the local station and the listed station: Supervisor, Peer, or Subordinate. This value is specified in the Add Stations window using the Desired Role property.
Joined	Indicates if the remote station is joined to the local station (true or false).
Auto Replicate	Indicates if auto replication is enabled (true or false).
Replication Status	Reports the replication result. If replication occurred successfully on the last attempt, this column indicates {ok}.
Last Replication	Displays the time of the last replication.

Discovered pane

To view this pane, click the Discover control button () at the top of the **Database** view.


The Add control button () in the **Discovered** pane adds the selected, discovered station to the **Data-base** pane.

Table 59 Discovered pane columns


Column	Description
Station Name	Identifies the station, by name. Station names should be unique in a Station Manager Database.
Host Name	Identifies the host by IP address.
Scheme	Reports if you are using fox or foxs for communication. Foxs uses TLS encryption and server authentication and is more secure than fox communication.
Fox Port	Identifies the host port number that the station is communicating on.
Already Exists	Indicates if the station already exists (true) or not (false).

Add (or edit) Station windows

This view creates a new station.

Figure 201 Add Stations window

To create, you access this window by clicking the New button () in the **Database** pane of the **Station Manager – Database** view.

To edit, you access these windows by selecting a station in the **Station Manager – Database** view and clicking the Edit button ()

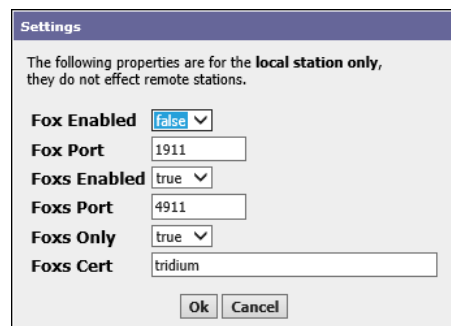
Two consecutive Add station windows contain station properties.


Property	Value	Description
Enabled	true or false	For both a local and remote stations, adds the station with either one or both stations enabled (<code>true</code>) or disabled (<code>false</code>) state. You change the status after adding the station by clicking the Edit control button, and using the Edit window.
Credential Store	drop-down list (defaults to <code>UsernameAndPassword</code>)	Selects how to authenticate the target station. <code>UsernameAndPassword</code> provides properties to authenticate using a user name and password. <code>CertificateAliasCredential</code>
Username	text	For both a local and remote stations, defines the login name for the account.
Password	strong text	For both a local and remote stations, defines the login password for the account.
Use Foxs	true (default) or false	Selects secure communication, which includes data encryption and server authentication.
Fox Port	number	Identifies the host port number that the station is communicating on.
Desired Role	drop-down list	Selects the station's role: <code>Peer</code> , <code>Subordinate</code> , or <code>Supervisor</code> from the perspective of the local station.

Settings windows

This window configures communications from the local system to one or more remote stations. This is equivalent to FoxService in Workbench.

Figure 202 Example of a Settings window



You access this window, select a station in the **Station Manager – Database** view and click the Settings button ()

Property	Value	Description
Fox Enabled	true or false (default)	Turns Fox communication on (true) and off (false). Fox communication does not provide encryption or server authentication.
Fox Port	number (defaults to 1911)	Specifies the port for Fox communication.
Foxs Enabled	true (default) or false	Turns Foxs communication on (true) and off (false). Foxs communication provides data encryption and server authentication using the TLS (Transport Layer Security) protocol.
Foxs Port	number (defaults to 4911)	Specifies the port for Foxs communication.
Foxs Only	true (default) or false	Indicates if the station supports only Foxs (true) or both Foxs and Fox communication (false).
Foxs Cert	text (defaults to tridium)	Identifies the TLS server certificate to use for the station.

Schedules tab

This tab contains properties related to the station device extensions. Use the hyperlinked properties to navigate to other views. This tab is available in the Supervisor station.

Examples of some useful Device Ext links that appear on this tab include:

- **Schedules** links to the **Distributed Schedule Manager** view.
- **Intrusion** links to the **Distributed Intrusion Zone Manager** view.
- **Cameras** links to the **Remote Video Camera Manager** view.

NOTE: You can use this **Video Camera Manager** view from a remote controller to discover cameras without having to add the video network to the remote controller. With the Supervisor selected (under the **Station Manager** view) use this link to open the **Video Camera** view of the Supervisor station for the purpose of discovering and adding cameras to your remote controller.

Join (Add) Station view

This view sets up and initiates the process of joining one or more remote stations with a Supervisor station. It is available in a Supervisor station only. The title of the view reflects the name of the station. This is why it can be called the “join” or “add” station view.

Figure 203 Join Station view

Add Acme_Bldg_1

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

Supervisor Time 22-Jan-16 12:26 PM IST
Subordinate Time 22-Jan-16 12:26 PM IST
Time Difference < 1min

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

[Distributed Schedule Manager](#)

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

Record Type	Import Status
Tenants	2 Matched Objects
Keypad Formats	3 Matched Objects
Wiegand Formats	7 Matched Objects
Personnel	11 Matched Objects, 6 Warnings
Additional Personnel Data	3 Matched Objects
Badges	8 Matched Objects
Niagara Integration IDs	1 Matched Objects
Access Rights	6 Matched Objects
Intrusion Zones	No Objects
Intrusion Pins	No Objects
Readers	3 Matched Objects
Floors	No Objects
Threat Level Groups	4 Matched Objects
Threat Level Range	6 Matched Objects

This view opens from the main menu when you click **Controller Setup→Remote Devices→Station Manager**, followed by selecting a station in the **Station Manager – Database** view and clicking the Join button ().

The top left corner of the view displays the name of the station that is to be added or joined to the Supervisor. Below the title are three control buttons, step instructions, a link to the **Distributed Schedule Manager**, and a table of records.

Links

These links are at the top of the view under the title.

- **Commit** is available only after the object matching step is completed (all items in the Import Status column are configured). Click this button to start the join process.
- **Retrieve Import Status** automatically configures all record types and returns their import status in the Import Status column. Click this button to start the join process.
- **NiagaraNetwork** links to the **Station Manager – Database** view.
- **Reset Import Status** clears any matched objects displayed in the table of records.
- **Synchronize Time** initiates a time synchronization job that brings the time of the remote station to within one minute of the supervisor station time.

Instruction steps

Instruction steps include the following:

- **Step 1: Make sure the System Date Times are synchronized within 1 min of each other.** This instruction and the associated **Synchronize Time** button align the times of the two stations (Supervisor and remote controller) to within one minute of each other. This alignment is required before importing records to the Supervisor station.

- Step 2: Use the Distributed Schedule Manager to import schedules. This instruction reminds you that this step requires a different view.
- Step 3: Make sure the database will be imported properly. This instruction cautions you to prepare for a proper import of records from the remote station to the Supervisor station. You use the **Retrieve Import Status** and **Reset Import Status** buttons at the top of the view to match records. Table of records

Table of records

Table of Record Types

This two-column table lists each type of record that is available for configuring. The Record Type column indicates what the record is and the Import Status column displays a status, including warnings or errors (if any) and shows how many objects are:

- Matched Objects
- New Objects
- No Objects
- Delete Objects
- Error

Object details

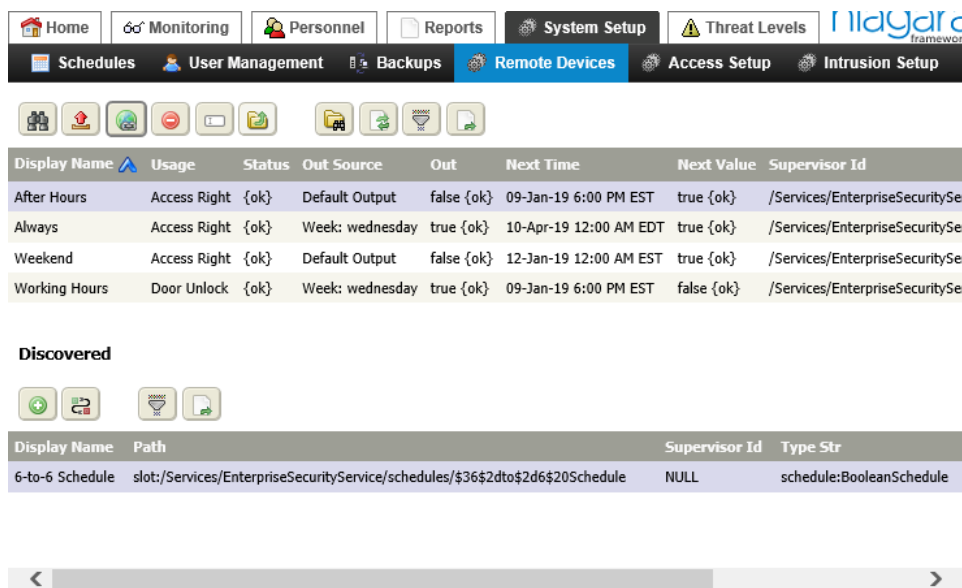
A table or window displays when you click an the Status column of a new, matched, or deleted object. This window or table shows more details about the selected record.

Distributed Schedule Manager - Database view



This view provides a way to discover and import schedules from a remote station to the local station. All stations have a **Distributed Schedule Manager** view. The relationship between the local and remote stations is independent of each station’s role (subordinate, peer, or Supervisor). For the purposes of propagating schedules, the relationship depends on which station initiates the discovery job.

A Supervisor station discovers schedules in a remote station before adding the remote station to the system.

Figure 204 Distributed Schedule Manager - Database view



To access this view do either of the following:

- From the main menu, click **System Setup→Remote Devices→Station Manager**, select a station in the database, and click the Join button (). Then, from the **Join (Add) Station** view, click the Distributed Schedule Manager link.
- From the main menu, select **Controller (System) Setup→Remote Devices→Station Manager**, select a station and click the Summary button (). Then, in the **Station Device Properties** view, choose the **Device Exts** tab and click the Schedules link.Database pane

Database pane

In addition to the standard control buttons, this pane provides two export buttons:



-  Sends (pushes) the selected schedule(s) from the local to the remote station. You might use this function to immediately update changed schedules in a remote station instead of waiting for a replication job.
-  Export opens the Export window for creating a PDF or CSV formatted report of the current table.

Table 60 Distributed Schedule Manager columns

Column	Description
Display Name	Identifies the name of the schedule.
Out Source	Describes the current output as one of four options: Special Event: <Special Event Name> or Week <Day of the Week>
Out	Displays <code>true</code> or <code>false</code> . Output is true during any configured calendar day(s), otherwise it is false.
Next Time	Defines the date and time of the next scheduled output change for the component. If it is more than a year away, this value is null.
Next Value	Displays the next scheduled output value. Value is meaningless when Next Time is null.
Supervisor ID	Reports the URL that identifies the Supervisor station.

Discovered pane

In addition to the standard control buttons (Filter and Export), these buttons support schedules:



-  Add imports the selected schedule in the Discovered pane from the remote station to the local station. You might use this to add a schedule that exists on a subordinate station to a Supervisor.
-  Match synchronizes the schedule selected in the **Database** pane with the schedule selected in the **Discovered** pane creating a single schedule in the local station. Match helps to prevent multiple versions of the same, or similar schedules.

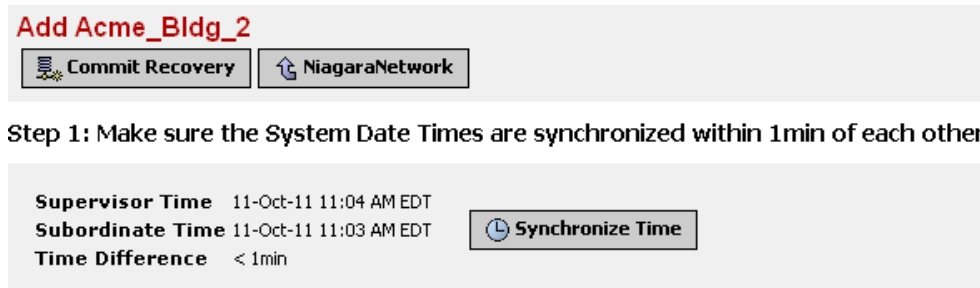
Table 61 Discovered columns

Column	Description
Name	Provides the schedule name.
Path	Reports the URL that identifies the schedule.
Supervisor ID	Reports the URL that identifies the Supervisor station.

Recover Station view

This view sets up and initiates the station recovery process. Recovery uses station data from the Supervisor to restore a remote station when a remote station backup is not possible or would result in lost or data conflicts.

Figure 205 Recover Station view



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

Supervisor Time	11-Oct-11 11:04 AM EDT	
Subordinate Time	11-Oct-11 11:03 AM EDT	
Time Difference	< 1min	

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

[Distributed Schedule Manager](#)

To access this view from the main menu, click **Controller (System) Setup→Remote Devices→Station Manager**, select a station and click the **Recover** button ().

The top left corner of the view displays the name of the station that is to be added or joined. Below the title are three control buttons, step instructions, a link to the **Distributed Schedule Manager**, and a table of records.

Links

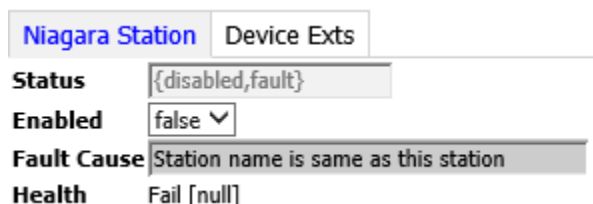
- **Commit Recovery** button starts the recovery process.
- **NiagaraNetwork** button links to the **Station Manager – Database** view.
- **Synchronize Time** button initiates a time synchronization job that sets the time of the remote station to within one minute of the Supervisor station’s time. This ensures that records added to the Supervisor database during the join process share a common time reference.

NOTE: The **Recover Station** view does not import schedule records. You must import any schedules using the **Distributed Schedule – Database** view.

Station Device Properties view

Stations that are part of a system’s network (NiagaraNetwork) are represented under the network as station devices. This view displays properties and device extensions that apply to the selected station. It uses the station name as the title of the view.

Figure 206 Niagara Station tab



To access this view, click **System Setup→Remote Devices→Station Manager** and click the **Summary** button ().

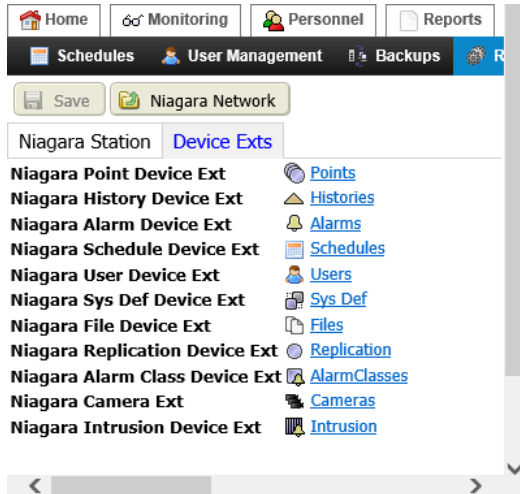
Properties

This view includes the standard system properties.

Device Ext tab

This tab configures the floors, which the elevator is required to service.

Figure 207 Station Device Exts tab

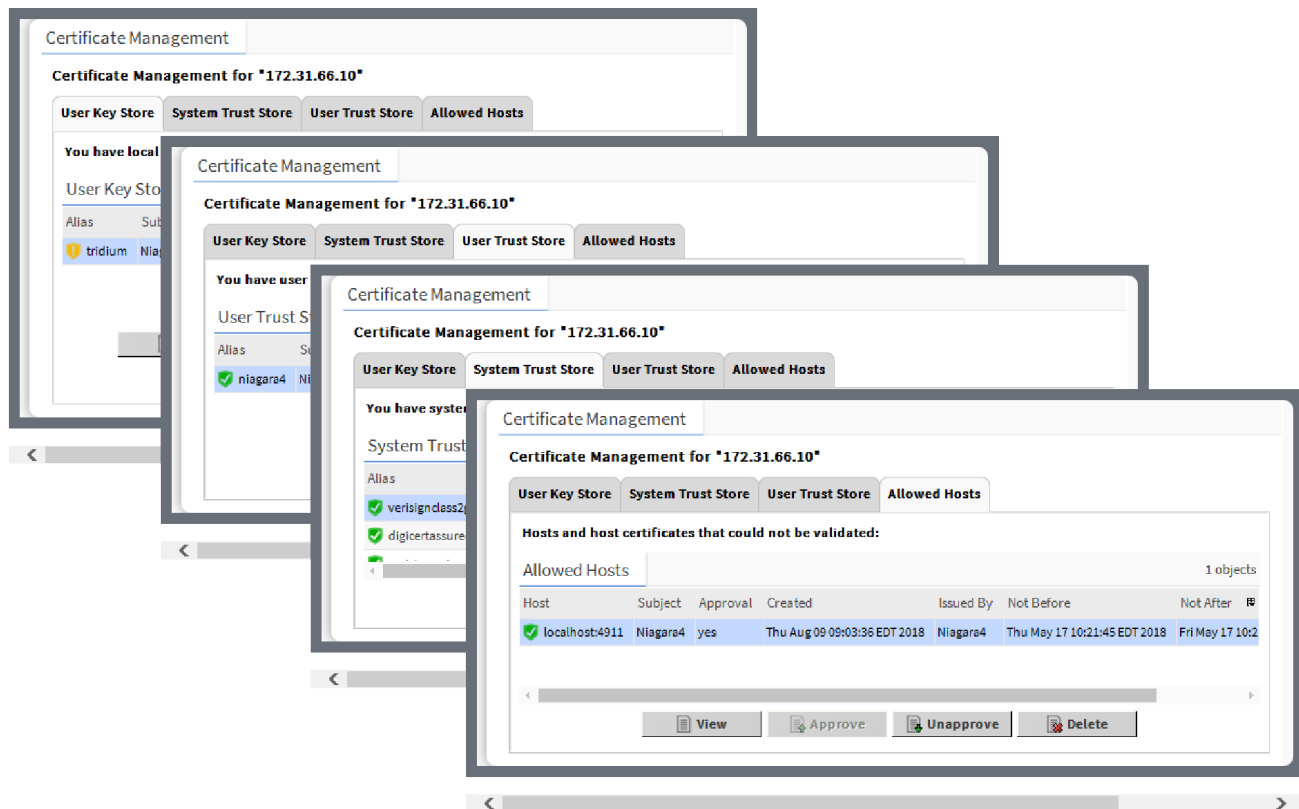


You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Station Manager**, followed by double-clicking a station, and clicking the **Device Exts** tab.

Certificate Management view

This view manages PKI (Public Key Infrastructure) digital certificates, creates Certificate Signing Requests (CSRs), and imports and exports keys and certificates to and from the Supervisor and controller trust stores.

Figure 208 The certificate store tabs



You access this view and tabs by clicking **Controller (System) Setup→Remote Devices→Certificate Management**.

User Key Store

This store lists server, intermediate, and code-signing certificates with their public and private keys. You use this store to create and manage certificates.

Trust Stores (System Trust Store tab and User Trust Store tab)

The trust stores (system and user) contain signed and trusted root CA certificates with their public keys. These stores contain no private keys. A trust store supports the client side of the relationship by using its root CA certificates to verify the signatures of the certificates it receives from each server. If a client cannot validate a server certificate's signature, an error message allows you to approve or reject a security exemption (on the **Allowed Hosts** tab).

The **System Trust Stores** contain installed signed certificates by trusted entities (CA authorities) recognized by the Java Runtime Engine (JRE) of the currently opened platform. A **User Trust Store** contains installed signed certificates by trusted entities that you have imported (your own certificates).

Only certificates with public keys are stored in the trust stores. The majority of certificates in the **System Trust Store** come from the JRE. You add your own certificates to a **User Trust Store** by importing them.

Feel free to pass out such root certificates to your team; share them with your customers; make sure that any client that needs to connect to one of your servers has the server's root certificate in its client trust store.

Allowed Hosts tab

This tab lists self-signed certificates that have been manually approved for use to authenticate a server. As such, they have not been signed by a CA. They should not be approved unless you are certain that the communication they facilitate will be secure.

Columns

Many columns are shared by the tabs. This table lists all columns.

Column	Description
Alias	Identifies certificates by location or function.
Issued By	Identifies the entity that created the certificate.
Subject	Identifies the company that owns the certificate.
Not Before	Displays the date before which the certificate is not valid.
Not After	Displays the expiration date for the certificate.
Key Algorithm	Names the mathematical formula used to calculate the certificate keys.
Key Size	Shows the size of the keys in bits. Four key sizes are allowed: 1024 bits, 2048 bits (this is the default), 3072 bits, and 4096 bits. The bigger the key, the longer it takes to generate.
Signature Algorithm	Names the mathematical formula used to sign the certificate.
Signature Size	Shows the size of the signature.
Valid	Displays the dates between which the certificate is valid.
Self Signed	Indicates that the certificate was signed with its own private key.

Buttons

This list contains in alphabetical order all the buttons available in the stores.

- **Approve manually** validates the selected certificate in the **User Trust Store** and **Allowed Hosts** tabs.
CAUTION: Do not approve a self-signed certificate automatically. Always confirm that you recognize the Alias, Issued By and Subject properties as valid entities.
 You can reverse the approval action on the **Allowed Hosts** tab by selecting the certificate and clicking **Unapprove**.
- **Cert Request** opens a **Certificate Request** window, used to create a Certificate Signing Request (CSR).
- **Delete** removes the certificate from the store.
- **Export** saves a copy of the certificate to the hard disk with the .pem extension.
- **Import** adds a certificate (.pem file) to the **Key Store** or a company's root CA certificate to the User Trust Store.
- **New** opens the **Generate Self Signed Certificate** window, used to create CA and server certificates.
- **Reset** (available only in the Key Store) deletes all certificates in the **Key Store** and creates a new default certificate. It does not matter which certificate is selected when you click **Reset**.
CAUTION: The Reset button facilitates creating a new key pair (private and public keys) for the entity, but may have unintended consequences if you delete valid certificates. Export all certificates before you reset.
- **Unapprove** is available on the Allowed Hosts tab. This button removes approval from the selected certificate. The next time the server that uses this certificate connects to the station the system warns you that the certificate is not valid.
- **View** opens the selected certificate so you can to view its details.

Generate Self-Signed Certificate window

This window defines the important information required to create a certificate. You use this window to create your own certificates along with a key pair (public and private).

Figure 209 Default view of the Generate Self-Signed Certificate window

This window opens when you click **New** at the bottom of the **User Key Store** tab.

A self-signed certificate provides data encryption only. Since it is not signed by a CA (Certificate Authority) it cannot verify server identify. Generating a self-signed certificate should be a temporary measure until a signed certificate is installed in the browser's and station's trust stores. After installing the signed certificate you should delete any self-signed certificates.

There is a limit of 64 characters for each of the following properties. Although blank properties are permitted, it is recommended to correctly fill in all properties, as not doing so may generate errors, or cause third-party CAs to reject your certificate. Spaces and periods are allowed. Enter full legal names.

Name	Value	Description
Alias	text	A short name used to distinguish certificates from one another in the Key Store . This property is required. It may identify the type of certificate (root, intermediate, server), location or function. This name does not have to match when comparing the server certificate with the CA certificate in the client's Trust Store.
Common Name (CN)	text, required, alphanumeric; do not use "*" or "?" as part of the name	Also known as the Distinguished Name, this field should be the host name. It appears as the Subject in the User Key Store .
Organizational Unit (OU)	text	The name of a department within the organization or a Doing-Business-As (DBA entry). Frequently, this entry is listed as "IT", "Web Security," "Secure Services Department" or left blank.
Organization (O)	text	The legally registered name of your company or organization. Do not abbreviate this name. This property is required.

Name	Value	Description
Locality (L)	text	The city in which the organization for which you are creating the certificate is located. This is required only for organizations registered at the local level. If you use it, do not abbreviate.
State/Province (ST)	text	The complete name of the state or province in which your organization is located. This property is optional.
Country Code (C)	two-character ISO-format country code.	If you do not know your country's two-character code, check www.countrycode.org . This property is required.
Not Before	date	Specifies the date before which the certificate is not valid. This date on a server certificate should not exceed the Not Before date on the root CA certificate used to sign it.
Not After	date (defaults to one year from the Not Before date)	Specifies the expiration date for the certificate. This date on a server certificate should not exceed the Not After date on the root CA certificate used to sign it. A period no longer than a year ensures regular certificate changes making it more likely that the certificate contains the latest cryptographic standards, and reducing the number of old, neglected certificates that can be stolen and re-used for phishing and drive-by malware attacks. Changing certificates more frequently is even better.
Key Size	number	Specifies the size of the keys in bits. Four key sizes are allowed: 1024 bits, 2048 bits (this is the default), 3072 bits, and 4096 bits. Larger keys take longer to generate but offer greater security.
Certificate Usage:	text	Specifies the purpose of the certificate: server, client or CA certificate. Other certificate management software utilities may allow other usages.
Alternative Server Name	text	This property provides a name other than the Subject (Common Name) that the system can use to connect to the server. Like the Common Name, the system uses the Alternative Server Name to validate the server certificate making it possible to specify both an IP (Internet Protocol) and FQDN (Fully Qualified Domain Name).
Email Address	email address	The contact address for this certificate. It may also be the address to which your signed certificate (.pem file) will be sent.

Private Key Password window

This window creates a password, which the system requires when you export and import private keys.

This window has standard password-creation properties and control buttons.

Video Network views

The framework supports three video networks: Axis, Milestone and Maxpro.

Axis network

The Axis video driver (naxisVideo) supports Axis video cameras.

Supported features include:

- Automatic discovery of cameras
- PTZ operation, including Go To preset
- Focus and iris
- Surveillance Viewer
- Remote video connections
- Fox video streaming
- Graphics widgets
- Motion detection from the camera

These Axis features are not supported:

- Alarm video playback
- Live video playback
- Switching between live and playback video
- Bidirectional alarms

The Axis driver has been tested with these cameras:

- Axis P5635–E PTZ Dome Network Camera with firmware version 6.50.2.3
- AXIS M 1065-L Network Camera with firmware version 8.30.1.1

Other models may or may not work with the driver depending on the firmware version installed. It is recommended to upgrade the Axis camera to the current firmware when using this video driver.

Axis video driver requirements include the following:

- IP access between the camera and remote network controller
- Appropriate ports open; the defaults are port 80 for the web, port 554 for control, and port 9000 for data
- Security status of each camera. The software defaults to TLS (Transport Layer Security) secure communication.

NOTE: If one or more of your cameras does not support or is not configured to support secure communication, you can add a second network with TLS disabled for those cameras. In this scenario, you can keep all of your https-supported cameras on the Axis TLS network and add the legacy http cameras to the non-TLS enabled network.

Milestone network

Milestone provides four video management software products:

- XProtect Enterprise
- XProtect Professional
- XProtect Professional+
- XProtect Corporate

The framework supports these three products with two drivers:

- The **Milestone Network (nmilestone)** driver supports the XProtect Enterprise XProtect Professional, and XProtect Professional+ products.
- The **Milestone XProtect Network (xprotect)** driver supports the XProtect Corporate product.

CAUTION: The Milestone products do not support secure communication, therefore, it is not possible to secure the connection between a station and its Milestone devices.

Maxpro network

This network supports Maxpro cameras and NVRs (Network Video Recorder)

Supported features include:

- Automatic discovery of cameras
- NVR (Network Video Recorder) and camera health Status
- PTZ (Pan Tilt Zoom) operation including control and go-to presets
- Live and recorded video streams
- H.264 Codec
- RTSP (Real Time Streaming Protocol) and HPS (Honeywell Progressive Streaming)
RTSP streaming has been tested with Honeywell's HDZMD series camera.
- Read camera events and alarms
- Forward, rewind, fast forward, and fast rewind
- 1/2, 1, 2, 4, 6, 8 & 16 replay speeds
- Custom RTSP URL for RTSP streaming

The Maxpro driver does not support Fox streaming.

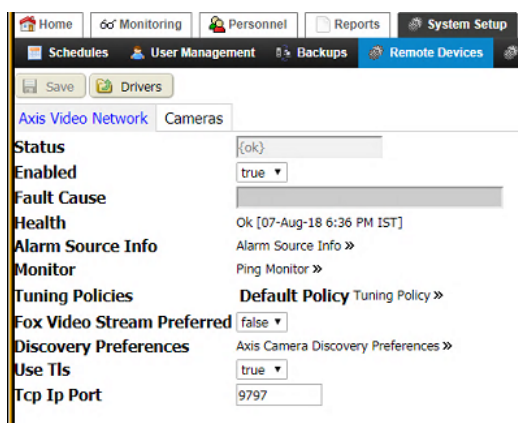
The Maxpro driver defaults to secure TLS communication with the exception of its RTSP protocol, which, in the Niagara 4.9 release does not support TLS. If your installation requires a connection to a camera or NVR that does not support TLS, you should replace the device with one that does support secure communication. If you must use a device that is not secure, change `Use Tls` (Network component Property Sheet) to `false` and change the `Address`, `Port` (Network and NVR Property Sheets) from 443 to 80.

CAUTION: Be aware that these changes relax the driver's security settings, compromising security to connect to a device that does not support secure communication. This opens your network to the potential of being hacked.

Axis Video Network tab

This view configures an Axis Video Network, which is primarily used for reader devices.

Figure 210 Axis Video Network tab



You access this tab from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Axis Video Network row in the table.

Properties

In addition to the common **Status**, **Enabled**, **Fault Cause** and **Health** properties, this tab includes these properties.

Property	Value	Description
Alarm Source Info	additional properties	Contains a set of properties for configuring and routing alarms when this component is the alarm source.
Monitor	additional properties	Configures ping properties. Refer to Monitor properties, page 223 .
Tuning Policies	additional properties	Defines the assigned tuning policy. Refer to (later in this topic).
Fox Video Stream Preferred	true or false (default)	
Discovery Preference, Do Not Ask Again	true or false (default)	true uses the fox connection to route video output from the camera to the station. false disables this feature.
Discovery Preference, Timeout	hours, minutes, seconds	This is the setting for specifying how long to try to discover an Axis camera before going to a timeout state.
Use Tls	true (default) or false	Configures secure communication between the station and network devices. By default, the system uses TLS secure communication. You would change this network property to false only if a legacy device (camera) cannot support TLS. 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.
Tcp Ip Port	number (defaults to 9797)	Identifies the network port, which connects the station to the network. If you have more than one Axis network in your system, each network requires its own unique port. As a best practice, consider using the default port (9797) for a legacy network with cameras that do not support security. When you create a second network for the camera(s) that support security, change this value to 9798.

Monitor properties

Property	Value	Description
Ping Enabled	true (default) or false	<p>Controls the monitor ping.</p> <p>true a ping occurs for each device under the network, as needed.</p> <p>false device status pings do not occur. The device status cannot change from what existed when this property was last true.</p> <p>It is recommended you leave Ping Enabled as true in almost all cases.</p>
Ping Frequency	hours:minutes:seconds	<p>Specifies the interval between periodic pings of all devices. Typical default value is every 5 minutes (05m 00s), you can adjust differently if needed.</p>
Alarm On Failure	true (default) or false	<p>Controls the recording of ping failure alarms.</p> <p>If true, the system records an alarm in the station's AlarmHistory upon each ping-detected device event ("down" or subsequent "up").</p> <p>If false, the system ignores and does not record device "down" and "up" events in the station's AlarmHistory.</p>
Startup Alarm Delay	hours:minutes:seconds	<p>Specifies the period a station must wait after restarting before device "down" or "up" alarms are generated. Applies only if the Monitor's property Alarm On Failure is true.</p>

Axis Network Tuning Policy

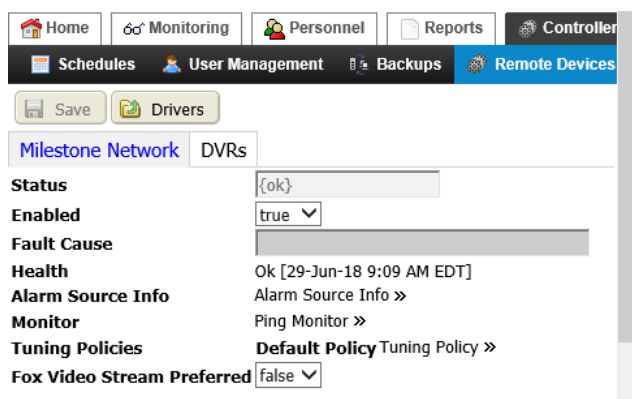
During polling, the system uses the network driver's tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.

Property	Value	Description
Min Write Time	hours minutes seconds	Specifies the minimum amount of time allowed between writes to writable proxy points, thus providing a method to throttle rapidly changing values so that only the last value is written. A value of zero (0) disables this rule causing all value changes to attempt to write.
Max Write Time	hours minutes seconds	If nothing else triggers a write to a proxy point, this property specifies the maximum amount of time to wait before rewriting the value. Any write action resets this timer. The default (zero) disables this rule resulting in no timed rewrites.
Stale Time	hours minutes seconds; defaults to 0 (zero)	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). 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}. The default value (zero) disables the stale timer causing points to become stale immediately when unsubscribed. Do not configure an amount of time shorter than the poll cycle time. If you do, points will go stale in the course of normal polling. Instead, set this time to be longer than the largest expected poll cycle time.

Milestone Network tab

This tab configures Milestone network properties.

Figure 211 Milestone Network tab



You access these properties from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Milestone Network row in the table.

To add a Milestone Network, click the Manage Drivers button (🔧), click **Add**, select the network and click **Ok**.

Properties

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties may be configured for a Milestone Network.

Property	Value	Description
Monitor	additional properties	Configures ping properties, alarm on failure and startup alarm delay. Refer to Monitor properties, page 225 .
Tuning Policies	additional properties	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Fox Video Stream Preferred	true or false (default)	

Monitor properties

Property	Value	Description
Ping Enabled	true (default) or false	Indicates of the ability to ping the network is on or off. Pinging the network ensures the system that its surveillance capabilities are up and running.
Ping Frequency	hours, minutes, seconds (defaults to 5 minutes)	Configures when to automatically ping the network.
Alarm On Failure	true (default) or false	Indicates if the failure of a ping should result in an alarm.
Startup Alarm Delay	hours, minutes, seconds (defaults to 5 minutes)	Configures a period of time before the system generates the alarm.

Milestone X Protect Network tab

This view and tab configures Milestone X Protect network properties.

Figure 212 Milestone X Protect Network tab

Home Monitoring Personnel Reports System Setup

Schedules User Management Backups Remote Devices

Save Drivers

Milestone X Protect Network DVRs

Status {ok}

Enabled true

Fault Cause

Health Ok [13-Sep-18 2:58 PM EDT]

Alarm Source Info Alarm Source Info >>

Monitor Ping Monitor >>

Tuning Policies Default Policy Tuning Policy >>

Fox Video Stream Preferred false

Native Process Port 58320

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support Milestone X Protect networks.

Property	Value	Description
Monitor	additional properties	Configures ping properties, alarm on failure and startup alarm delay. Refer to Monitor properties, page 226 .
Tuning Policies	additional properties	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Fox Video Stream Preferred	true or false (default)	
Native Process Port	read-only	Displays the port.

Monitor properties

Property	Value	Description
Ping Enabled	true (default) or false	Indicates of the ability to ping the network is on or off. Pinging the network ensures the system that its surveillance capabilities are up and running.
Ping Frequency	hours, minutes, seconds (defaults to 5 minutes)	Configures when to automatically ping the network.
Alarm On Failure	true (default) or false	Indicates if the failure of a ping should result in an alarm.
Startup Alarm Delay	hours, minutes, seconds (defaults to 5 minutes)	Configures a period of time before the system generates the alarm.

Maxpro Network tab

This view configures an Maxpro Network, which is primarily used for reader devices.

Figure 213 Maxpro Network tab

The screenshot displays the 'Maxpro Network' configuration page. At the top, there is a navigation bar with tabs for Home, Monitoring, Personnel, Reports, System Setup (selected), and Threat Levels. Below this is a secondary menu with Schedules, User Management, Backups, Remote Devices (selected), and Access Setup. The main content area has a 'Save' button and a 'Drivers' button. The configuration fields are as follows:

- Status:** {ok}
- Enabled:** true
- Fault Cause:** (empty field)
- Health:** Ok [12-Dec-19 4:19 PM EST]
- Alarm Source Info:** Alarm Source Info »
- Monitor:** Ping Monitor »
- Tuning Policies:** Default Policy Tuning Policy »
- Fox Video Stream Preferred:** false

You access this tab from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Maxpro Network row in the table.

Properties

In addition to the common **Status**, **Enabled**, **Fault Cause** and **Health** properties, this tab includes these properties.

Property	Value	Description
Alarm Source Info	additional properties	Contains a set of properties for configuring and routing alarms when this component is the alarm source.
Monitor	additional properties	Configures ping properties. Refer to Monitor properties, page 227 .
Tuning Policies	additional properties	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests. Refer to Tuning Policy, page 227 (later in this topic).
Fox Video Stream Preferred	true or false (default)	

Monitor properties

Property	Value	Description
Ping Enabled	true (default) or false	Controls the monitor ping. true a ping occurs for each device under the network, as needed. false device status pings do not occur. The device status cannot change from what existed when this property was last true. It is recommended you leave Ping Enabled as true in almost all cases.
Ping Frequency	hours:minutes:seconds	Specifies the interval between periodic pings of all devices. Typical default value is every 5 minutes (05m 00s), you can adjust differently if needed.
Alarm On Failure	true (default) or false	Controls the recording of ping failure alarms. If true, the system records an alarm in the station's AlarmHistory upon each ping-detected device event ("down" or subsequent "up"). If false, the system ignores and does not record device "down" and "up" events in the station's AlarmHistory.
Startup Alarm Delay	hours:minutes:seconds	Specifies the period a station must wait after restarting before device "down" or "up" alarms are generated. Applies only if the Monitor's property Alarm On Failure is true.

Tuning Policy

During polling, the system uses the network driver's tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.

Property	Value	Description
Min Write Time	hours minutes seconds	Specifies the minimum amount of time allowed between writes to writable proxy points, thus providing a method to throttle rapidly changing values so that only the last value is written. A value of zero (0) disables this rule causing all value changes to attempt to write.
Max Write Time	hours minutes seconds	If nothing else triggers a write to a proxy point, this property specifies the maximum amount of time to wait before rewriting the value. Any write action resets this timer. The default (zero) disables this rule resulting in no timed rewrites.
Stale Time	hours minutes seconds; defaults to 0 (zero)	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). 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}. The default value (zero) disables the stale timer causing points to become stale immediately when unsubscribed. Do not configure an amount of time shorter than the poll cycle time. If you do, points will go stale in the course of normal polling. Instead, set this time to be longer than the largest expected poll cycle time.

DVR and NVR views

Cameras and displays (Milestone only) connect to network network through a DVR (Digital Video Recorder) or NVR (Network Video Recorder).

The system supports these DRV's and an NVR:

- The nmilestone driver supports the Milestone DVR.
- The xprotect driver supports an X Protect DVR.
- The maxpro driver supports a Maxpro NVR.

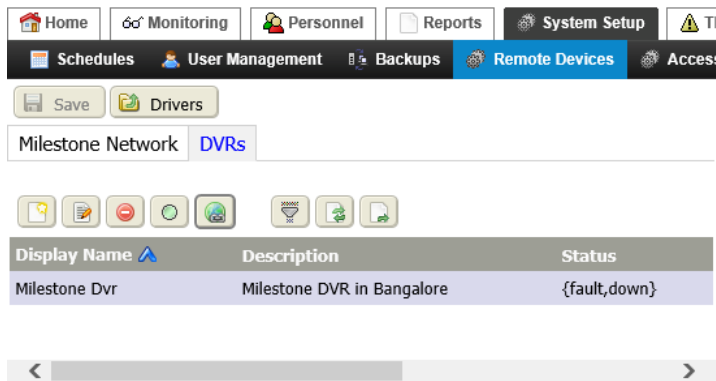
Both a DVR and an NVR record video. They differ in where they process the video stream and in the type of camera each requires:

- DVRs are wired security systems that use analog cameras. They process and store video data at the recorder.
- NVRs can be wired or wireless systems. Most require IP cameras. NVRs encode and process video at the camera, then stream the video to the recorder, which provides storage and remote viewing.

Milestone DVRs tab

This tab and view list the DVRs (Digital Video Recorders) supported by the nmilestone driver.






Figure 214 DVRs tab



You access this view from the main menu by clicking **System Setup**→**Remote Devices**→**Drivers** followed by double-clicking the Milestone Network row in the table, and clicking the **DVRs** tab.

Buttons

In addition to the standard buttons (Delete, Filter, Refresh and Export), these buttons support Milestone DVRs.

-  New opens the **New** window for adding a Milestone network driver.
-  Edit opens the component's Edit window.
-  or  Ping (or wink) sends a command to the remote device or server.
-  Hyperlink opens the DVR view at the **Milestone Dvr** tab.

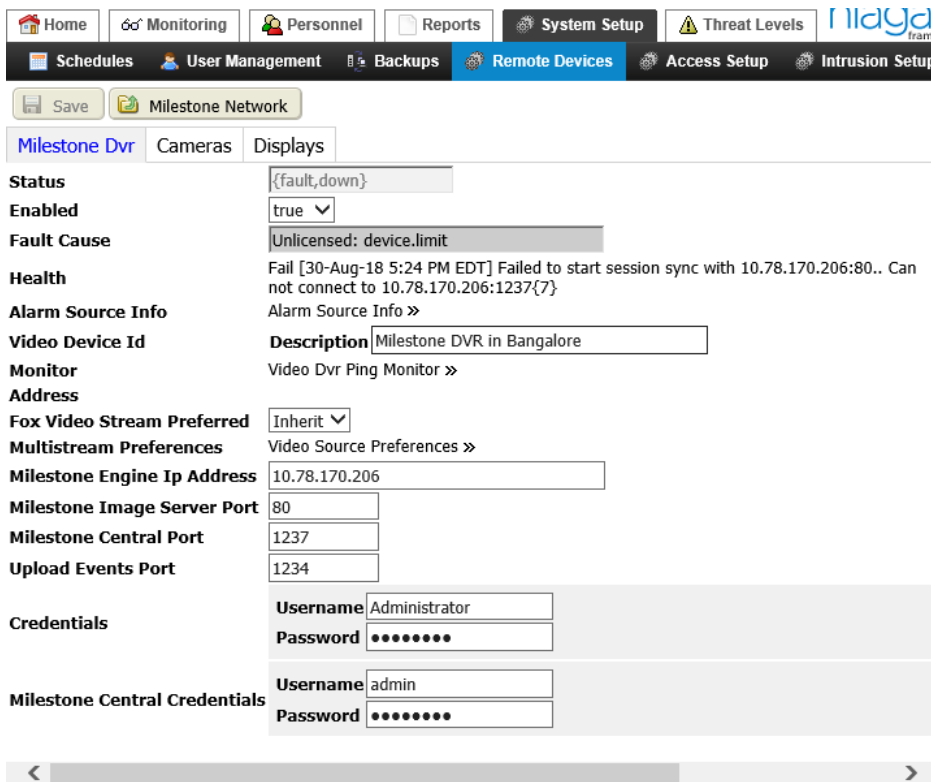
Columns

Column	Description
Display Name	Displays the name given to this DVR when the database record was created.
Description	Displays additional information about the DVR, such as its location, etc.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}

Milestone Dvr tab

This tab configures the nmilestone driver.

Figure 215 Milestone DVR tab



You access this tab from the main menu by clicking **Controller (System) Setup**→**Remote Devices**→**Remote Drivers**, double-clicking the Milestone Network, clicking the DVRs tab, followed by double-clicking a row in the DVR Manager table.

In addition to the common **Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info** properties, these properties support the DVR.

Property	Value	Description
Video Device Id, Description	text	Defines the name of the DVR that appears in the manager view.
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 Monitor properties, page 231 .
Fox Video Stream Preferred		For a network component, selects (<i>true</i>) or declines (<i>false</i>) the use of Fox streaming. For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level. <i>Inherit</i> sets this property to the value set for its parent component (the DVR, NVR or network component). <i>Yes</i> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.

Property	Value	Description
		<p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p>No sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to High without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Multistream Preferences		Refer to Multistream Preferences, page 232 .
Milestone Engine IP Address	IP address	Displays an IP address.
Milestone Image Server Port	number (defaults to 80)	Configures the DVR port.
Milestone Central Port	number (defaults to 1237)	Defines the port.
Upload Events Port	number (defaults to 1234)	Defines the port.
Credentials, Username and Password	text	Identify the username and password required to access the DVR.
Milestone Central Credentials, Username and Password	text	Identify the username and password required to access the server.

Monitor properties

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.

Multistream Preferences

Property	Value	Description
Preferred Background Color	color chooser (defaults to black)	Opens the color chooser. The color you select affects the border or margin area around the video display.
Preferred Aspect Ratio	drop-down list (defaults to Standard Definition (1.33:1))	<p>Defines the ratio of the width to the height of the video frame. Options include <i>Inherit from camera</i> (default), <i>Standard Definition</i>, <i>Inherit from Stream</i>, <i>Fit to Screen</i>, etc.</p> <p>Resolution at the device or network may be linked to the video stream options and inherited. In some cases, this may adversely affect the aspect ratio of your streaming video. If video images display distorted, try setting the camera's Preferred Aspect Ratio to the <i>Standard Definition</i> option.</p>
Preferred Resolution	drop-down list (defaults to High)	Specifies the pixel resolution of each transmitted frame. Options are: <i>High</i> , <i>Medium</i> , or <i>Low</i> . The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list (defaults to Low)	Defines the speed of the video stream. Options are: <i>Low</i> , <i>Medium</i> , and <i>High</i> . You can configure each rate.
Preferred Compression	drop-down list (defaults to Medium)	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <i>None</i> , <i>Low</i> , <i>Medium</i> , or <i>High</i> .
Preferred Video Stream Fox	drop-down list (defaults to Inherit)	<p>For a network component, selects (<i>true</i>) or declines (<i>false</i>) the use of Fox streaming.</p> <p>For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level.</p> <p><i>Inherit</i> sets this property to the value set for its parent component (the DVR, NVR or network component).</p> <p><i>Yes</i> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.</p> <p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p><i>No</i> sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to <i>High</i> without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>

Property	Value	Description
Timestamp Preferred	true (default) or false	Configures the camera to record and display (true) a timestamp on the video.
Interframe Timeout	hours, minutes, seconds	Defines the maximum amount of time permitted to elapse between frames. A video stream that takes longer than this amount of time to retrieve a video frame needs to be re-established.

Milestone New DVR window

This window configures Milestone DVR properties

Figure 216 New DVR window

You open this window from the main menu by clicking **Controller Setup**→**Remote Devices**→ followed by double-clicking the Milestone Network row in the table, clicking the **DVRs** tab., and clicking the New button (🔑).

Properties

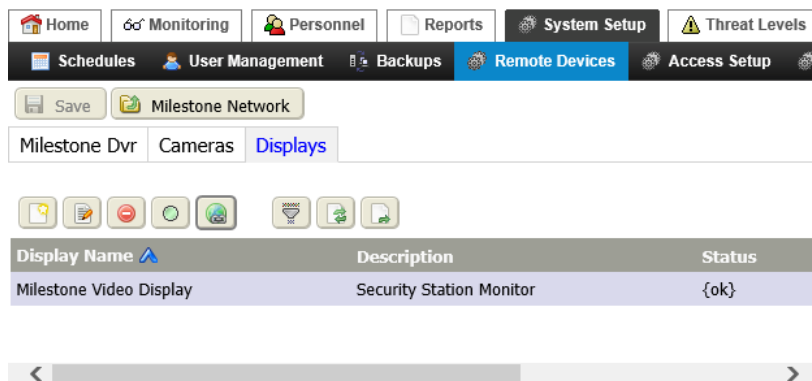
Property	Value	Description
Display Name	text	Provides a unique name for the DVR.
Description	text	Provides additional information about the DVR.
Fox Video Stream Preferred	true or false (default)	
Milestone Engine Ip Address	IP address	Identifies the DVR software by its IP address.
Milestone Image Server Port	number	Identifies the port to use by the Image server (one of Milestone's two servers).
Milestone Central Port	number	Identifies the port used by the Central server (the other of Milestone's two servers).
Upload Events Port	number	Not supported in Niagara Enterprise Security 4.8 or later.

Property	Value	Description
Credentials	Username and Password	Specifies the credentials required for the Milestone Image Server, which supports live playback video streaming.
Milestone Central Credentials	Username and Password	Specifies credentials the required by the Central server, which supports motion events.

Milestone Displays tab






This view manages the Milestone display(s).

Figure 217 Displays view



Buttons

In addition to the standard buttons (Delete, Filter, Refresh and Export), these buttons support Milestone displays.

-  New opens the **New** window for adding a Milestone display. This window contains two properties: **Display Name**, and **Description**.
-  Edit opens the component's Edit window.
-  or  Ping (or wink) sends a command to the remote device or server.
-  Hyperlink opens the Display camera grid.

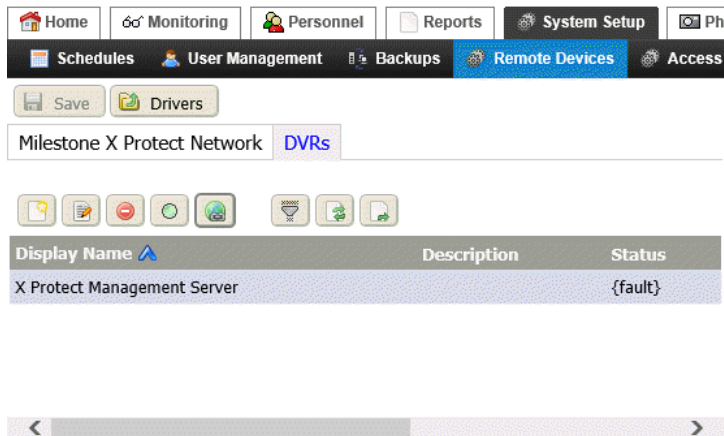
Columns

Column	Description
Display Name	Displays the name given to this display when the database record was created.
Description	Displays additional information about the display, such as its location, etc.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}

X Protect DVRs tab

This tab and view list the DVRs (Digital Video Recorders) supported by the Milestone xprotect driver.






Figure 218 Milestone X Protect DVRs tab



You access this view from the main menu by clicking **System Setup**→**Remote Devices**→**Drivers** followed by double-clicking the Milestone XProtect Network row in the table, and clicking the **DVRs** tab.

Buttons

In addition to the standard buttons (Delete, Filter, Refresh and Export), these buttons support Milestone X Protect DVRs.

-  New opens the **New** window for adding a DVR.
-  Edit opens the component's Edit window.
-  or  Ping (or wink) sends a command to the remote device or server.
-  Hyperlink opens the DVR view at the **Milestone Dvr** tab.

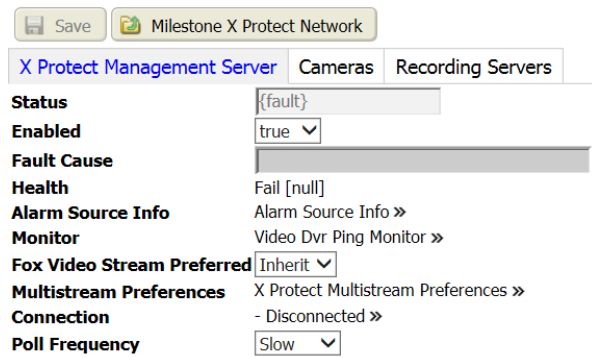
Columns

Column	Description
Display Name	Displays the name given to this DVR when the database record was created.
Description	Displays additional information about the DVR, such as its location, etc.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}

X Protect Management Server tab

This tab configures server properties.

Figure 219 X Protect Management Server tab



In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support the Milestone X Protect Management Server.

Property	Value	Description
Monitor	additional properties	Refer to Monitor properties, page 237 .
Fix Video Stream Preferred	drop-down list	Configures the source of the video stream.
Multistream Preferences	additional properties	Refer to Multistream Preferences, page 237 .
Connection	additional properties	Refer to Connection properties, page 238 .
Poll Frequency	drop-down list, defaults to <code>Slow</code>	Selects polling frequency. The Polling Service defines the value for each rate. <code>Fast</code> defines a target polling rate—often one second. <code>Normal</code> defines a medium target polling rate—often five seconds. <code>Slow</code> defines a moderate target polling rate—often 30 seconds.

Monitor properties

Property	Value	Description
Ping Enabled	true (default) or false	Controls the monitor ping. true a ping occurs for each device under the network, as needed. false device status pings do not occur. The device status cannot change from what existed when this property was last true. It is recommended you leave Ping Enabled as true in almost all cases.
Ping Frequency	hours:minutes:seconds	Specifies the interval between periodic pings of all devices. Typical default value is every 5 minutes (05m 00s), you can adjust differently if needed.
Alarm On Failure	true (default) or false	Controls the recording of ping failure alarms. If true, the system records an alarm in the station's AlarmHistory upon each ping-detected device event ("down" or subsequent "up"). If false, the system ignores and does not record device "down" and "up" events in the station's AlarmHistory.

Multistream Preferences

Property	Value	Description
Preferred Background Color	opens a color chooser (defaults to black)	Opens the color chooser. The color you select affects the border or margin area around the video display.
Preferred Aspect Ratio	drop-down list (defaults to Standard Definition (1.33:1))	Defines the ratio of the width to the height of the video frame. Options include Inherit from camera (default), Standard Definition, Inherit from Stream, Fit to Screen, etc. Resolution at the device or network may linked to the video stream options and inherited. In some cases, this may adversely affect the aspect ratio of your streaming video. If video images display distorted, try setting the camera's Preferred Aspect Ratio to the Standard Definition option.
Preferred Resolution	drop-down list, defaults to High	Specifies the pixel resolution of each transmitted frame. Options are: High, Medium, or Low. The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list, defaults to Low	Defines the speed of the video stream. Options are: Low, Medium, and High. You can configure each rate.
Preferred Compression	drop-down list, defaults to Medium	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: None, Low, Medium, or High
Preferred Video Stream Fox	drop-down list, defaults to Inherit	For a network component, selects (true) or declines (false) the use of Fox streaming.

Property	Value	Description
		<p>For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level.</p> <p>Inherit sets this property to the value set for its parent component (the DVR, NVR or network component).</p> <p>Yes sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.</p> <p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p>No sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to High without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Timestamp Preferred	true (default) or false	Configures the camera to record and display (true) a timestamp on the video.
Interframe Timeout	hours, minutes, seconds	Defines the maximum amount of time permitted to elapse between frames. A video stream that takes longer than this amount of time to retrieve a video frame needs to be re-established.

Connection properties

Figure 220 Connection properties

192.168.1.111 - Connected ▾

Host Name

X Protect Auth Config ▾

Auth Type Basic ▾

Auth

Domain

Username admin

Password

Connection State Connected ▾

X Protect Auth Attributes ▾

Auth Attributes

Token

Token Expiration 07 ▾ Nov ▾ 2019 09 ▾ : 23 ▾ AM ▾ IST

Uri

Server Id

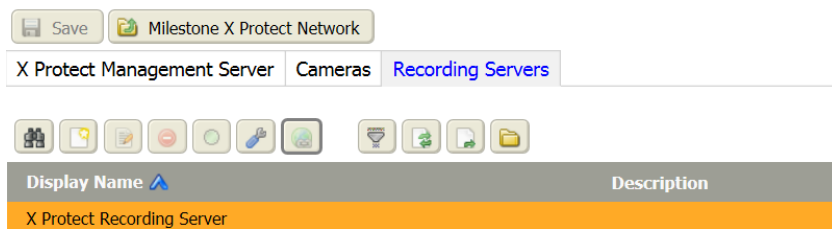
Property	Value	Description
Host Name	text	Defines the xprotect corporate server’s host name.
Auth, Auth Type	drop-down list (defaults to Basic)	Defines the type of authentication to use to access the Milestone corporate server: Basic or Windows-based user authentication.

Property	Value	Description
Auth, Domain	domain name format	Defines the domain name when the authentication type is Windows.
Auth, Username	text	Defines the user name required by the Milestone corporate server.
Auth, Password	text	Defines the password required by the Milestone corporate server.
Connection State	read-only	Reports the status of the connection.
Auth Attributes, Token	read-only	Indicates the token Enterprise Security receives upon completion of a successful authentication. This token is used later.
Auth Attributes, Token Expiration	read-only	Indicates when the token becomes no longer valid. Until this date, the system uses the token in any number of image-server connect requests. During an open image-server session, the token stands in for the user name and password. The framework sends a request for a new token before the current token expires.
Auth Attributes, Uri	read-only	Reports the URI to which to connect to get an updated token.
Auth, Server Id	read-only	Identifies the Milestone xprotect corporate server.

X Protect Recording Servers tab

This tab and view list the X Protect recording servers associated with the xprotect driver.






Figure 221 X Protect Recording Servers view



You access this view from the main menu by clicking **System Setup**→**Remote Devices**→**Drivers** followed by double-clicking the Milestone X Protect Network row in the table, and clicking the **Recording Servers** tab.

Buttons

In addition to the standard buttons (Discover, Delete, Filter, Refresh and Export), these buttons support X Protect servers

-  New opens the **New** window for adding an X Protect server.
-  Edit opens the component's Edit window.
-  or  Ping (or wink) sends a command to the remote device or server.
-  Hyperlink opens the X Protect Recording Server view.

Columns

Column	Description
Display Name	Displays the name given to this X Protect server when the database record was created.
Description	Displays additional information about the server, such as its location, etc.

X Protect Recording Server tab

This tag configures properties for the X Protect Recording Server.

Figure 222 X Protect Recording Server tab

You access this view from the main menu by clicking **System Setup**→**Remote Devices**→**Drivers** followed by double-clicking the Milestone X Protect Network row in the table, and clicking the **Recording Servers** tab, followed by double-clicking a server row.

Properties

In addition to the standard properties (Status and Enabled), these properties support an X Protect recording server.

Property	Value	Description
Id	additional properties	Refer to Id properties, page 240 .
Poll Frequency	drop-down list, defaults to <code>Slow</code>	Selects polling frequency. The Polling Service defines the value for each rate. <code>Fast</code> defines a target polling rate—often one second. <code>Normal</code> defines a medium target polling rate—often five seconds. <code>Slow</code> defines a moderate target polling rate—often 30 seconds.

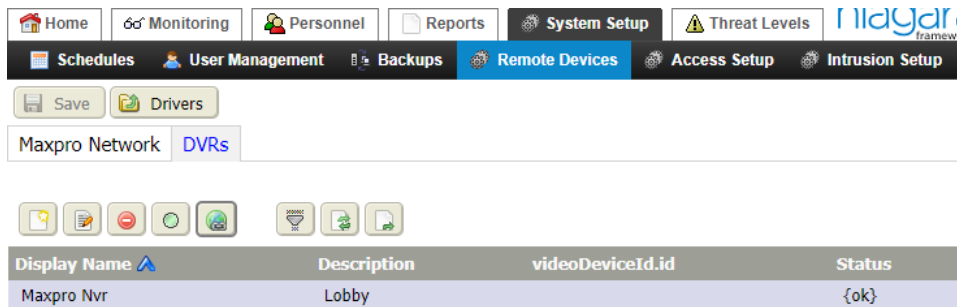
Id properties

Property	Value	Description
Description	text	Defines the name of the server that appears in the manager view.
Server Type	drop-down list	Selects the type of server.
Hostname	text	Defines the server host name.
Port	number	Defines the port with which the server communicates.
Id	number	Defines a unique ID for the server.

Maxpro Nvrs tab

This tab and view list the NVRs (Network Video Recorders) supported by the Maxpro driver.






Figure 223 Maxpro Nvrs tab



You access this view from the main menu by clicking **System Setup**→**Remote Devices**→**Drivers** followed by double-clicking the Maxpro Network row in the table, and clicking the **NVRs** tab.

Buttons

In addition to the standard buttons (Delete, Filter, Refresh and Export), these buttons support Maxpro NVRs.

-  New opens the **New** window for adding a new NVR.
-  Edit opens the component's Edit window.
-  or  Ping (or wink) sends a command to the remote device or server.
-  Hyperlink opens the NVR view at the **Maxpro** tab.

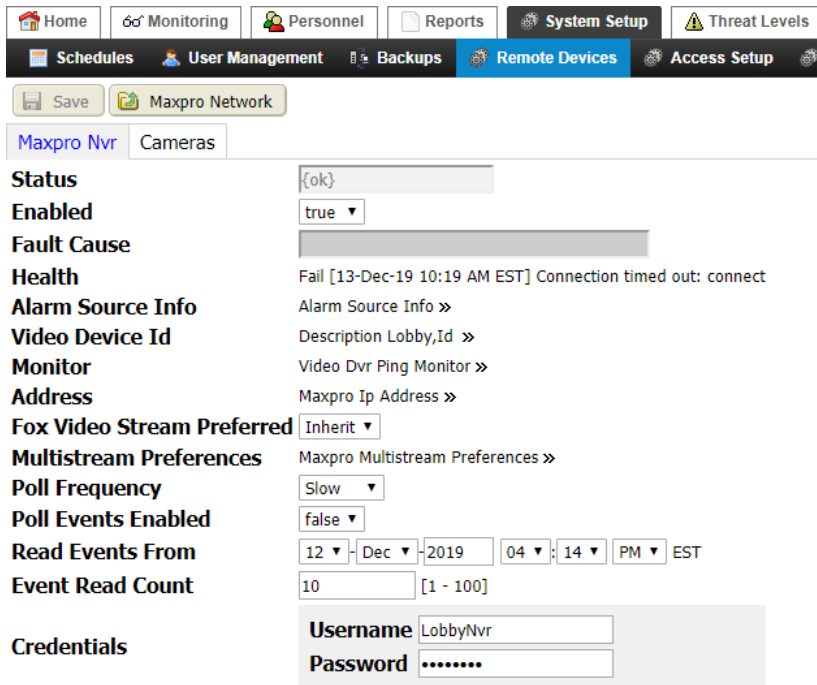
Columns

Column	Description
Display Name	Displays the name given to this NVR when the database record was created.
Description	Displays additional information about the NVR, such as its location, etc.
videoDeviceId	Displays the ID of this video device.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}

Maxpro NVR tab

This tab configures the maxpro driver to support an NVR.

Figure 224 Maxpro NVR tab



You access this view from the main menu by clicking **System (Setup) Controller→Remote Devices→Drivers** followed by double-clicking the Maxpro Network row in the table, clicking the **NVRs** tab and double-clicking the NVR row in the table.

In addition to the common **Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info** properties, these properties support the NVR.

Property	Value	Description
Video Device Id, Description	text	Identifies the Display Name and Description for the NVR.
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 Monitor properties, page 243 .
Address	IP address	Defines the Maxpro IP address.
Fox Video Stream Preferred	drop-down list	For a network component, selects (<i>true</i>) or declines (<i>false</i>) the use of Fox streaming. For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level. <i>Inherit</i> sets this property to the value set for its parent component (the DVR, NVR or network component). <i>Yes</i> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.

Property	Value	Description
		<p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p>No sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to High without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Multistream Preferences	additional properties	Refer to Multistream Preferences, page 244 .
Poll Frequency	drop-down list (defaults to Slow)	<p>Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its input value. The network's Poll Service 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>
Poll Events Enabled	true or false (default)	Enables or disables the Poll Scheduler.
Read Events From	from and to dates	Defines a selected period from which to report events.
Event Read Count	number	Configures the number of events to report.
Credentials, Username and Password	text	Defines the user name and password required to access the NVR.

Monitor properties

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.

Multistream Preferences

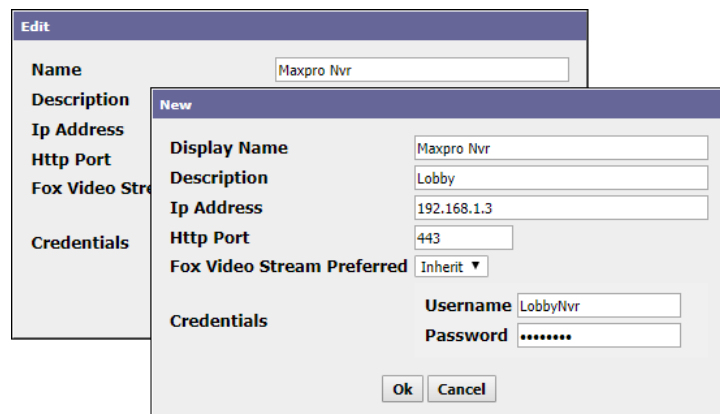
Property	Value	Description
Preferred Background Color	color chooser (defaults to black)	Opens the color chooser. The color you select affects the border or margin area around the video display.
Preferred Aspect Ratio	drop-down list (defaults to Standard Definition (1.33:1))	<p>Defines the ratio of the width to the height of the video frame. Options include <i>Inherit from camera</i> (default), <i>Standard Definition</i>, <i>Inherit from Stream</i>, <i>Fit to Screen</i>, etc.</p> <p>Resolution at the device or network may be linked to the video stream options and inherited. In some cases, this may adversely affect the aspect ratio of your streaming video. If video images display distorted, try setting the camera's Preferred Aspect Ratio to the <i>Standard Definition</i> option.</p>
Preferred Resolution	drop-down list (defaults to High)	Specifies the pixel resolution of each transmitted frame. Options are: <i>High</i> , <i>Medium</i> , or <i>Low</i> . The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list (defaults to Low)	Defines the speed of the video stream. Options are: <i>Low</i> , <i>Medium</i> , and <i>High</i> . You can configure each rate.
Preferred Compression	drop-down list (defaults to Medium)	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <i>None</i> , <i>Low</i> , <i>Medium</i> , or <i>High</i> .
Preferred Video Stream Fox	drop-down list (defaults to Inherit)	<p>For a network component, selects (<i>true</i>) or declines (<i>false</i>) the use of Fox streaming.</p> <p>For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level.</p> <p><i>Inherit</i> sets this property to the value set for its parent component (the DVR, NVR or network component).</p> <p><i>Yes</i> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.</p> <p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p><i>No</i> sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to <i>High</i> without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Timestamp Preferred	<i>true</i> (default) or <i>false</i>	Configures the camera to record and display (<i>true</i>) a timestamp on the video.
Interframe Timeout	hours, minutes, seconds	Defines the maximum amount of time permitted to elapse between frames. A video stream that takes longer than this

Property	Value	Description
		amount of time to retrieve a video frame needs to be re-established.
Lo Frame Rate	from one (1) to 30 frames per second (defaults to 4)	Configures what a low frame rate means.
Med Frame Rate	from one (1) to 30 frames per second (defaults to 15)	Configures what a medium frame rate means.
Hi Frame Rate	from one (1) to 30 frames per second (defaults to 30)	Configures what a high frame rate means.

Maxpro New and Edit NVR windows

This window configures an NVR for use on a Maxpro network.

Figure 225 Example of a New NVR window

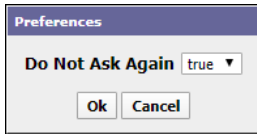


Property	Value	Description
Display Name/Name	text	Defines a short name for the Nvr.
Description	text	Provides an opportunity for additional information.
Ip Address	IP address	Defines the IP address of the Nvr.
Http Port	number (defaults to 443)	Defines the Internet port over which to transmit the Nvr data. 443 supports only secure communication (TLS). RTSP does not support TLS. If your application requires RTSP, change this property to 80. CAUTION: Be aware that the framework cannot prevent a flooding attack or other malicious activity if you choose to configure your application without secure communication.
Fox Video Stream Preferred		
Credentials		Sets up the user name and password required by the Nvr.

Maxpro camera Preferences window

This window configures Maxpro camera properties

Figure 226 Maxpro camera Preferences property



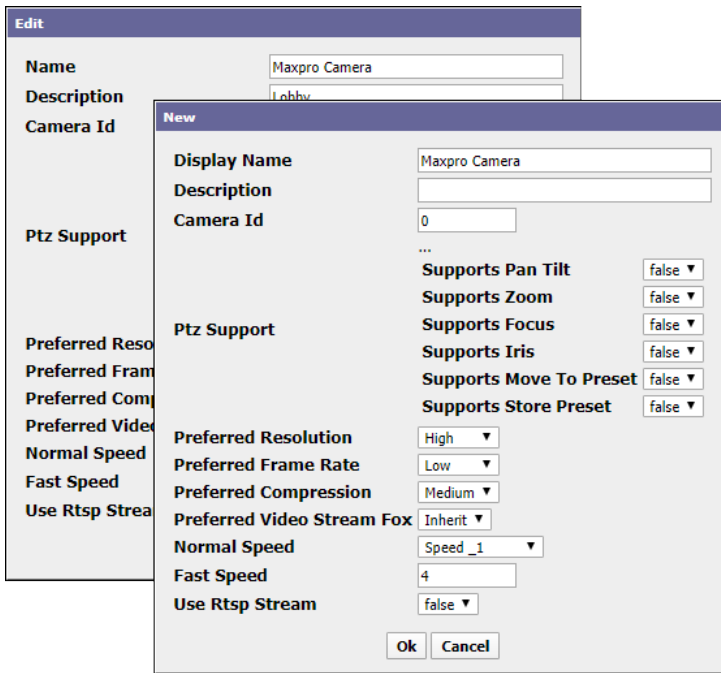
You open this window from the main menu by clicking **Controller (System) Setup→Remote Devices→Remote Drivers**, double-clicking the Maxpro Network, clicking the NVRs tab, double-clicking a row in the NVR Manager table, followed by selecting an existing camera and clicking the Preferences button (🔧).

Property	Value	Description
Do Not Ask Again	true (default) or false	

Maxpro New and Edit camera windows

This window configures camera properties

Figure 227 Maxpro Edit and New camera window properties



You open this window from the main menu by clicking **Controller (System) Setup→Remote Devices→Remote Drivers**, double-clicking the Maxpro Network, clicking the NVRs tab, double-clicking a row in the NVR Manager table, followed by clicking the New button (👤) or selecting an existing camera and clicking the Edit button (🔧).

Property	Value	Description
Display Name/ Name	text	Provides a short name for the camera.
Description	text	Provides a longer name for the camera. This name could include the camera's location or special configuration properties.
Camera Id	number	Assigns a number to the camera.
Ptz Support	additional properties	Turns Pan Tilt, Zoom, Focus, Iris, Move To Preset, and Store Preset features on (<code>true</code>), and off (<code>false</code>). Your camera may or may not support these features. For each feature the camera supports, select <code>true</code> . For unsupported features, select <code>false</code> . NOTE: If these properties are not enabled, PTZ functions do not work. This means that any widgets that use PTZ controls do not work.
Control Timing	hours, minutes and seconds	Configures intervals between actions and timeout values. These settings affect how long a camera continues to respond to control communications after a control message is received. The reason for these limits is to prevent a camera from being left in a state of continual movement or adjustment (iris, focus, or zoom) in case communication with the device is lost.
Preferred Resolution	drop-down list	Specifies the pixel resolution of each transmitted frame. Options are: <code>High</code> , <code>Medium</code> , or <code>Low</code> . The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list	Defines the speed of the video stream. Options are: <code>Low</code> , <code>Medium</code> , and <code>High</code> . You can configure each rate.
Preferred Compression	drop-down list	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <code>None</code> , <code>Low</code> , <code>Medium</code> , or <code>High</code>
Preferred Video Stream Fox	drop-down list	Configures the degrees of pan and tilt and the speed at which the camera zooms in and out. Values depend on the specific camera.
Normal Speed	<code>true</code> or <code>false</code>	Turns the automatic configuration of the Ptz properties on <code>true</code> and off <code>false</code> .
Fast Speed	drop-down list	Defines the speed of a quick pan or tilt.
Use Rtsp Stream	<code>true</code> or <code>false</code> (default)	Turns RTSP (Real Time Streaming Protocol) on and off. This protocol controls a camera using DVD-style controls (play, pause, etc.) CAUTION: RTSP does not support TLS secure communication. Using this protocol may open your video network to be hacked. <code>true</code> enables RSTP streaming. <code>false</code> enables HPS (Honeywell Progressive Streaming). Playback video always streams using HPS.

Video camera views

The system supports video cameras from these manufacturers: Axis, Milestone and Maxpro. For the specific models supported, refer to the manufacturer's documentation.

Axis

Axis network cameras function in many environments. To add one of these cameras to your network, navigate to **Controller Setup**→**Remote Devices**→**Remote Drivers** and add an Axis Video Network or double-click the existing Axis Video Network row in the table. Next click the **Cameras** tab and discover already connected cameras or add one or more new cameras.

Milestone cameras and displays

Milestone cameras are specifically designed for building management applications. To add one of these cameras or a display to your network, navigate to **Controller Setup**→**Remote Devices**→**Remote Drivers** and add a Milestone Network (driver: nmilestone) or a MilestoneXProtectNetwork (driver: xprotect), or double-click the existing row in the table. Next click the **DVRs** tab, add a DVR, double-click its row in the table, and click the **Cameras** tab. Finally, discover already connected cameras or add one or more new cameras.

To add a display, click the **Displays** tab under the Milestone DVR view.

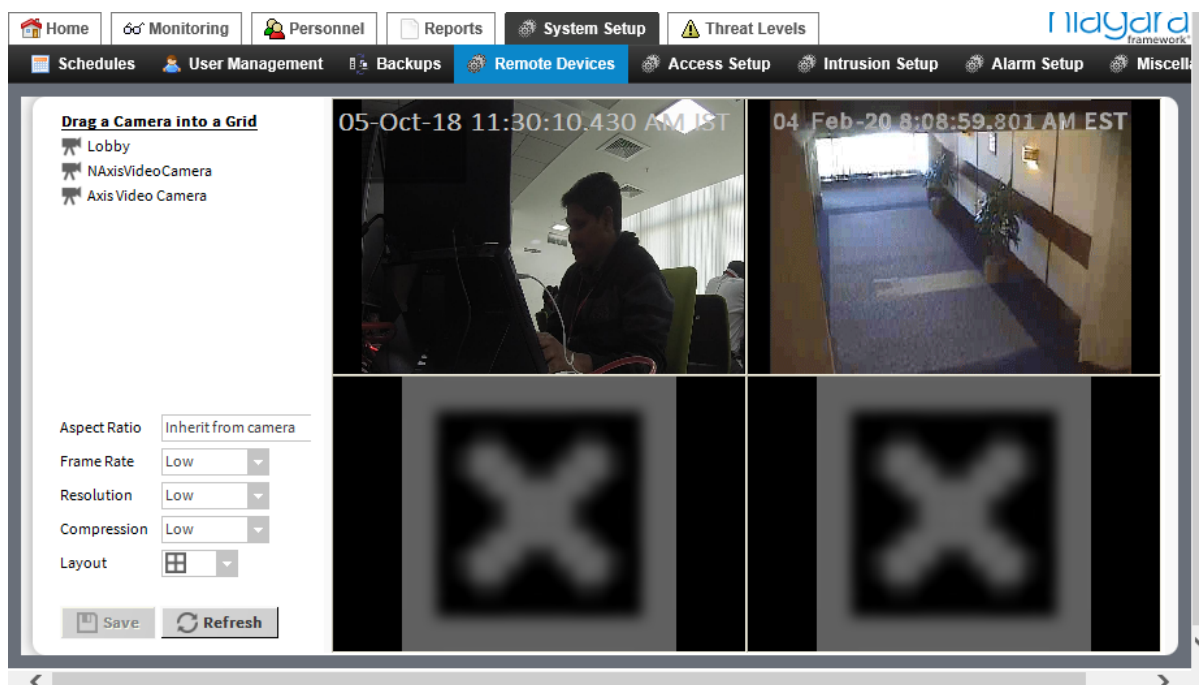
Maxpro cameras

Maxpro cameras support building management applications. To add one of these cameras to your network, navigate to **Controller Setup**→**Remote Devices**→**Remote Drivers** and add a Maxpro Network (driver: maxpro) or double-click the existing row in the table. Next click the **NVRs** tab, add an NVR, double-click its row in the table, and click the **Cameras** tab. Finally, discover already connected cameras or add one or more new cameras.

Display camera grid

This view displays live video feeds from up to nine cameras.

Figure 228 Display camera grid



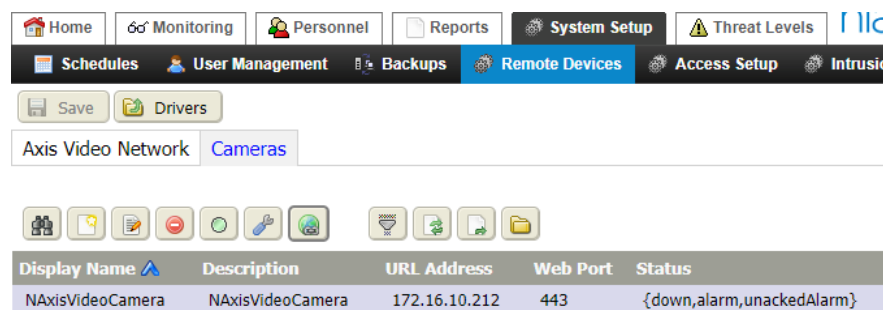
Properties

Property	Value	Description
Aspect Ratio	drop-down list	Specifies the ratio of the image width to image height.
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.

Axis Cameras tab

This view discovers and configures an Axis camera.




Figure 229 Axis Video Network, Cameras tab



You access this tab from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Axis Video Network row in the table, and clicking the **Cameras** tab.

Buttons

In addition to the common control buttons (Discover, New, Edit Delete, Hyperlink, Filter, Refresh, Export and Learn Mode), these buttons provide camera functions:

-  or  Ping (or wink) sends a command to the remote device or server.
-  Preferences opens a Preferences window with common configuration properties.

Columns

Column	Description
Display Name	Reports the camera name.
Description	Provides additional information.
URL Address	Identifies the camera's address, usually the IP address.
Web Port	Reports the port used to communicate with the camera feed over the Internet. Port 433 is secure; 80 is not.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}

Axis New camera window

This window configures camera properties.

Figure 230 New Axis camera window

Property	Value	Description
Display Name	text	Defines the name of the camera that appears in the Camera Manager view.
Description	text	Provides an opportunity for additional information.
Url Address	text	Defines a URL or IP address for the camera.
Web Port	number (defaults to 443)	<p>Defines the port, when using the web UI, over which to transmit the camera’s video signal. 443 supports only secure communication between the camera and the station.</p> <p>For a camera that does not support TLS secure communication, that is, if Use Rtsp Stream is true or if you are using the HTTP protocol (Use Tls is false and Use Rtsp Stream is false), change this property to 80.</p> <p>CAUTION: Be aware that the framework cannot prevent a flooding attack or other malicious activity if you choose to configure your application without secure communication.</p> <p>If using fox streaming, which uses the station to render the video stream, this port should be different from the station’s fox</p>

Property	Value	Description
		port. If you are not using fox streaming, this port should be the same as the station's fox port.
Ptz Support, Pan Tilt, Zoom, Focus, Iris, Move to Preset, Supports Tore Preset	true or false (default)	Turns these camera features on (<i>true</i>), and off (<i>false</i>). NOTE: If these properties are not enabled, PTZ functions do not work. This means that any widgets that use PTZ controls do not work.
Preferred Resolution	drop-down list, defaults to High	Specifies the pixel resolution of each transmitted frame. Options are: <i>High</i> , <i>Medium</i> , or <i>Low</i> . The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list, defaults to Low	Defines the speed of the video stream. Options are: <i>Low</i> , <i>Medium</i> , and <i>High</i> . You can configure each rate.
Preferred Compression	drop-down list, defaults to Medium	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <i>None</i> , <i>Low</i> , <i>Medium</i> , or <i>High</i>
Preferred Video Stream Fox	drop-down list, defaults to <i>Inherit</i>	For a network component, selects (<i>true</i>) or declines (<i>false</i>) the use of Fox streaming. For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level. <i>Inherit</i> sets this property to the value set for its parent component (the DVR, NVR or network component). <i>Yes</i> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network. NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station. <i>No</i> sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to <i>High</i> without impacting CPU usage. In essence, this removes the station from the equation. In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.
Credentials, Username and Password	text	Defines the credentials required by the system to connect the camera to the station.
Use Tcp Transport	true (default) or false	Transport Control Protocol (TCP) is selected by default.
Use Rtsp Stream	true or false (default)	Turns RTSP (Real Time Streaming Protocol) on and off. This popular protocol controls a camera using DVD-style controls (play, pause, etc.)

Property	Value	Description
Rtsp Username	text, defaults to root	Defines the username required by RTSP to control the camera.
Rtsp Password	text	Defines the password required by RTSP to control the camera.
Host Name	URL (in the following format): <ip-address>/axis-media/media.amp>	Defines the host, which is required by RTSP.
Web Client Http Port	number (defaults to 80)	Identifies the standard port (not secure) used to communicate the camera feed over the Internet. If using fox streaming to have the station render the video stream, this port should be different from the station's fox port. If you are not using fox streaming, this port should be the same as the station's fox port.
Web Client Https Port	number (defaults to 443)	Identifies the secure port used to communicate the camera feed over the Internet. If using fox streaming, which uses the station to render the video stream, this port should be different from the station's fox port. If you are not using fox streaming, this port should be the same as the station's fox port.
Token Over Https	true (default) or false	Defines the protocol to use when fetching the authentication token from the camera. This property applies only when authentication uses the token mechanism. true fetches the token from the camera using a secure connection (https) when a user logs in to the station. This is the preferred (and default) option. false fetches the token from the camera using a connection that is not secure (http).
Web Auth Scheme	drop-down list (defaults to Token Or Browser)	Selects an authentication scheme for verifying the authenticity of the camera. Token retrieves a small piece of code called a token from the camera, which the system uses with digest authentication to validate the camera as a video streaming server. Some cameras, such as Axis cameras, whose firmware version is below 7.10, do not support tokens. In this case, use Browser or Token Or Browser authentication. Browser pops up an authentication window for entering the camera's Username and Password. Once a user enters these credentials, they remain in the browser cache until cache is cleared. Token Or Browser attempts token authentication. If token authentication works, streaming video begins. If not, the browser pops up the window for entering the camera's credentials.

Axis Video Camera tab

This tab edits the discovered Axis video camera properties.

Figure 231 Axis Video Camera properties

The screenshot shows the 'Axis Video Camera' configuration page. The top navigation bar includes 'Home', 'Monitoring', 'Personnel', 'Reports', 'System Setup', and 'Threat Levels'. Below this, a secondary bar contains 'Schedules', 'User Management', 'Backups', 'Remote Devices', 'Access Setup', and 'Intrusion Setup'. The 'Remote Devices' tab is active, and the 'Axis Video Network' row is selected. The main content area is divided into two tabs: 'Axis Video Camera' (selected) and 'Events'. The 'Axis Video Camera' tab contains the following sections and fields:

- Status:** A text input field containing '{down,alarm,unackedAlar'.
- Enabled:** A dropdown menu set to 'true'.
- Fault Cause:** A greyed-out text input field.
- Health:** A text area displaying 'Fail [18-Dec-19 3:04 PM EST] No connection established or no response for ping request.'
- Alarm Source Info:** A text area with 'Alarm Source Info »'.
- Video Device Id:** A text area with 'Description Axis Video Camera,Url Address ###.###.###.###,Web Port 443 »'.
- Ptz Support:** A text area with '... »'.
- Control Timing:** A text area with 'Camera Control Timings »'.
- Video Preferences:** A text area with 'Video Source Preferences »'.
- Credentials:** Two text input fields for 'Username' and 'Password'.
- Preset Text:** Three icons (add, edit, delete) and a table with columns 'Ordinal' and 'Name'.
- Pan Tilt Zoom Settings:** A text area with 'Axis Video Pan Tilt Zoom Settings »'.
- Resolution Settings:** A text area with 'Axis Video Resolution Settings »'.
- High Compression Codec:** A dropdown menu set to 'Ffmpeg _ C O D E C _ I D _ M P E G 4'.
- Use Tcp Transport:** A dropdown menu set to 'true'.
- Use Rtsps Stream:** A dropdown menu set to 'false'.
- Rtsp Username:** A text input field containing 'root'.
- Rtsp Password:** A text input field containing '.....'.
- Host Name:** A text input field.
- Control Port:** A text input field containing '554'.
- Data Port:** A text input field containing '9000'.
- Web Client Http Port:** A text input field containing '80'.
- Web Client Https Port:** A text input field containing '443'.
- Token Over Https:** A dropdown menu set to 'true'.
- Web Auth Scheme:** A dropdown menu set to 'Token Or Browser'.

You access this tab from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Axis Video Network row in the table, clicking the **Cameras** tab, and double-clicking a camera row in the table.

Links

In addition to the **Save** and **Axis Video Network** links, the **Live View** link opens for viewing the real-time video stream.

Properties

In addition to the common **Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info** properties, these properties support the camera.

Property	Value	Description
Video Device Id	additional properties	Refer to Video Device ID, page 256 .
Ptz Support	additional properties	Turns Pan Tilt, Zoom, Focus, Iris, Move To Preset, and Store Preset features on (<code>true</code>), and off (<code>false</code>). Your camera may or may not support these features. For each feature the camera supports, select <code>true</code> . For unsupported features, select <code>false</code> . NOTE: If these properties are not enabled, PTZ functions do not work. This means that any widgets that use PTZ controls do not work.
Control Timing	hours, minutes and seconds	Configures intervals between actions and timeout values. These settings affect how long a camera continues to respond to control communications after a control message is received. The reason for these limits is to prevent a camera from being left in a state of continual movement or adjustment (iris, focus, or zoom) in case communication with the device is lost.
Video Preferences	additional properties	Refer to Video Preferences, page 256 .
Credentials, Username and Password	text	Identify the username and password required to access the station. The camera uses these credentials to connect to the station.
Preset Text	two properties with Add , Edit and Delete buttons	Defines a set of pre-defined camera instructions each as a pair that consists of an integer (ordinal) and text command for controlling the camera. What to enter here depends on the camera.
Pan Tilt Zoom Settings	additional properties	Configures the degrees of pan and tilt and the speed at which the camera zooms in and out. Values depend on the specific camera.
Resolution Settings	additional properties	High, Medium, Low
High Compression Codec	drop-down list (defaults to MPEG4)	Defines the compression codec to use.
Use Tcp Transport	<code>true</code> (default) or <code>false</code>	Transport Control Protocol (TCP) is selected by default.
Use Rtsp Stream	<code>true</code> or <code>false</code> (default)	Turns RTSP (Real Time Streaming Protocol) on and off. This protocol controls a camera using DVD-style controls (play, pause, etc.) CAUTION: RTSP does not support TLS secure communication. Using this protocol may open your video network to be hacked. <code>true</code> enables RSTP streaming. <code>false</code> enables HPS (Honeywell Progressive Streaming). Playback video always streams using HPS.
Rtsp Username	text	Defines the user name required by RTSP to control the camera.
Rtsp Password	text	Defines the password required by RTSP to control the camera.

Property	Value	Description
Host Name	URL <ip-address>/axis-media/media.amp>	
Control Port	number (defaults to 554)	Identifies the control port for RTSP streaming.
Data Port	number (defaults to 9000)	Identifies the port used to receive RTSP data. (Could be an open port.)
Web Client Http Port	number (defaults to 80)	Identifies the standard port (not secure) used to communicate the camera feed over the Internet. If using fox streaming to have the station render the video stream, this port should be different from the station's fox port. If you are not using fox streaming, this port should be the same as the station's fox port.
Web Client Https Port	number (defaults to 443)	Identifies the secure port used to communicate the camera feed over the Internet. If using fox streaming, which uses the station to render the video stream, this port should be different from the station's fox port. If you are not using fox streaming, this port should be the same as the station's fox port.
Token Over Https	true (default) or false	Defines the protocol to use when fetching the authentication token from the camera. This property applies only when authentication uses the token mechanism. true fetches the token from the camera using a secure connection (https) when a user logs in to the station. This is the preferred (and default) option. false fetches the token from the camera using a connection that is not secure (http).
Web Auth Scheme	drop-down list (defaults to Token Or Browser)	Selects an authentication scheme for verifying the authenticity of the camera. Token retrieves a small piece of code called a token from the camera, which the system uses with digest authentication to validate the camera as a video streaming server. Some cameras, such as Axis cameras, whose firmware version is below 7.10, do not support tokens. In this case, use Browser or Token Or Browser authentication. Browser pops up an authentication window for entering the camera's Username and Password. Once a user enters these credentials, they remain in the browser cache until cache is cleared. Token Or Browser attempts token authentication. If token authentication works, streaming video begins. If not, the browser pops up the window for entering the camera's credentials.

Video Device ID

Property	Value	Description
Description	text	Provides additional information, which could include the camera’s geographical location or other unique information.
Url Address	IP address in the format: ###.###.###.###	Defines the URL or IP address of the video device (camera or DVR).
Web port	number (defaults to 443)	<p>Defines the port, when using the web UI, over which to transmit the camera’s video signal. 443 supports only secure communication between the camera and the station.</p> <p>For a camera that does not support TLS secure communication, that is, if Use Rtsp Stream is <code>true</code> or if you are using the HTTP protocol (Use Tls is <code>false</code> and Use Rtsp Stream is <code>false</code>), change this property to 80.</p> <p>CAUTION: Be aware that the framework cannot prevent a flooding attack or other malicious activity if you choose to configure your application without secure communication.</p> <p>If using fox streaming, which uses the station to render the video stream, this port should be different from the station’s fox port. If you are not using fox streaming, this port should be the same as the station’s fox port.</p>

Video Preferences

Figure 232 Video Preferences properties



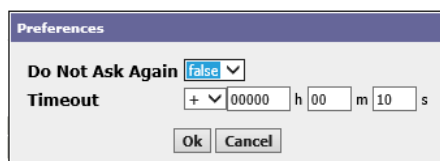
Property	Value	Description
Preferred Background Color	color chooser	Assigns a color, gradient, or image to open as the background of the widget.
Preferred Aspect Ratio	drop-down list (defaults to Standard Definition (1.33:1))	<p>Defines the ratio of the width to the height of the video frame. Options include <i>Inherit from camera</i> (default), <i>Standard Definition</i>, <i>Inherit from Stream</i>, <i>Fit to Screen</i>, etc.</p> <p>Resolution at the device or network may linked to the video stream options and inherited. In some cases, this may adversely affect the aspect ratio of your streaming video. If video images display distorted, try setting the camera’s Preferred Aspect Ratio to the <i>Standard Definition</i> option.</p>
Preferred Resolution	drop-down list (defaults to High)	Specifies the pixel resolution of each transmitted frame. Options are: <i>High</i> , <i>Medium</i> , or <i>Low</i> . The actual pixel values for these three relative settings are defined in the video device.

Property	Value	Description
Preferred Frame Rate	drop-down list (defaults to <code>Low</code>)	Defines the speed of the video stream. Options are: <code>Low</code> , <code>Medium</code> , and <code>High</code> . You can configure each rate.
Preferred Compression	drop-down list (defaults to <code>Medium</code>)	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <code>None</code> , <code>Low</code> , <code>Medium</code> , or <code>High</code> .
Preferred Video Stream Fox	drop-down list (defaults to <code>Inherit</code>)	<p>For a network component, selects (<code>true</code>) or declines (<code>false</code>) the use of Fox streaming.</p> <p>For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level.</p> <p><code>Inherit</code> sets this property to the value set for its parent component (the DVR, NVR or network component).</p> <p><code>Yes</code> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.</p> <p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p><code>No</code> sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to <code>High</code> without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Timestamp Preferred	<code>true</code> (default) or <code>false</code>	Configures the camera to record and display (<code>true</code>) a timestamp on the video.
Interframe Timeout	hours, minutes, seconds	Defines the maximum amount of time permitted to elapse between frames. A video stream that takes longer than this amount of time to retrieve a video frame needs to be re-established.

Axis camera Preferences window

This window configures common properties associated with an Axis video camera.

Figure 233 Axis Video Camera Preferences window



This window opens from the main menu when you click **Controller (System) Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Axis Video Network row in the table, clicking the **Cameras** tab, and clicking the Preferences button (🔧).

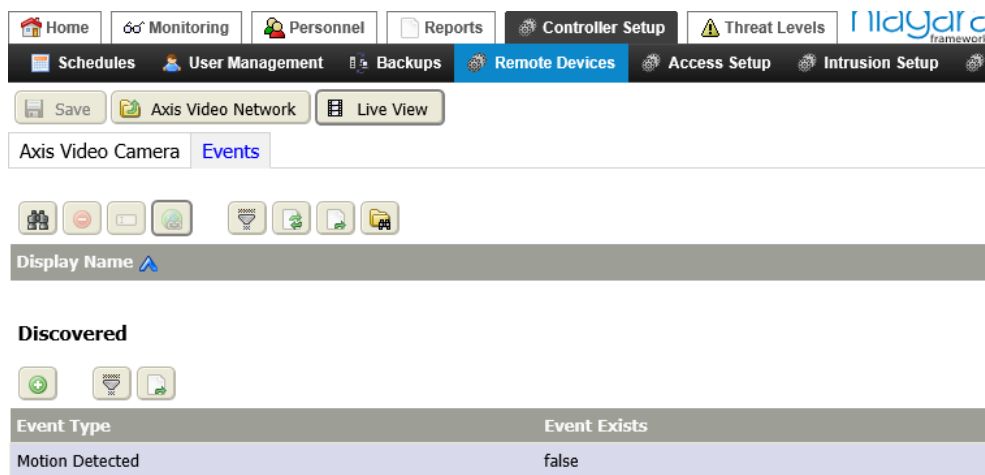
Properties

Property	Value	Description
Do Not Ask Again	true or false (default)	The false option allows for setting a timeout value. The true option inhibits the Discovery window from opening again before the system initiates the discovery search.
Timeout	hours, minutes, seconds	The maximum amount of time that discovery will attempt to find a camera on the network before reverting to a "timeout" state.

Axis Events tab

This view discovers events detected by the Axis camera.

Figure 234 Axis Camera Events view



You access this tab from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the **Axis Video Network** row in the table, clicking the **Cameras** tab, double-clicking a camera row in the table, and clicking the **Events** tab.

Links

In addition to the standard **Save** and **Axis Video Network** links, this view provides a link to view the camera feed live (**Live View**).

Buttons

Standard buttons are available in this view. These include Discover, Delete, Rename Filter, Refresh, Export and Learn Mode. These buttons support camera events.

- Hyperlink opens the Configuration tab for the event. Using this tab you can edit event facets, access event proxy extension properties and check event status.
- Add moves the event to the Database table from where clicking **Save** writes the event record to the station database.

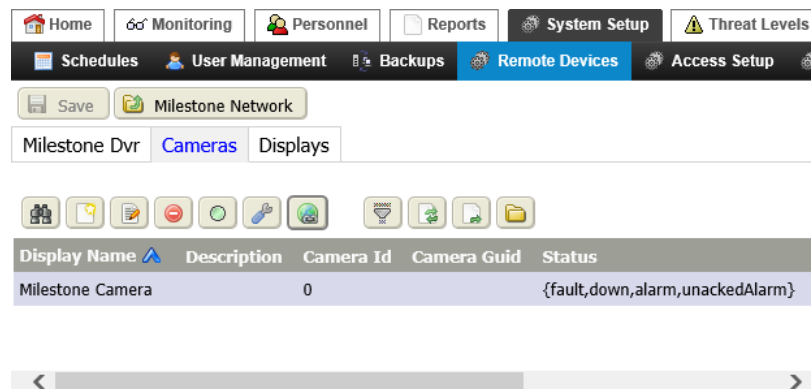
Columns

Column	Description
Display Name	Reports the name of the camera/
Event Type	Reports what caused the system to register an event.
Event Exists	On discovering events, this property reports if the condition currently exists (<code>true</code>) or not (<code>false</code>) in the database. For example, if a "Motion Detected" Event has been added to database previously, then discovery shows that the Event exists already (<code>true</code>).

Milestone Cameras tab

This tab and view manages the cameras connected to the Milestone DVR.







Figure 235 Cameras tab



You access this tab from the main menu by clicking **Controller (System) Setup→Remote Devices→Remote Drivers**, double-clicking the Milestone Network, clicking the DVRs tab, double-clicking a row in the DVR Manager table, followed by clicking the **Cameras** tab.

Buttons

In addition to the standard buttons (Discover, Delete, Filter, Refresh and Export), these buttons support Milestone cameras.

-  New opens the **New** window for adding a Milestone camera.
-  Edit opens the component's Edit window.
-  or  Ping (or wink) sends a command to the remote device or server.
-  Configure opens a properties window.
-  Hyperlink opens the DVR view at the **Milestone Camera** tab.

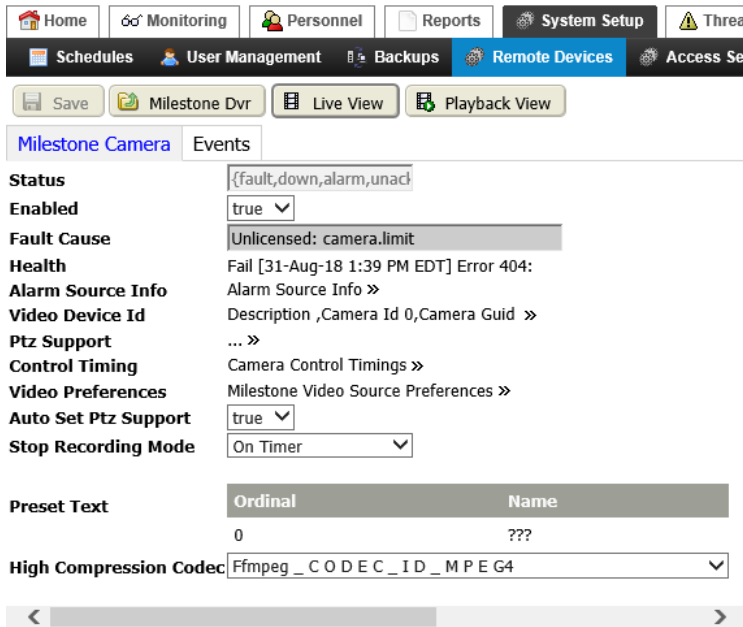
Columns

Column	Description
Display Name	Displays the name given to this camera when the database record was created.
Description	Displays additional information about the camera, such as its location, etc.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}

Milestone Camera tab

This view manages one or more Milestone cameras.

Figure 236 Milestone Camera tab



You access this tab from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Milestone Network row in the table, clicking the **Cameras** tab, and double-clicking a Milestone camera row in the table.

Links

In addition to the Milestone Dvr link, which returns to the Milestone table view, this tab provides these links.

- **Live View** opens the real-time camera feed.
- **Playback View** opens a view from which you can play back pre-recorded video clips.

Properties

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support Milestone cameras.

Property	Value	Description
Video Device Id	additional properties	Refer to Video Device Id, page 261 .
Ptz Support	additional properties	Turns Pan Tilt, Zoom, Focus, Iris, Move To Preset, and Store Preset features on (<i>true</i>), and off (<i>false</i>). Your camera may or may not support these features. For each feature the camera supports, select <i>true</i> . For unsupported features, select <i>false</i> . NOTE: If these properties are not enabled, PTZ functions do not work. This means that any widgets that use PTZ controls do not work.
Control Timing	hours, minutes and seconds	Configures intervals between actions and timeout values. These settings affect how long a camera continues to respond to control communications after a control message is received.

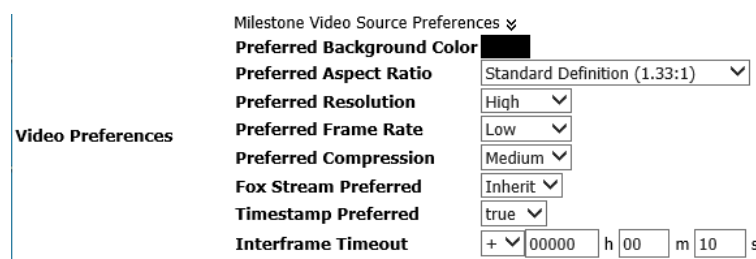
Property	Value	Description
		The reason for these limits is to prevent a camera from being left in a state of continual movement or adjustment (iris, focus, or zoom) in case communication with the device is lost.
Video Preferences	additional properties	Refer to Video Preferences, page 256 .
Auto Set Ptz Support	true or false	Turns the automatic configuration of the Ptz properties on true and off false.
Stop Recording Mode	drop-down list	Indicates when to stop recording.
Preset Text	two properties with Add , Edit and Delete buttons	Defines a set of pre-defined camera instructions each as a pair that consists of an integer (ordinal) and text command for controlling the camera. What to enter here depends on the camera.
High Compression CODEC	drop-down list	Defines the type of video compression to use.

Video Device Id

Property	Value	Description
Description	text	Provides additional information, which could include the camera’s geographical location or other unique information.
Camera Id	number	Identifies the specific camera.
Camera Guid	32–digit hexadecimal number	Identifies the camera’s globally unique identifier (a 32–hexadecimal digit that identifies the camera).

Video Preferences

Figure 237 Video Preferences properties



Property	Value	Description
Preferred Background Color	color chooser (defaults to black)	Opens the color chooser. The color you select affects the border or margin area around the video display.
Preferred Aspect Ratio	drop-down list (defaults to Standard Definition (1.33:1))	Defines the ratio of the width to the height of the video frame. Options include <i>Inherit from camera (default)</i> , <i>Standard Definition</i> , <i>Inherit from Stream</i> , <i>Fit to Screen</i> , etc. Resolution at the device or network may linked to the video stream options and inherited. In some cases, this may adversely affect the aspect ratio of your streaming video. If video

Property	Value	Description
		images display distorted, try setting the camera's Preferred Aspect Ratio to the <code>Standard Definition</code> option.
Preferred Resolution	drop-down list (defaults to <code>High</code>)	Specifies the pixel resolution of each transmitted frame. Options are: <code>High</code> , <code>Medium</code> , or <code>Low</code> . The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list (defaults to <code>Low</code>)	Defines the speed of the video stream. Options are: <code>Low</code> , <code>Medium</code> , and <code>High</code> . You can configure each rate.
Preferred Compression	drop-down list (defaults to <code>Medium</code>)	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <code>None</code> , <code>Low</code> , <code>Medium</code> , or <code>High</code>
Preferred Video Stream Fox	drop-down list (defaults to <code>Inherit</code>)	<p>For a network component, selects (<code>true</code>) or declines (<code>false</code>) the use of Fox streaming.</p> <p>For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level.</p> <p><code>Inherit</code> sets this property to the value set for its parent component (the DVR, NVR or network component).</p> <p><code>Yes</code> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.</p> <p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p><code>No</code> sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to <code>High</code> without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Timestamp Preferred	<code>true</code> or <code>false</code> (defaults to <code>true</code>)	Configures the camera to record and display (<code>true</code>) a timestamp on the video.
Interframe Timeout	hours, minutes, seconds	Defines the maximum amount of time permitted to elapse between frames. A video stream that takes longer than this amount of time to retrieve a video frame needs to be re-established.

Milestone New camera window

This window creates and edits camera records in the database.

Figure 238 New Milestone camera window

Properties

In addition to the common **Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info** properties, these properties support the Milestone DVR camera.

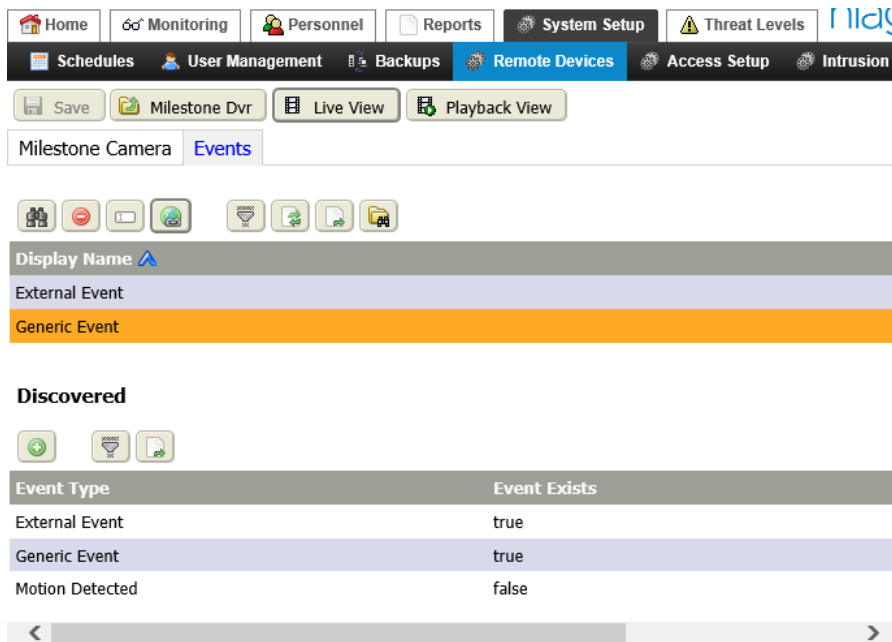
Property	Value	Description
Video Device Id, Description	text	Defines a text string to identify the camera.
Video Device Id, Camera Id	number between 0 and 99	Defines a unique camera identity number.
Camera Guid	number	Defines a number to identify the camera.
Ptz Support	additional properties	Turns Pan Tilt, Zoom, Focus, Iris, Move To Preset, and Store Preset features on (<code>true</code>), and off (<code>false</code>). Your camera may or may not support these features. For each feature the camera supports, select <code>true</code> . For unsupported features, select <code>false</code> . NOTE: If these properties are not enabled, PTZ functions do not work. This means that any widgets that use PTZ controls do not work.
Control Timing	hours, minutes, and seconds	Configures intervals between actions and timeout values. These settings affect how long a camera continues to respond to control communications after a control message is received. The reason for these limits is to prevent a camera from being left in a state of continual movement or adjustment (iris, focus, or zoom) in case communication with the device is lost.
Preferred Resolution	drop-down list, defaults to <code>High</code>	Specifies the pixel resolution of each transmitted frame. Options are: <code>High</code> , <code>Medium</code> , or <code>Low</code> . The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list, defaults to <code>Low</code>	Defines the speed of the video stream. Options are: <code>Lo Frame Rate</code> , <code>Med Frame Rate</code> , and <code>Hi Frame Rate</code> . You can configure each rate.

Property	Value	Description
Preferred Compression	drop-down list, defaults to <code>Medium</code>	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <code>None</code> , <code>Low</code> , <code>Medium</code> , or <code>High</code>
Fox Stream Preferred	drop-down list, defaults to <code>Inherit</code>	<p>Selects or declines the use of Fox streaming.</p> <p><code>inherit</code> sets this property to the value set for its parent component (the DVR or network component).</p> <p><code>yes</code> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.</p> <p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p><code>false</code> sends the video stream directly from the video camera to the Workbench interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to <code>High</code> without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In either case, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Auto Set Ptz Support	<code>true</code> (default) or <code>false</code>	Turns the automatic configuration of the Ptz properties on <code>true</code> and off <code>false</code> .
Stop Recording Mode	Drop-down list (defaults to <code>On Timer</code>)	Indicates when to stop recording. <code>On Timer</code> <code>On Alarm to Normal</code>


Milestone Events tab

This tab discovers events and adds them to the database.

Figure 239 Events tab



Buttons

In addition to the standard buttons (Discover, Delete, Rename, Filter, Refresh, Export and Learn Mode), the Hyperlink button () opens the **Edit Points** view.

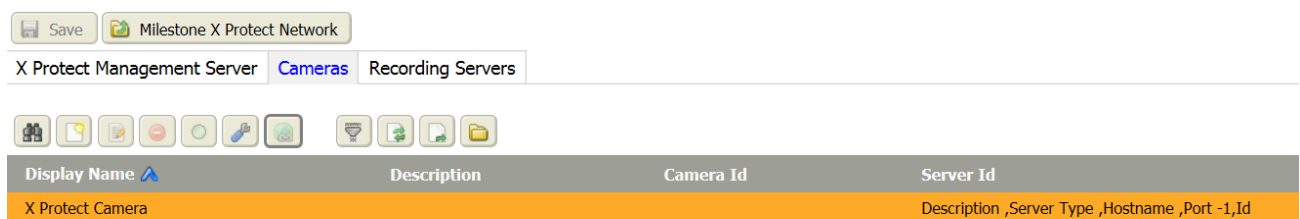
Columns

Column	Description
Event Type	Identifies the source of the event. External Event Generic Event Motion Detected indicates that motion has been detected: true or false.
Event Exists	Indicates if this event has occurred (true).

X Protect Cameras tab







This tab lists the X Protect cameras on the network.

Figure 240 X Protect Cameras tab



Buttons

In addition to the standard buttons (Discover, Edit, Delete, Filter, Refresh, and Export), these buttons support X Protect cameras.

-  New opens the **New** window for adding a Milestone camera.
-  Edit opens the component’s Edit window.
-  or  Ping (or wink) sends a command to the remote device or server.
-  Configure opens a properties window.
-  Hyperlink opens the DVR view at the **Milestone Camera** tab.

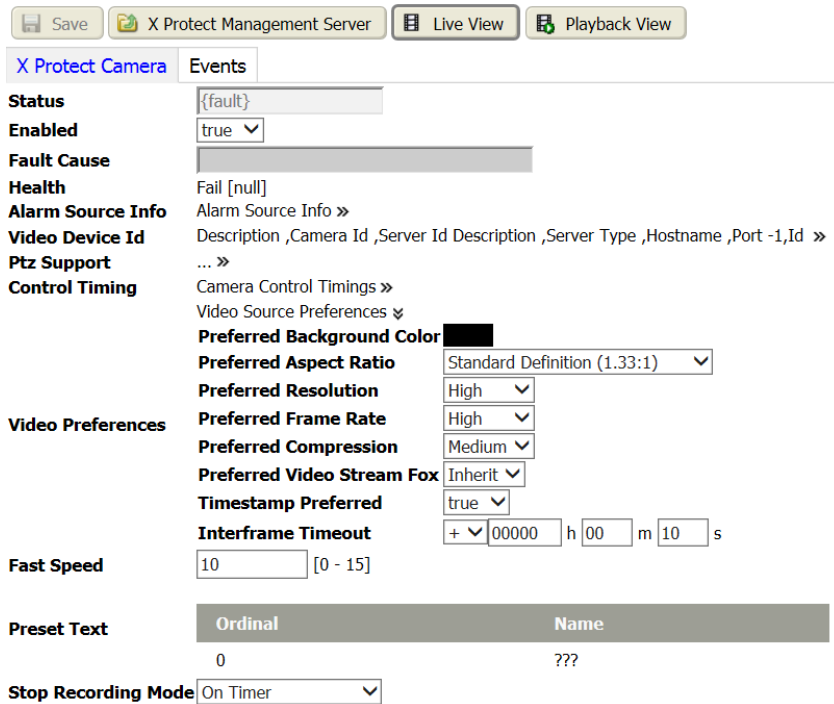
Columns

Column	Description
Display Name	Displays the name given to this camera when the database record was created.
Description	Displays additional information about the camera, such as its location, etc.
Camera ID	Identifies the camera.
Server ID	Identifies the server.

X Protect Camera tab

This tab configures X Protect camera properties.

Figure 241 X Protect Camera tab



The screenshot shows the configuration interface for an X Protect camera. At the top, there are buttons for 'Save', 'X Protect Management Server', 'Live View', and 'Playback View'. Below these are tabs for 'X Protect Camera' and 'Events'. The main configuration area is divided into several sections:

- Status:** A dropdown menu showing '{fault}'.
- Enabled:** A dropdown menu set to 'true'.
- Fault Cause:** A greyed-out field.
- Health:** A dropdown menu set to 'Fail [null]'.
- Alarm Source Info:** A dropdown menu set to 'Alarm Source Info »'.
- Video Device ID:** A dropdown menu set to 'Description ,Camera Id ,Server Id Description ,Server Type ,Hostname ,Port -1,Id »'.
- Ptz Support:** A dropdown menu set to '... »'.
- Control Timing:** A dropdown menu set to 'Camera Control Timings »'.
- Video Source Preferences:** A dropdown menu set to 'Video Source Preferences ▾'.
- Preferred Background Color:** A color selection box.
- Preferred Aspect Ratio:** A dropdown menu set to 'Standard Definition (1.33:1)'.
- Preferred Resolution:** A dropdown menu set to 'High'.
- Preferred Frame Rate:** A dropdown menu set to 'High'.
- Preferred Compression:** A dropdown menu set to 'Medium'.
- Preferred Video Stream Fox:** A dropdown menu set to 'Inherit'.
- Timestamp Preferred:** A dropdown menu set to 'true'.
- Interframe Timeout:** A field set to '+ 00000 h 00 m 10 s'.
- Fast Speed:** A field set to '10' with a range of '[0 - 15]'.
- Preset Text:** A table with two columns: 'Ordinal' and 'Name'. The first row shows '0' and '???'.
- Stop Recording Mode:** A dropdown menu set to 'On Timer'.

You access this tab from the main menu by clicking **Controller Setup→Remote Devices→Remote Drivers** followed by double-clicking the X Protect Network row in the table, clicking the **Cameras** tab, and double-clicking an X Protect camera row in the table.

Links

In addition to the Milestone Dvr link, which returns to the Milestone table view, this tab provides these links.

- **Live View** opens the real-time camera feed.
- **Playback View** opens a view from which you can play back pre-recorded video clips.

Properties

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support Milestone X Protect cameras.

Property	Value	Description
Video Device Id	additional properties	Refer to Video Device Id, Server Id properties, page 267 .
Ptz Support	additional properties	Turns Pan Tilt, Zoom, Focus, Iris, Move To Preset, and Store Preset features on (<code>true</code>), and off (<code>false</code>). Your camera may or may not support these features. For each feature the camera supports, select <code>true</code> . For unsupported features, select <code>false</code> . NOTE: If these properties are not enabled, PTZ functions do not work. This means that any widgets that use PTZ controls do not work.
Control Timing	hours, minutes and seconds	Configures intervals between actions and timeout values. These settings affect how long a camera continues to respond to control communications after a control message is received. The reason for these limits is to prevent a camera from being left in a state of continual movement or adjustment (iris, focus, or zoom) in case communication with the device is lost.
Video Preferences	additional properties	Refer to Video Preferences, page 268 .
Auto Set Ptz Support	<code>true</code> or <code>false</code>	Turns the automatic configuration of the Ptz properties on <code>true</code> and off <code>false</code> .
Fast Speed	number between zero (0) and 15 (defaults to 10)	Defines the speed of a quick pan or tilt.
Preset Text	two properties with Add , Edit and Delete buttons	Defines a set of pre-defined camera instructions each as a pair that consists of an integer (ordinal) and text command for controlling the camera. What to enter here depends on the camera.
Stop Recording Mode	drop-down list	Indicates when to stop recording.

Video Device Id, Server Id properties

Figure 242 Video Device ID and Server Id properties

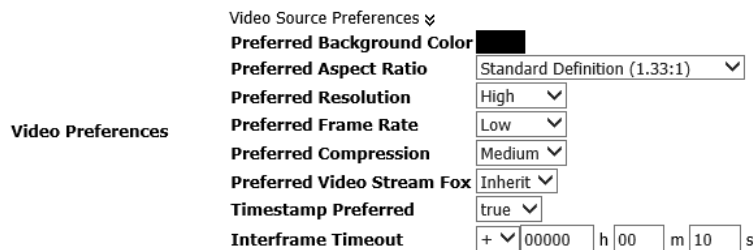
Video Device Id	Description	<input type="text"/>
	Server Type	XPCORS
Server Id	Hostname	desktop-9gju3iv
	Port	7563
	Id	ccaac8da-6c02-4f8d-b838-b11e5300b33e

Most of these properties are read-only because it is not possible to create a recording server manually. Instead, the framework discovers recording servers.

Property	Value	Description
Description	text	Provides additional information, which could include the camera's geographical location or other unique information.
Camera Id	number	Identifies the specific camera.
Server Id, Description	additional properties	Allows you to enter text to describe the discovered recording server.
Server Id, Server Type	read-only	Identifies the type of the discovered recording server.
Server Id, Hostname	read-only	Reports the host name of the discovered recording server.
Server Id, Port	read-only	Identifies the port used by the discovered recording server.
Server Id, Id	read-only	Identifies the unique identifier assigned in the Milestone server to the DVR.

Video Preferences

Figure 243 Video Preferences properties



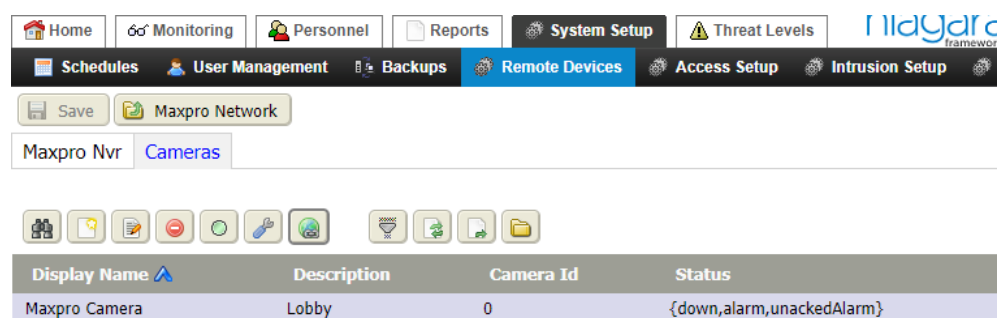
Property	Value	Description
Preferred Background Color	color chooser (defaults to black)	Opens the color chooser. The color you select affects the border or margin area around the video display.
Preferred Aspect Ratio	drop-down list (defaults to Standard Definition (1.33:1))	Defines the ratio of the width to the height of the video frame. Options include Inherit from camera (default), Standard Definition, Inherit from Stream, Fit to Screen, etc. Resolution at the device or network may be linked to the video stream options and inherited. In some cases, this may adversely affect the aspect ratio of your streaming video. If video images display distorted, try setting the camera's Preferred Aspect Ratio to the Standard Definition option.
Preferred Resolution	drop-down list (defaults to High)	Specifies the pixel resolution of each transmitted frame. Options are: High, Medium, or Low. The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list (defaults to Low)	Defines the speed of the video stream. Options are: Low, Medium, and High. You can configure each rate.
Preferred Compression	drop-down list (defaults to Medium)	Specifies what level of compression is used during live video streaming. The actual compression values for these relative

Property	Value	Description
		settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <code>None</code> , <code>Low</code> , <code>Medium</code> , or <code>High</code>
Preferred Video Stream Fox	drop-down list (defaults to <code>Inherit</code>)	<p>For a network component, selects (<code>true</code>) or declines (<code>false</code>) the use of Fox streaming.</p> <p>For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level.</p> <p><code>Inherit</code> sets this property to the value set for its parent component (the DVR, NVR or network component).</p> <p><code>Yes</code> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.</p> <p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p><code>No</code> sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to <code>High</code> without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Timestamp Preferred	<code>true</code> or <code>false</code> (defaults to <code>true</code>)	Configures the camera to record and display (<code>true</code>) a timestamp on the video.
Interframe Timeout	hours, minutes, seconds	Defines the maximum amount of time permitted to elapse between frames. A video stream that takes longer than this amount of time to retrieve a video frame needs to be re-established.

Maxpro Cameras tab

This tab and view manages the cameras connected to the Maxpro NVR.







Figure 244 Cameras tab



You access this tab from the main menu by clicking **Controller (System) Setup**→**Remote Devices**→**Remote Drivers**, double-clicking the Maxpro Network, clicking the NVRs tab, double-clicking a row in the NVR Manager table, followed by clicking the **Cameras** tab.

Buttons

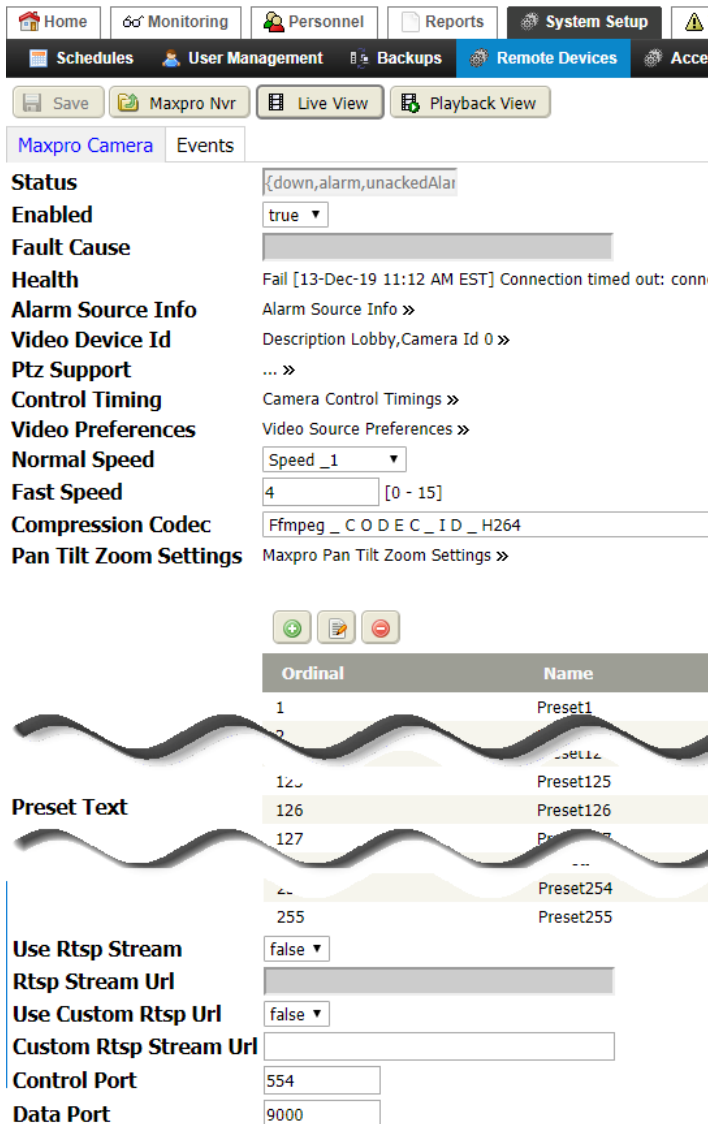
In addition to the standard buttons (Discover, Delete, Filter, Refresh and Export), these buttons support Maxpro cameras.

-  New opens the **New** window for adding a Maxpro camera.
-  Edit opens the component’s Edit window.
-  or  Ping (or wink) sends a command to the remote device or server.
-  Preferences opens a **Preferences** window, which is documented in a separate topic.
-  Hyperlink opens the **Maxpro Camera** tab, which is documented in a separate topic.

Maxpro Camera tab

This view manages one or more Maxpro cameras.

Figure 245 Maxpro Camera tab



The screenshot displays the Maxpro Camera configuration interface. At the top, there is a navigation bar with tabs for Home, Monitoring, Personnel, Reports, System Setup, and Alerts. Under System Setup, there are sub-tabs for Schedules, User Management, Backups, Remote Devices, and Access. Below the navigation are buttons for Save, Maxpro Nvr, Live View, and Playback View. The main content area is split into two sections: Maxpro Camera and Events. The Maxpro Camera section includes the following fields:

- Status:** {down,alarm,unackedAlar
- Enabled:** true
- Fault Cause:** [Redacted]
- Health:** Fail [13-Dec-19 11:12 AM EST] Connection timed out: conn
- Alarm Source Info:** Alarm Source Info »
- Video Device Id:** Description Lobby,Camera Id 0 »
- Ptz Support:** ... »
- Control Timing:** Camera Control Timings »
- Video Preferences:** Video Source Preferences »
- Normal Speed:** Speed_1
- Fast Speed:** 4 [0 - 15]
- Compression Codec:** Ffmpeg_C O D E C_ I D _ H264
- Pan Tilt Zoom Settings:** Maxpro Pan Tilt Zoom Settings »

The Events section contains a table with the following data:

Ordinal	Name
1	Preset1
2	Preset2
125	Preset125
126	Preset126
127	Preset127
...	...
254	Preset254
255	Preset255

Below the table are the following fields:

- Use Rtsp Stream:** false
- Rtsp Stream Url:** [Redacted]
- Use Custom Rtsp Url:** false
- Custom Rtsp Stream Url:** [Redacted]
- Control Port:** 554
- Data Port:** 9000

You access this tab from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Maxpro Network row in the table, clicking the **Cameras** tab, and double-clicking a Maxpro camera row in the table.

Links

In addition to the Maxpro Nvr link, which returns to the Maxpro table view, this tab provides these links.

- **Live View** opens the real-time camera feed.
- **Playback View** opens a view from which you can play back pre-recorded video clips.

Properties

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support Maxpro cameras.

Property	Value	Description
Video Device Id	additional properties	Refer to Video Device Id, page 272 .
Ptz Support	additional properties	Turns Pan Tilt, Zoom, Focus, Iris, Move To Preset, and Store Preset features on (<code>true</code>), and off (<code>false</code>). Your camera may or may not support these features. For each feature the camera supports, select <code>true</code> . For unsupported features, select <code>false</code> . NOTE: If these properties are not enabled, PTZ functions do not work. This means that any widgets that use PTZ controls do not work.
Control Timing	hours, minutes and seconds	Configures intervals between actions and timeout values. These settings affect how long a camera continues to respond to control communications after a control message is received. The reason for these limits is to prevent a camera from being left in a state of continual movement or adjustment (iris, focus, or zoom) in case communication with the device is lost.
Video Preferences	additional properties	Refer to Video Preferences, page 272 .
Normal Speed	<code>true</code> or <code>false</code>	Turns the automatic configuration of the Ptz properties on <code>true</code> and off <code>false</code> .
Fast Speed	drop-down list	Defines the speed of a quick pan or tilt.
Compression CODEC	drop-down list	Defines the type of video compression to use.
Pan Tilt Zoom Settings	additional properties	Configures the degrees of pan and tilt and the speed at which the camera zooms in and out. Values depend on the specific camera.
Preset Text	two properties with Add , Edit and Delete buttons	Defines a set of pre-defined camera instructions each as a pair that consists of an integer (ordinal) and text command for controlling the camera. What to enter here depends on the camera.
Use Rtsp Stream	<code>true</code> or <code>false</code> (default)	Turns RTSP (Real Time Streaming Protocol) on and off. This protocol controls a camera using DVD-style controls (play, pause, etc.)

Property	Value	Description
		<p>CAUTION: RTSP does not support TLS secure communication. Using this protocol may open your video network to be hacked.</p> <p><code>true</code> enables RSTP streaming.</p> <p><code>false</code> enables HPS (Honeywell Progressive Streaming). Playback video always streams using HPS.</p>
Use Custom Rtsp Url	text	Defines the user name required by RTSP to control the camera.
Custom Rtsp Stream Url	text	
Control Port	number (defaults to 554)	Defines the RTSP port.
Data Port	number (defaults to 9000)	Defines the data port.

Video Device Id

Property	Value	Description
Description	text	Provides additional information, which could include the camera's geographical location or other unique information.
Camera Id	number	Identifies the specific camera.

Video Preferences

Figure 246 Video Preferences properties

Video Preferences

- Preferred Background Color [Color Chooser]
- Preferred Aspect Ratio Standard Definition (1.33:1) ▾
- Preferred Resolution High ▾
- Preferred Frame Rate Low ▾
- Preferred Compression Medium ▾
- Preferred Video Stream Fox Inherit ▾
- Timestamp Preferred true ▾
- Interframe Timeout + ▾ 00000 h 00 m 10 s

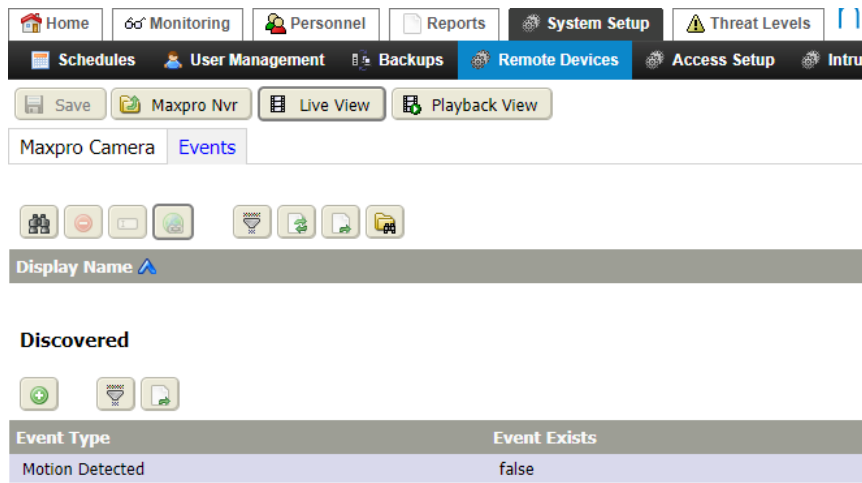
Property	Value	Description
Preferred Background Color	color chooser (defaults to black)	Opens the color chooser. The color you select affects the border or margin area around the video display.
Preferred Aspect Ratio	drop-down list (defaults to Standard Definition (1.33:1))	<p>Defines the ratio of the width to the height of the video frame. Options include Inherit from camera (default), Standard Definition, Inherit from Stream, Fit to Screen, etc.</p> <p>Resolution at the device or network may linked to the video stream options and inherited. In some cases, this may adversely affect the aspect ratio of your streaming video. If video images display distorted, try setting the camera's Preferred Aspect Ratio to the Standard Definition option.</p>

Property	Value	Description
Preferred Resolution	drop-down list (defaults to <code>High</code>)	Specifies the pixel resolution of each transmitted frame. Options are: <code>High</code> , <code>Medium</code> , or <code>Low</code> . The actual pixel values for these three relative settings are defined in the video device.
Preferred Frame Rate	drop-down list (defaults to <code>Low</code>)	Defines the speed of the video stream. Options are: <code>Low</code> , <code>Medium</code> , and <code>High</code> . You can configure each rate.
Preferred Compression	drop-down list (defaults to <code>Medium</code>)	Specifies what level of compression is used during live video streaming. The actual compression values for these relative settings are defined in the video device. Higher compression uses less bandwidth but negatively affects image quality. Options are: <code>None</code> , <code>Low</code> , <code>Medium</code> , or <code>High</code> .
Preferred Video Stream Fox	drop-down list (defaults to <code>Inherit</code>)	<p>For a network component, selects (<code>true</code>) or declines (<code>false</code>) the use of Fox streaming.</p> <p>For a child component (DVR, NVR or camera) selects or declines the use of Fox streaming at the child component level.</p> <p><code>Inherit</code> sets this property to the value set for its parent component (the DVR, NVR or network component).</p> <p><code>Yes</code> sends the video stream from the video camera to the station (controller) and then forwards it to the Workbench interface through the standard Fox/Foxs connection. This overcomes fire wall issues in the event that the video surveillance system is not exposed to the outside world on its network.</p> <p>NOTE: This option assumes that the controller is exposed - otherwise you could not even connect to the station.</p> <p><code>No</code> sends the video stream directly from the video camera to the interface. Using this setting allows you to set the Preferred Resolution and Frame Rate to <code>High</code> without impacting CPU usage. In essence, this removes the station from the equation.</p> <p>In all cases, the client-side computer expends some of its CPU utilization to render the video on the screen.</p>
Timestamp Preferred	<code>true</code> or <code>false</code> (defaults to <code>true</code>)	Configures the camera to record and display (<code>true</code>) a timestamp on the video.
Interframe Timeout	hours, minutes, seconds	Defines the maximum amount of time permitted to elapse between frames. A video stream that takes longer than this amount of time to retrieve a video frame needs to be re-established.


Maxpro Events tab

This tab discovers events and adds them to the database.

Figure 247 Events tab



Buttons

In addition to the standard buttons (Discover, Delete, Rename, Filter, Refresh, Export and Learn Mode), the Hyperlink button () opens the **Edit Points** view.

Columns

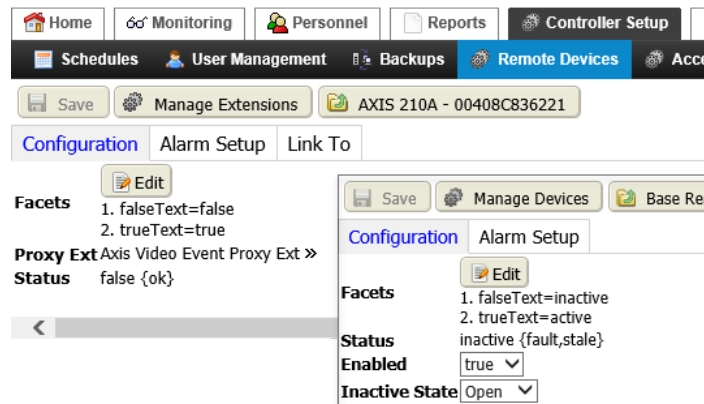
Column	Description
Event Type	Identifies the source of the event. External Event Generic Event Motion Detected indicates that motion has been detected: true or false.
Event Exists	Indicates if this event has occurred (true).

Edit Point view, Configuration tab

This view configures individual points. These can be module points or camera event points. You use this view to set up alarms for the event and to configure histories. You can also provide links from an event to other available Boolean-writable points.

NOTE: This description covers both reader and input/output points. Differences are noted where appropriate.

Figure 248 Edit Point (input view) for a remote module



The point's display name appears at the top of the view. The screen captures show two flavors of this view. The one with three tabs opens when you edit a camera event point. The one with two tabs opens when you edit a remote module point.

There are several ways to access the views that edit points. For example:

- To access camera points, you click **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Axis Video Network row in the table, click the **Cameras** tab, double-click a camera row in the table, click the **Events** tab, discover events, and double-click an event row.
- To access module points you click **Controller Setup**→**Remote Devices**→**Remote Modules**→**Remote Module Setup**, double-click the module row in the table, click the **Additional Points** tab, and click a link to a point.

Module point links

- The **Manage Devices** link opens the **Manage Devices** window.
- The **Base Reader Module** link opens the Base Reader Module properties.

Camera event point links

- The **Manage Extensions** link opens the **Manage Point Extensions** window.
- The camera configuration view opens the camera tab.

Remote module point properties

In addition to **Status** and **Enabled**, these properties support the configuration of points.

Property	Value	Description
Edit button and Facets	button and additional properties	Determine how values are formatted for display depending on the context and the type of data. For example, instead of the Boolean facets <code>trueText</code> and <code>falseText</code> you may want to display ON and OFF , Access Granted and Access Denied or Locked and Unlocked . You access facets by clicking an Edit button or a chevron >> . Both open an Edit Facets window.
Inactive State	Open and Closed	Defines the normally inactive state of the digital input or relay output as either <code>Open</code> or <code>Closed</code> , depending on the device requirements.

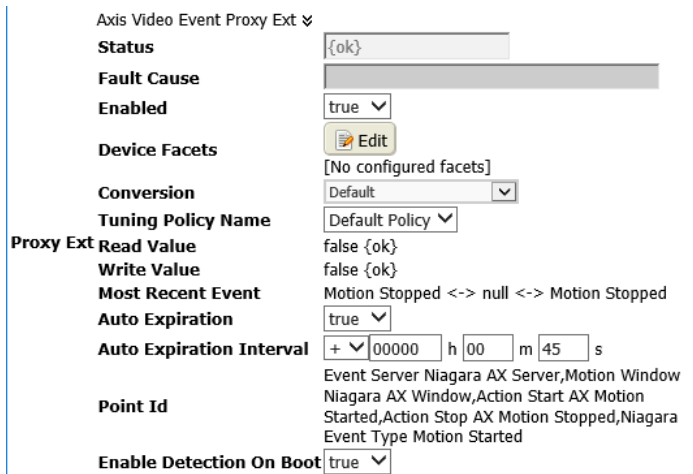
Camera event point properties

In addition to **Status**, these properties support camera event points.

Properties	Value	Description
Facets	Edit button	Opens a window for configuring the text that appears when a camera event occurs.
Proxy Ext	additional properties	Expands to display proxy extension properties, which apply to camera events. Refer to Proxy Extension properties, page 276 .

Proxy Extension properties

Figure 249 Proxy Ext properties



In addition to the standard properties (**Status**, **Fault Cause**, and **Enabled**), these properties support camera events.

Property	Value	Description
Device Facets	additional properties	Determine how values are formatted for display depending on the context and the type of data. For example, instead of the Boolean facets <code>trueText</code> and <code>falseText</code> you may want to display ON and OFF , Access Granted and Access Denied or Locked and Unlocked . You access facets by clicking an Edit button or a chevron >> . Both open an Edit Facets window.
Conversion	drop-down list, defaults to <code>Default</code>	Defines how the system converts proxy extension units to parent point units. <code>Default</code> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point. NOTE: In most cases, the standard <code>Default</code> conversion is best. <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. <code>Linear With Unit</code> is an extension to the existing linear conversion property. This specifies whether the unit conversion

Property	Value	Description
		<p>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> .	Identifies the assigned tuning policy. During polling, the system uses such collections of rules to evaluate both write requests and the acceptability (freshness) of read requests.
Read Value	read-only	Reports the last value read using device facets.
Write Value	read-only	Reports the last value written using device facets. Applies only to writable points.
Most Recent Event	read-only	Indicates the most recent “motion start” or “motion stopped” event.
Auto Expiration	<code>true</code> (default) or <code>false</code>	Turns this feature on and off.
Auto Expiration Interval	+ or — hours, minutes, seconds (defaults to 45 seconds).	Configures when the event is no longer valid.
Point Id	read-only	Identifies the point.
Enable Detection On Boot	<code>true</code> (default) or <code>false</code>	Configures the system to enable detection of this point when the station starts.

Inputs

A digital input (DI) is a device that monitors the state of electronic contacts.

- Door sensors are contact devices that monitor the state of a door.
- Exit requests are devices that provide access to leave through a door without having to present a badge.

- ADA (Americans with Disabilities Act) Controls could be used with power assisted doors that open automatically. Typically, this control is configured similarly to an Exit Request if it is inside the building. If the control is on the outside of a facility it can be configured to open the door only when the door is unlocked (after a validation or during a scheduled unlock period).
- Other inputs can be devices that detect such things as glass break or motion sensors.

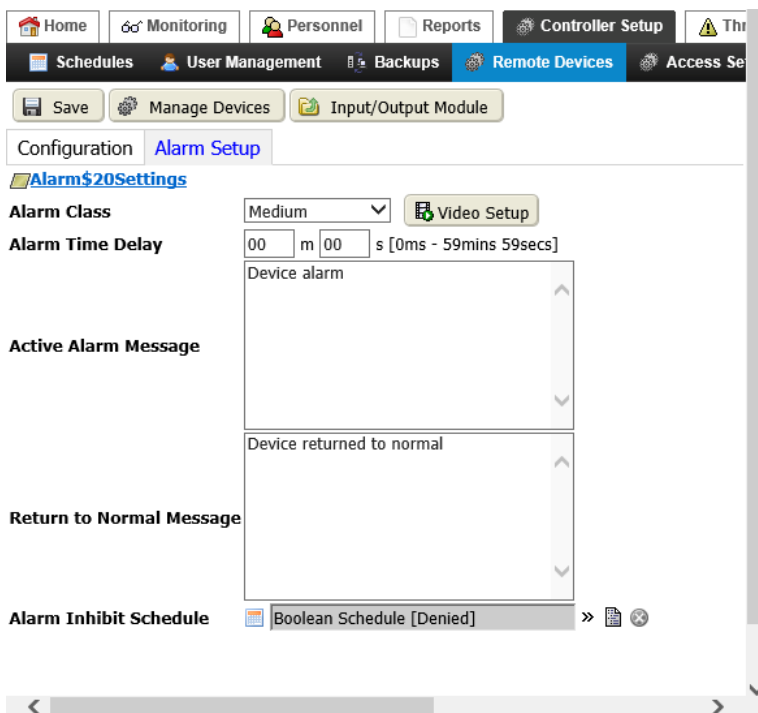
Outputs

A digital output (DO) is a device that controls door hardware or annunciates an alarm. For example, if a door contact senses that a door has been held open for too long, an output (bell or horn, for example) audibly alerts personnel that the door is open. Outputs may be used to turn lights, heaters, or air conditioners on and off.

Alarm Setup tab (inputs only)

This tab appears for input points and configures an alarm associated with the point. This includes additional points and camera events.

Figure 250 Alarm Setup tab



You access point views from more than one location. For example, from the main menu click **Remote Devices**→**Remote Modules**→**Remote Module Setup**, double-clicking the module row in the table, clicking the **Additional Points** tab, clicking a link to a point, and clicking the **Alarm Setup** tab. This step provides access to a remote module point.

The Alarm Settings link also opens the **Alarm Settings** view for this point. Alarm source extension properties are documented in *System Setup-Alarm Setup*.

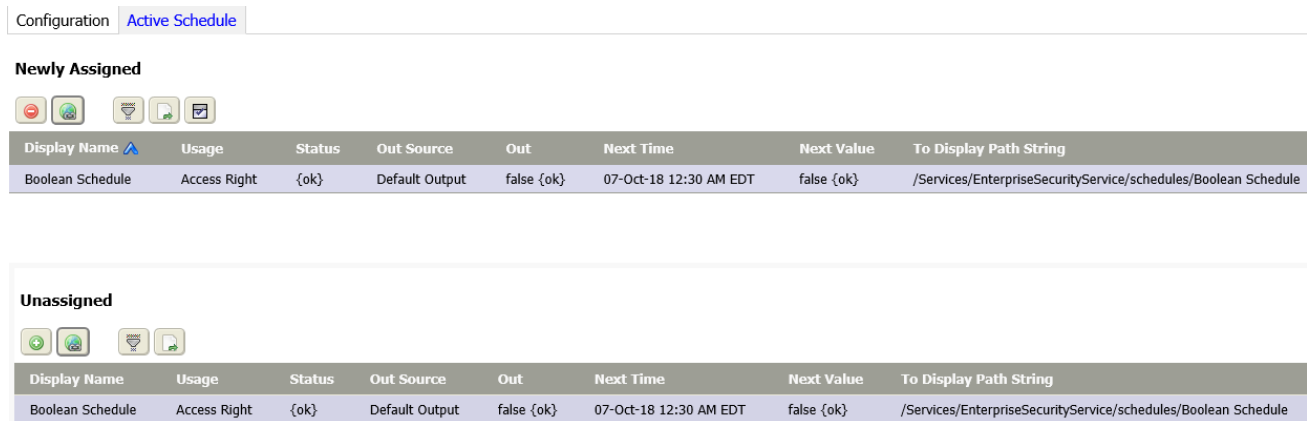
A Supervisor Fault Settings link displays on a supervised input (Sdi) only. This link identifies the point and navigates to the **Supervisor Fault Settings** view that displays a full list of alarm source extension properties. Alarm source extension properties are documented in *System Setup-Alarm Setup*.

Property	Value	Description
Alarm Class	drop-down list	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.
Alarm Time Delay	minutes and seconds (defaults to zero)	Prevents nuisance alarms caused by momentary changes in a state value (Normal, Low Limit, High Limit) by defining the minimum time period that an alarm condition must continuously exist before the object alarms. At the expiration of this time, an alarm is generated if the offnormal condition still exists. Alarm Time Delay does not affect alarms generated by a fault. There is no delay when transitioning in or out of a fault-generated alarm. Alarm Time Delay applies to entities that transition both in and out of alarm states. Therefore, an alarm status may continue to display as Offnormal (for example) for a time (equal to the time delay) after the value has come back to normal. The time delay is a minimum time period that a normal condition must exist before the object comes out of alarm.
Active Alarm Message	text	Creates a custom message that appears under the Type heading in several views and windows when the point is in an active alarm state.
Return to Normal Message	text	Creates a custom message that appears when a fault is cleared.
Alarm Inhibit Schedule or Alarm Ext Alarm Inhibit	Ref Chooser	Selects a schedule to inhibit alarms during certain time periods defined by the selected schedule. You must save any unsaved changes in this view before you can assign an inhibit schedule.
Video Setup button	button	Opens the Video Setup window, which selects, enables and configures a video camera to associate with the alarm point or device.
Supervisor Fault Settings (appears only on a supervised input (Sdi).	link	Identifies the point and allows you to navigate to the Edit Alarm Settings view, which displays a full list of alarm source extension fields. The properties displayed under this heading are described above in this table.

Active Schedule tab (outputs only)

This tab displays a table of assigned schedules and the standard control icons for assigning or un-assigning schedules that control when an output is effective. This tab appears on Relay Output points (Ro)

Figure 251 Active Schedule tab



The point’s display name appears at the top of the view (Ro3 in this example).

You access this tab from the **Edit Points** view. To access the **Edit Points** view, click **Remote Devices**→**Remote Modules**→**Remote Module Setup**, double-click the module row in the table, click the **Add Points** tab, click a link to an output point and click the **Active Schedule** tab.

You manually assign or unassign schedules to the currently displayed point using the learn mode, the assign and unassign buttons.

Columns

Table 62 Active Schedule columns

Column	Description
Display Name	Reports the name of the schedule.
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	Drives the output for the schedule. For example, an Out Source, such as “week:Thursday” means that events follow the weekly schedule for Thursday. If a special event is controlling the schedule, you may see, <code>Special event:Event Name</code> . Event Name is the name given to the special event when it was set up.
Out	Identifies the current state of the schedule.
Next Time	Identifies the next time the schedule will change.
Next Value	Identifies the next state the schedule will change to.
To Display Path String	Reports the station path for this point.

Edit meta data window

This window configures additional information to include with the camera event alarm.

Figure 252 Edit window

Facet Key	Facet Value
cameraHandleOrd	h:144f7
cameraOrd	slot:/Drivers/Axis Video
startRecording	false
videoEventDescription	Motion Started
videoEventTimestamp	null
videoEventType	Motion Started

You access this view from the main menu by clicking clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Axis Video Network row in the table, clicking the **Cameras** tab, double-clicking a camera row in the table, clicking the **Events** tab, discovering events, double-clicking an event row, clicking the **Alarm Setup** tab, and clicking the **Alarm Ext...** link.

Video Setup window

This window configures video properties. You can use this window to assign a camera to an alarm class and specify how that camera should react to the associated alarm class.

Figure 253 Video Setup window

You access this view from the main menu by clicking clicking **Controller Setup**→**Remote Devices**→**Remote Drivers** followed by double-clicking the Axis Video Network row in the table, clicking the **Cameras** tab, double-clicking a camera row in the table, clicking the **Events** tab, discovering events, double-clicking an event row, clicking the **Alarm Setup** tab, and clicking the **Video Setup...** link.

Properties

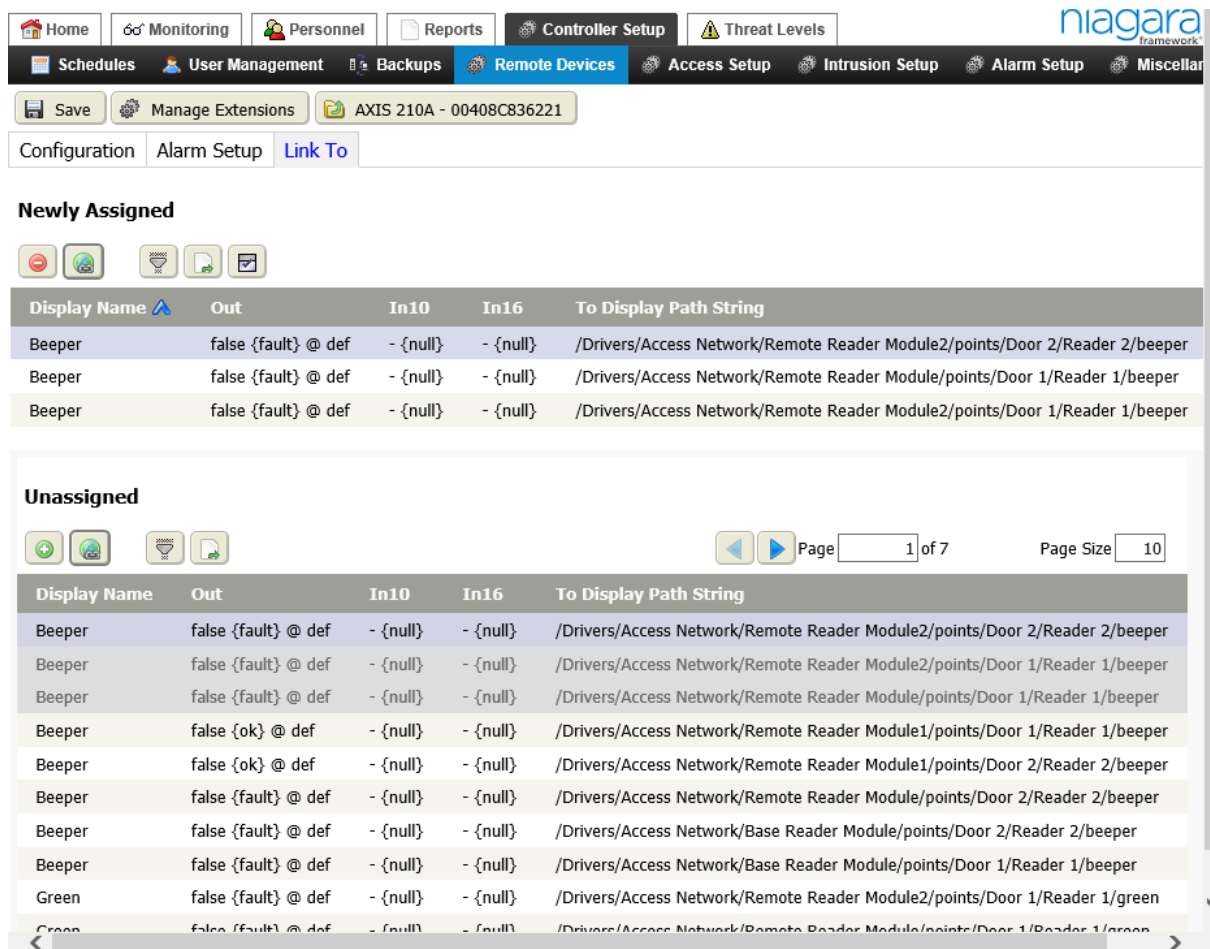
Property	Value	Description
Video Enabled	true or false (default)	Turns on and off the use of a video camera.
Camera	drop-down list of available cameras	Selects the camera to use from the list.
Go to Preset	true or false (default)	Turns the use of a video preset on and off. A preset is a preconfigured camera position and configuration that specifies what the camera points to and at what settings it records. false configures the camera to record without moving to the preset configuration. true configures the camera to record and moves to the preset configuration.

Property	Value	Description
Camera Preset	number	Identifies the number of the preset to use if Go to Preset is set to <code>true</code> .
Send Alarm to Display	<code>true</code> or <code>false</code> (default)	Enables and disables the sending of an alarm to a display (monitor).

Link To tab

This tab manages the connection between a camera event and another device, such as a beeper.

Figure 254 Example of a Link To tab



Buttons

In addition to the standard buttons (Delete, Filter, and Export), these buttons support links from the camera to another device.

- Hyperlink opens an **Edit Points** view.
- Assign Mode buttons open and close the **Unassigned** pane.
- Assign moves a discovered item from the **Unassigned** view to the **Assigned** view.

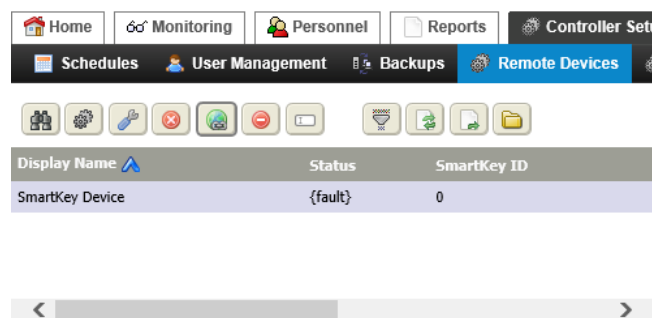
Columns

Column	Description
Display Name	Reports the name of the device to link to.
Out	Reports if the output source is ok or in fault.
In10	Reports if the first input point is ok or in fault.
In16	Reports if the last input point is ok or in fault.
To Display Path String	Identifies where in the station the device is located.

SmartKey Discovery view

This view provides a way to add SmartKey devices and other intrusion devices or keypads to your system using the discover and learn modes.

Figure 255 SmartKey Discovery view






You access this view from the main menu of a remote controller by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers**, and double-clicking the SmartKey Network row in the table.

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

Buttons



In addition to the standard control buttons (Manage Devices, Hyperlink, Delete, Rename, Filter, Refresh, Export, and Learn Mode), these control buttons perform unique functions:

-  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.
-  Preferences opens the **Preferences** window, which configures the SmartKey feature.
-  Set COM Port opens the **Set COM Port** window, which contains a text field that allows you to set a COM port used with SmartKey devices to communicate. Refer to the *Remote I/O Module (T-IO-16-485) Mounting and Wiring Instructions*.

NOTE: You do not need to use SmartKey discovery if you already added a device using a valid SmartKey ID number. If the device shows a valid status, {ok}, in the **SmartKey Devices** tab, it is already on line and discovery is not necessary.

Discovered view

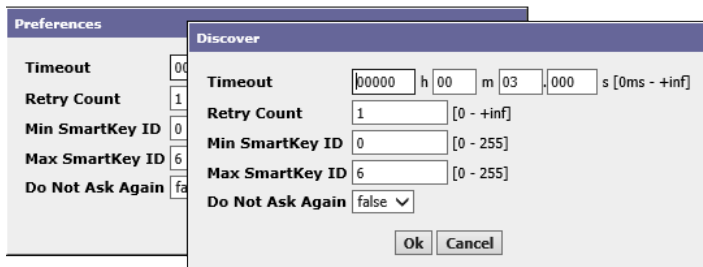
In addition to the standard functions of filter and export, the right-click menu and control buttons at the top of the pane provide these functions.


-  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 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.

Discover and Preferences windows

These two windows require the same properties.

Figure 256 Preferences and Discover windows



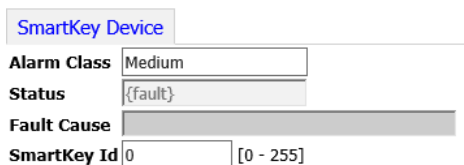
You access the Preferences window by clicking the Preferences button () on the **Smartkey Device Manager - Database** view.

Property	Value	Description
Timeout	hours minutes seconds	Defines the amount of time to wait for each device request before timing out.
Retry Count	number	Configures how many times to repeat a network read request, if no response is received before the response timeout interval elapses.
Min SmartKey ID	number	Limits the discovery to a range of device Id numbers beginning with this number.
Max SmartKey ID	number	Limits the discovery to a range of device Id numbers ending with this number.
Do Not Ask Again	true or false	Inhibits the Discovery window from opening again before the system initiates the discovery search.

SmartKey Device Manager - Database view

This window configures the SmartKey device.

Figure 257 SmartKey Device Manager - Database view



You access this view and tab by clicking the Manage Devices button () on the **Smartkey Device Manager - Database** view, followed by adding a device.

Properties

In addition to the standard properties (**Status** and **Fault Cause**), these properties support the SmartKey device.

Property	Value	Description
Alarm Class	drop-down list	Defines alarm routing options and priorities. Typical alarm classes include High , Medium and Low . An alarm class of Low might send an email message, while an alarm class of High might trigger a text message to the department manager.
SmartKey Id	number	Provides a unique device ID number used to identify the device on the network. A SmartKey ID must be entered using the device's keypad before it is connected to the system.

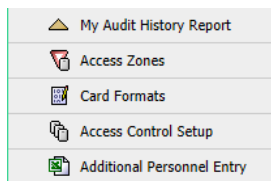
Chapter 9 Controller (System) Setup—Access Setup

Topics covered in this chapter

- ◆ Access Zones views
- ◆ Add New (or edit) Access Zone view
- ◆ Card Formats view
- ◆ Wiegand Format Editor view, Wiegand Format tab
- ◆ Access Control Setup view
- ◆ Additional Personnel Entry — Import Info tab

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 258 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.

Figure 259 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.

Buttons

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 63 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.

Figure 260 Access Zone view/tab

Display Name

Summary	Access Zone	Activity Alert Exts	Occupants	Supervisors	Entry Readers	Exit Readers	Grouping
---------	-----------------------------	---------------------	-----------	-------------	---------------	--------------	----------

Occupancy Count

Occupied

Lock Down

Occupancy Criteria

Passback Mode

Above High Threshold Enforcement

At High Threshold Enforcement

Below Low Threshold Enforcement

At Low Threshold Enforcement

Supervisor Required Enforcement

Pending Time m s [10secs - 1min]


Passback Timeout h m s [0ms - 1day]

Reset Occupancy Enabled

Reset Occupancy Time : : EDT

High Threshold

Low Threshold

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.

Links

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)	Enables and disables a lock down, which prohibits immediate access to the zone regardless of how the enforcement rules are configured: false allows normal operation. true disables (locks down) the zone.
Occupancy Criteria	drop-down list (defaults to Any)	Keeps track of who is in the zone: Any counts all personnel, including supervisors. This option applies no criteria regarding who must be present. Supervisors indicates that a supervisor (person) must be present.
Passback Mode	drop-down list (defaults to Hard)	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: Off disables passback mode, which allows personnel to exit and return as often as they wish. Soft grants return access again to the zone, but generates an alarm. Hard denies return access to the zone and generates an alarm.
Above High Threshold Enforcement	drop-down list (defaults to Off)	Specifies the type of enforcement to use when occupancy exceeds the high threshold setting: Off disables above-high-threshold enforcement. Soft allows access and generates an alarm. Hard denies access and generates an alarm.
At High Threshold Enforcement	drop-down list (defaults to Off)	Specifies the type of enforcement to use when occupancy meets the high threshold setting: Off disables enforcement. Soft grants access and generates an alarm.
Below Low Threshold Enforcement	drop-down list (defaults to Off)	Specifies the type of enforcement to use when occupancy falls below the low threshold setting: Off disables below-low-threshold enforcement. Hard grants access and generates an alarm.
At Low Threshold Enforcement	drop-down list (defaults to Off)	Specifies the type of enforcement to use when occupancy meets the low threshold setting: Off disables below-low-threshold enforcement. Soft grants access and generates an alarm.

Property	Value	Description
Supervisor Re- quired Enforcement	drop-down list	Denies access to all non-supervisory persons unless a supervisor is already an occupant. <i>Off</i> disables the requirement for a supervisor. <i>Soft</i> requires a supervisor. Grants access even though a supervisor is not present but generates an alarm. <i>Hard</i> denies access when a supervisor is not present and generates an alarm.
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 261 Add New Access Zone Summary tab



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 that contains this access zone.

Property	Description
Fallback Enforcement:	Reports the current state of fallback enforcement (Off, Soft, or Hard), 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 262 Activity Alert Exts on a reader

Display Name		Access Zone	
Summary	Access Zone	Activity Alert Exts	Occupants
Supervisors	Entry Readers	Exit Readers	Grouping
Anti Passback Violation Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Access Zone Disabled Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Occupancy Violation Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Supervisor Required Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Granted But Anti Passback Violation Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Granted But Occupancy Violation Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Granted But Access Zone Disabled Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging
Granted But Supervisor Required Alert	Alarm Class	Medium	Video Setup <input checked="" type="checkbox"/> Enable Logging

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 Passback Mode on the Access Zone tab is set to Hard and someone has attempted to re-enter the zone after leaving the zone.
Access Zone Disabled Alert	Configures what to do when Lock Down on the Access Zone tab is set to true , and an attempt has been made to enter the zone.
Occupancy Violation Alert	Configures what to do when the maximum occupancy as defined by High Threshold 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 Occupancy Criteria on the Access Zone tab is set to Supervisor , and no supervisor has entered the zone.
Granted But Anti Passback Violation Alert	Configures what to do when Passback Mode on the Access Zone tab is set to Soft 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 High Threshold 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 Lock Down on the Access Zone tab is set to true and someone has left the zone.
Granted but Supervisor Required Alert	Configures what to do when Occupancy Criteria on the Access Zone tab is set to Supervisor and no supervisor has entered the zone.

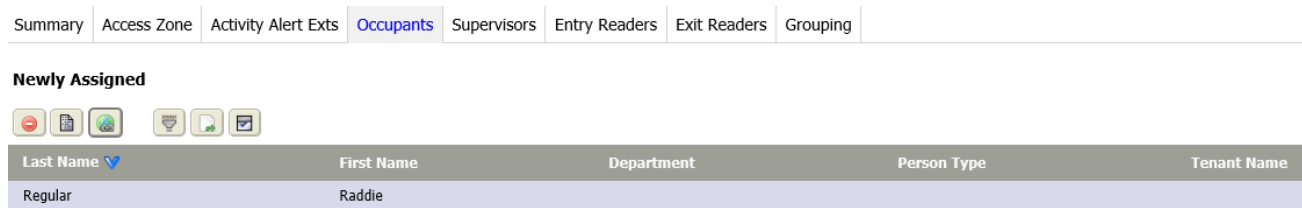
Properties

Property	Value	Description
Alarm Class	drop-down list; defaults to <i>Medium</i> for all alerts.	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.
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).

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.

Figure 263 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.

Buttons

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 64 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.

Figure 264 Access Zone Supervisors tab

Summary	Access Zone	Activity Alert Exts	Occupants	Supervisors	Entry Readers	Exit Readers	Grouping
Newly Assigned							
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.

Buttons

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 65 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.

Figure 265 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.

Buttons

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

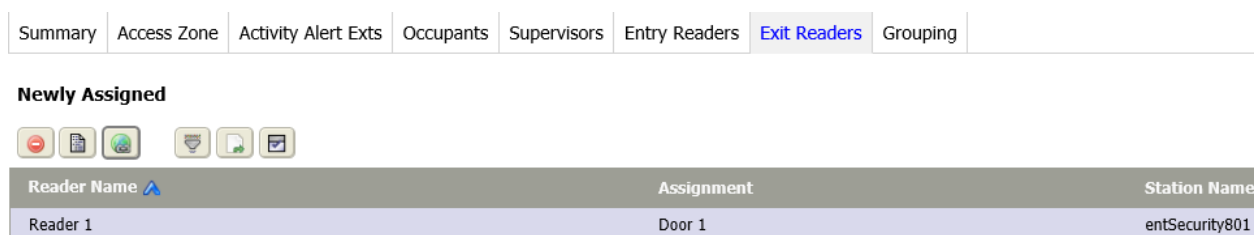
Table 66 Entry Readers columns

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.

Figure 266 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.

Buttons

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 67 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.

Figure 267 Grouping tab



Summary	Access Zone	Activity Alert Exts	Occupants	Supervisors	Entry Readers	Exit Readers	Grouping
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.

Buttons

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

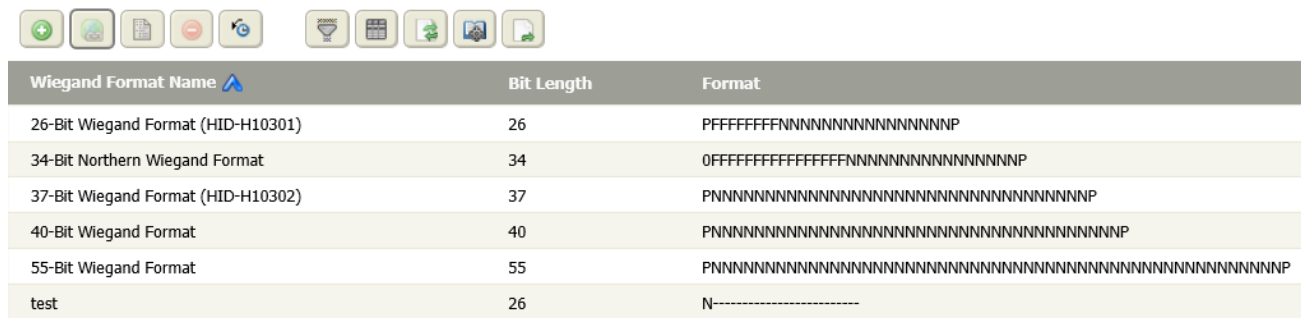
Table 68 Grouping tab columns

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.

Figure 268 Card Formats view






Wiegand Format Name	Bit Length	Format
26-Bit Wiegand Format (HID-H10301)	26	PFFFFFFFFNNNNNNNNNNNNNNNN
34-Bit Northern Wiegand Format	34	OFFFFFFFFFFFFFFFFNNNNNNNNNNNN
37-Bit Wiegand Format (HID-H10302)	37	PNNNNNNNNNNNNNNNNNNNNNNNNNN
40-Bit Wiegand Format	40	PNNNNNNNNNNNNNNNNNNNNNNNNNN
55-Bit Wiegand Format	55	PNNNNNNNNNNNNNNNNNNNNNNNNNN
test	26	N-----

To access this view from the main menu in a remote host station, click **Controller Setup**→**Access Setup**→**Card Formats**.

Buttons

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 69 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. NOTE: 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 269 Wiegand Format Editor view

The screenshot shows the 'Wiegand Format' tab in the editor. At the top, there are 'Save' and 'Wiegand Formats' buttons. Below are two tabs: 'Summary' and 'Wiegand Format'. The 'Wiegand Format' tab contains the following fields:

- Wiegand Format Name: [Text input field]
- Default Facility Code: [Text input field]
- Validation Bits: [Dropdown menu with 'All' selected]
- Bit Length: [Text input field with value '26' and range '[0 - 256]']
- Parity Bits: [Text input field with value '0' and range '[0 - 5]']
- Facility Start: [Text input field with value '0']
- Facility Length: [Text input field with value '0']
- Credential Start: [Text input field with value '0']
- Credential Length: [Text input field with value '1']
- Format: [Text input field with value '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.

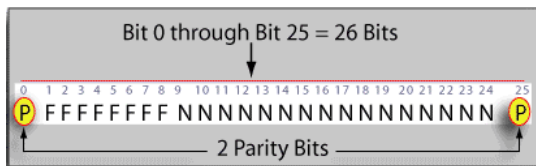
Wiegand Format tab properties

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 a badge. It does not need to match the Facility Length 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: All , the most restrictive or secure, validates bits representing all possible areas of the format. Credential and Facility Code only validates the Credential and Facility Code bits. Credential Only , the least restrictive or secure, only validates the Credential bits.

Property	Value	Description
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 Format property, page 298
Facility Start	number	Specifies the bit position that holds the first bit of the facility code. Refer to Format property, page 298
Facility Length	number	Specifies the total number of bits that are dedicated to facility code. Refer to Format property, page 298
Credential start	number	Specifies the bit position that holds the first bit of the credential numbers. Refer to Format property, page 298
Credential Length	number	Specifies the total number of bits that are dedicated to credential numbers. Refer to Format property, page 298
Format	text	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–parity bit (an extra bit added for error detection) F–facility code bit N–credential number bit 0–constant character of 0 (zero) 1–constant character of 1 (one) Refer to Format property, page 298
Parity Layout	one or more additional format properties	Define the expected parity: Odd or Even. Refer to Format property, page 298

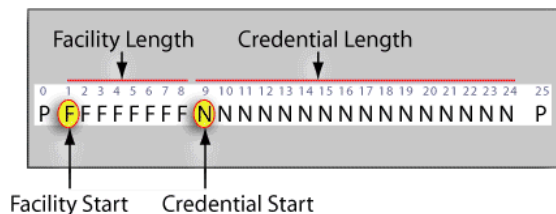
Format property

Parity Bits may be located anywhere in the format.

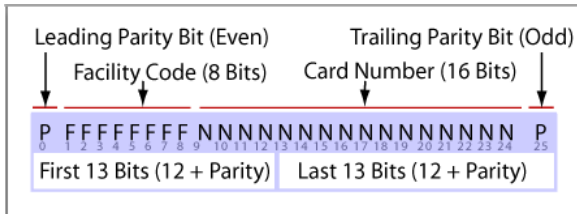


The example **Format** above has two parity bits. It specifies the location of these bits: one in the leading position, and the other in the trailing position.

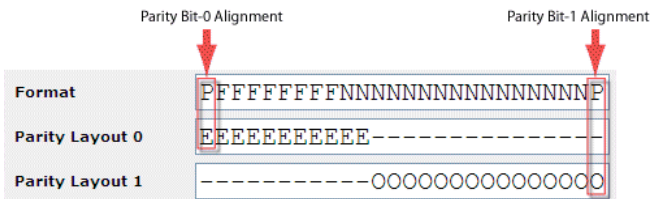
Facility Start, **Facility Length**, **Credential Start** and **Credential Length** identify where the information starts in the **Format**, and how many characters are involved.



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.



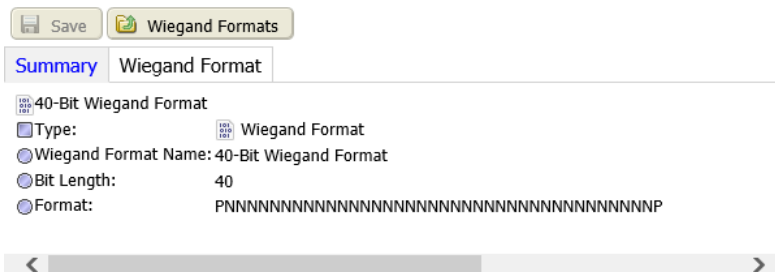
The locations of the “E” and “O” characters in the **Parity Layout** property designate the bits that are used to calculate the parity sum. Follow these rules as you enter these characters:

- 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 270 Wiegand format Summary tab



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.

Figure 271 Access Control Setup view

The screenshot shows the 'Access Control Service' configuration page. The 'Status' field contains '{ok}'. The 'Fault Cause' field is empty. The 'Cache Status' is set to 'Active'. The 'Enabled' field is a dropdown menu set to 'true'. The 'Display Unknown Wiegand Formats' field is a dropdown menu set to 'false'. The 'Has Pin Duress' field is a dropdown menu set to 'false'. The 'Pin Duress Offset' field is a text input containing the number '1'. The 'Remote Validation' field is a dropdown menu set to 'false'.

To access this view from the main menu of a remote host controller station, click **Controller Setup**→**Access Setup**→**Access Control Setup**.

Properties

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 Pin Duress Enabled property is set to true.
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 false. 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.

Figure 272 Additional Personnel Entry view

To access this view from the main menu of a remote host station, click **Controller Setup**→**Access Setup**→**Additional Personnel Entry**.

Links

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 273 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	FacilityCor	AccessRight0	StartDate0	EndDate0	AssignedThre	AccessRight1	StartDate1
2	Bruce				Emergency	FALSE					Bldg.2-Emergency Responder					
3	Todd			Afion Remote	FALSE	FALSE	Engineering				Bldg.1-Interior Doors			7		
4	Tracy	L			FALSE	FALSE										
5	Randy			Afion Remote	FALSE	FALSE	Engineering				Bldg.1-Interior Doors					
6	Robert		AHrPlmXE	Afion Remote	FALSE	FALSE	Sales	37-Bit Wiegand Foi	3744365	0	Bldg.1-Perimeter Doors					
7	Steven				Police	FALSE					Bldg.2-Police Responder					
8	Theodore	N	AHsXlmVgXh2GEBGITsj+vgXEC6l		FALSE	FALSE		26-Bit Wiegand Foi	0	0	Bldg.1-Interior Doors					Bldg.1-Perimeter Doors
9	Sandeev			Acme Pha	Operator	FALSE	Tracking	40-Bit Wiegand Foi	123456789	0	Bldg.1-Interior Doors					Bldg.1-Perimeter Doors
10	Sneepie				FALSE	FALSE		37-Bit Wiegand Foi	3744367	0	AA Night					Bldg.1-Interior Doors
11	John		AH9dlmXl10GFd2Ql8	Administra	FALSE	FALSE	District	37-Bit Wiegand Foi	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 Foi	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 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 274 Export Personnel Records window

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.
User Pass Key	text	Defines the password the system will require when importing this data back into the database.

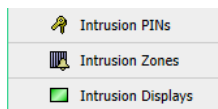
Chapter 10 Controller (System) Setup–Intrusion Setup

Topics covered in this chapter

- ◆ Intrusion Pins view
- ◆ Add New (or edit) Intrusion Pin view, Intrusion Pin tab
- ◆ Intrusion Zones views
- ◆ Add New (or edit) Intrusion Zone view
- ◆ Edit Existing Intrusion Pin view
- ◆ Intrusion Displays views
- ◆ Add New (or edit) Intrusion Display view

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 275 Intrusion menu

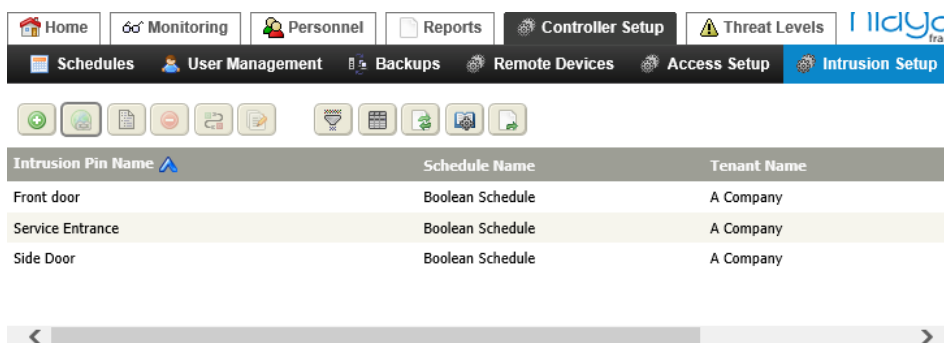


A Supervisor station does not include the Intrusion Displays menu item.

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 276 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

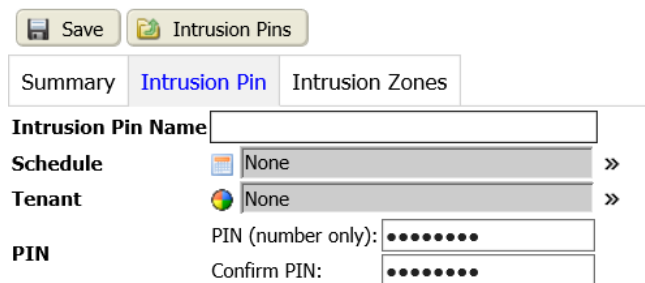
Table 70 Intrusion PIN table columns


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 277 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.
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 278 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.



Figure 279 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.

Buttons

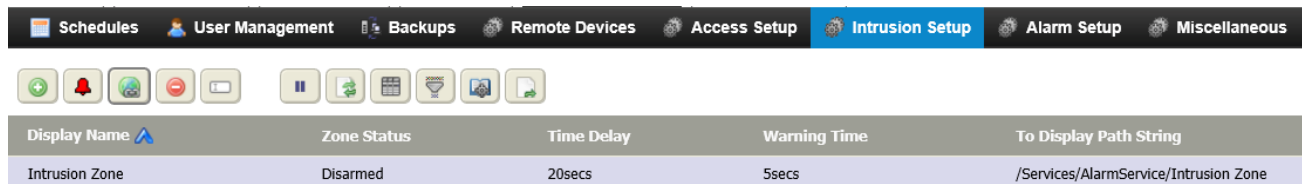
In addition to the standard buttons (Delete, Summary, Filter and Edit), these buttons support intrusion zones tab under the **Intrusion Pins** view:

-  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 280 Intrusion Zones view






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	Identifies the name of the intrusion zone.
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.

Figure 281 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 01 Jan 1970 05:30 AM IST

Escalation Level1 Enabled false

Escalation Level1 Delay 00000 h 05 m [1min - +inf]

Escalation Level2 Enabled false

Escalation Level2 Delay 00000 h 15 m [2mins - +inf]

Escalation Level3 Enabled false

Escalation Level3 Delay 00000 h 30 m [3mins - +inf]

Zone Enabled false {ok}

Zone Schedule None >>

Zone Input None >>

Zone Status Disarmed

Arming Test Status Success {ok}

Time Delay 00000 h 00 m 20 s [0ms - +inf]

Warning Time 00000 h 00 m 05 s [0ms - +inf]

Count Down 0 sec

Last Activity 01 Jan 1970 05:30 AM 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 ().

Links

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.

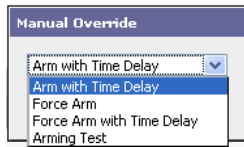
Property	Value	Description
Ack Required	check boxes	Sets the requirements for an alarm acknowledgment in this intrusion zone. Alarm acknowledgments are required only for selected options.
Priority	number between 1 (highest priority) and 255	Sets an importance level for each of the listed priority categories: 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.

Property	Value	Description
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 (true) or disabled (false).
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.
Zone Status	read-only	Displays the status of the intrusion zone: Armed, Disarmed, or Arming.
Arming Test Status	read-only true or false	Indicates if the last arming test was successful (true) or unsuccessful (false).
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 282 Manual Override window



The window opens when you click the **Manual Override** button on the edit intrusion zone view.

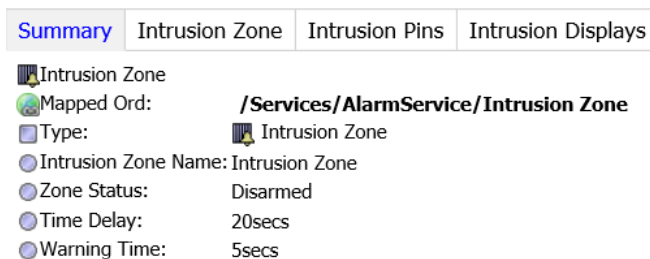
Table 71 Manual Override options

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. NOTE: 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 283 Intrusion Zone Summary tab



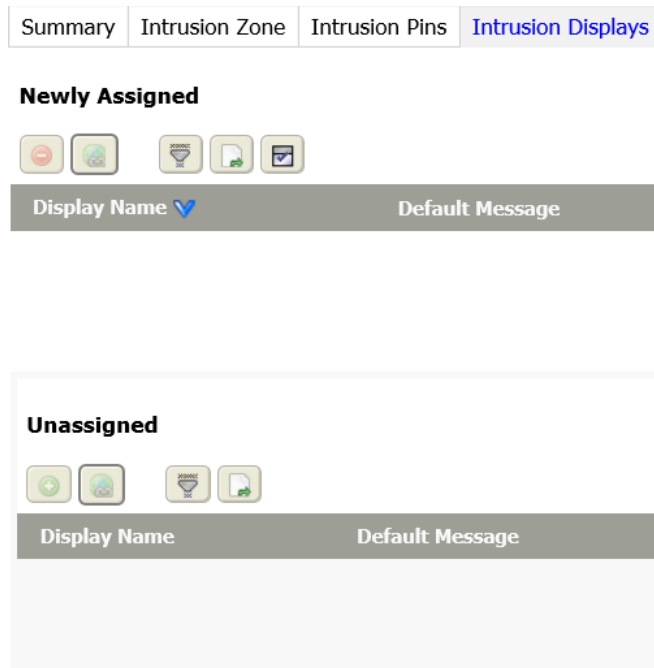
This view opens when you click **Controller (System) Setup→Intrusion Setup→Intrusion Zones** and double-click a zone in the table.

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.

Figure 284 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.

Links

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.

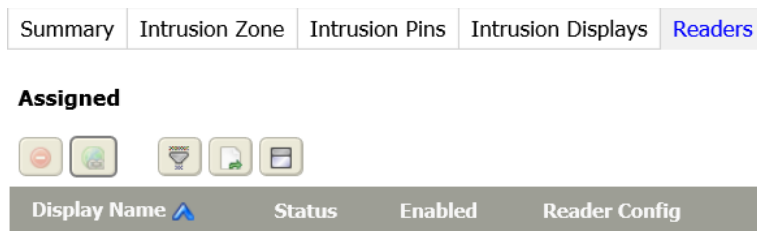
Columns

Column	Description
Display Name	Reports the name of the intrusion display.
Default Message	Reports the default message for this display.
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 285 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 286 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.

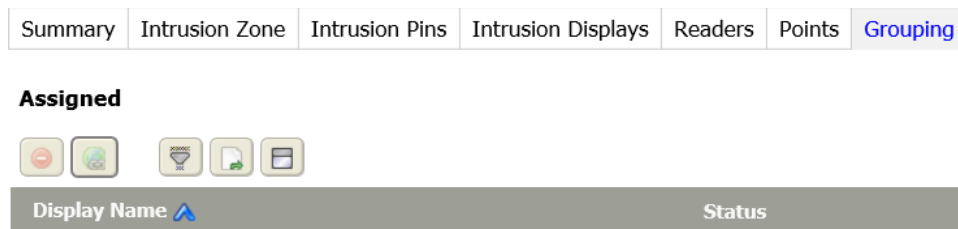
Columns

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.

Figure 287 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.

Buttons

This tab provides standard control buttons.

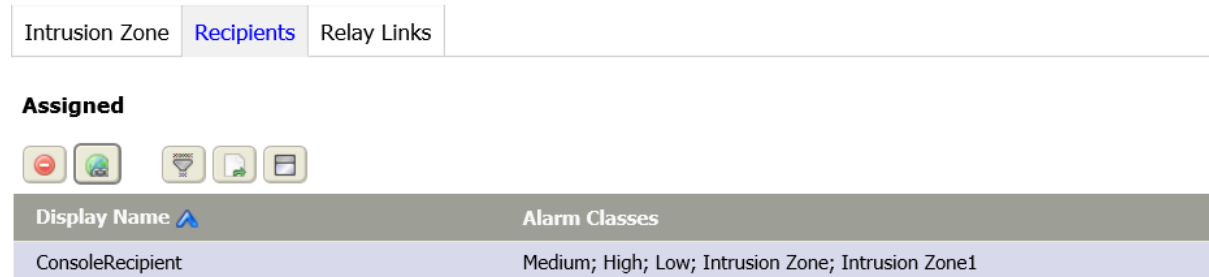
Columns

Column	Description
Display Name	Provides the name of the group.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}
To Display Path String	Displays the path to the group location.

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.

Figure 288 Intrusion Zone Recipients tab



To access this view from the main menu, click **Controller (System) Setup**→**Intrusion Setup**→**Intrusion Zones** the 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.

Buttons

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 72 Recipients columns

Column	Description
Display Name	Reports the name that describes the event or function.
Alarm Classes	Reports the Display Name 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.

Figure 289 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 **EscalationLevel1** 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.

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.

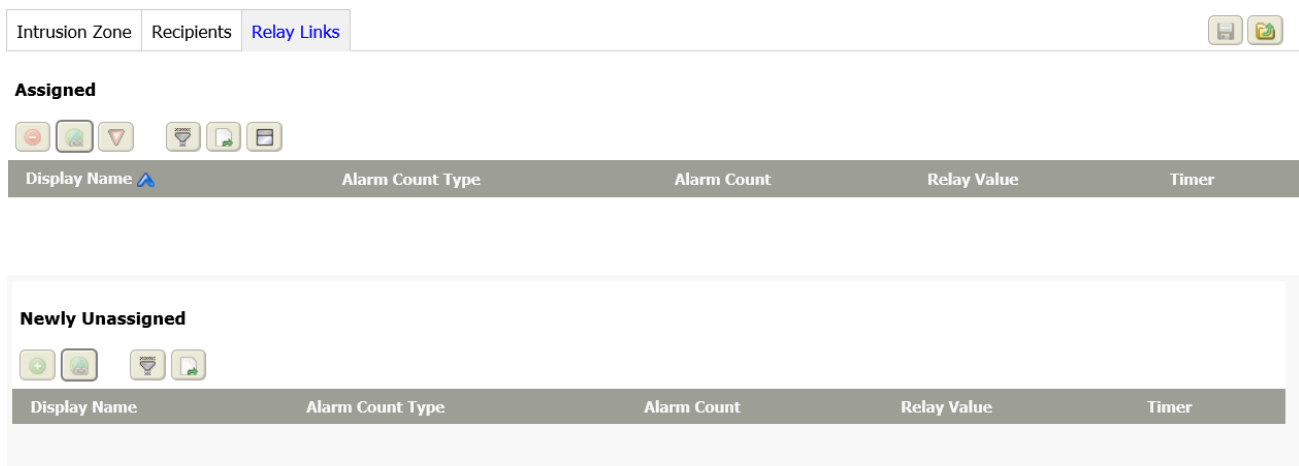
Columns

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 290 Intrusion zone Relay Links tab






To access this view from the main menu, click **Controller (System) Setup→Intrusion Setup→Intrusion Zones** the 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.

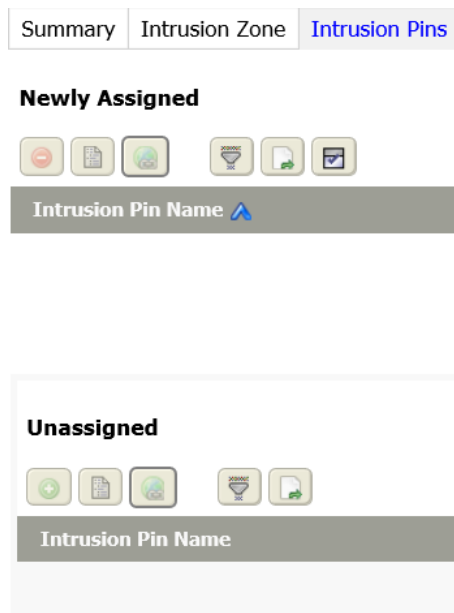
Columns

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 Timer or until the alarm is acknowledged. Open Alarm count activates the relay for the length of the time defined by Timer or until the alarm is cleared from the console. In Alarm Count activates the relay for the length of time defined by Timer or until the alarm returns to normal. Total Alarm Count activates the relay or the length of time defined by Timer 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.

Figure 291 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.



Links

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.

Figure 292 Intrusion Displays view



You access this view from the main menu by clicking **Controller Setup→Intrusion Setup→Intrusion Displays**.

Buttons

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.

Figure 293 Add New Intrusion Display view

Display Name

Intrusion Display | Activity Alert Exts | Intrusion Zones

Default Message

Smart Key Device

Scroll Start Delay h m s s [0ms - +inf]

Scroll Column Delay h m s s [0ms - +inf]

Change Delay h m s s [0ms - +inf]

Inactivity Time h m s [0ms - +inf]

Status Beep

Arming Pin Required


Status Pin Required

Point Display

Default Page

In Alarm Beep

In Alarm Max Beep h m 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.

Links

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.

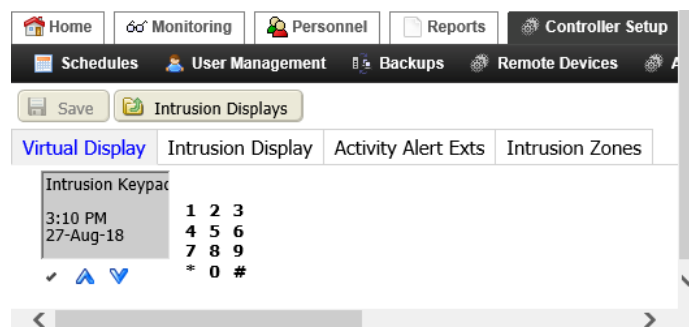
Property	Value	Description
Default Message	text	Defines what to display on the default Time screen, at the top of the display.
SmartKey Device	drop-down list (defaults to None)	Lists the SmartKey devices that are available to be assigned to the current intrusion display. NOTE: This list displays as a 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 (<i>true</i>) and off (<i>false</i>) 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 (<i>true</i>) or does not require (<i>false</i>) a valid PIN when arming an intrusion zone.
Status Pin Required	true or false	Requires (<i>true</i>) or does not require (<i>false</i>) 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. <i>No Path</i> displays the fault message without identifying the point. For example: <code>Supervisor Fault Detected</code> <i>Normal Path</i> displays the fault message followed by the point identity. For example: <code>Door1.Sensor.Supervisor Fault Detected</code> <i>Reverse Path</i> displays the point identity followed by the fault message. For example: <code>Supervised Fault Detected.Sensor.Door1</code>
Default Page	drop-down list	Assigns a default display page for the SmartKey device. This page opens at the end of the Inactivity Time and is, typically, the initial screen that a user sees at the SmartKey device. Summary sets the Summary screen as the default screen. This

Property	Value	Description
		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. Time 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 In Alarm Beep 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 294 Virtual Display tab



Intrusion Display tab (configuration)

This tab provides access to the intrusion display properties.

Display Name

Intrusion Display | Activity Alert Exts | Intrusion Zones

Default Message

Smart Key Device

Scroll Start Delay h m s s [0ms - +inf]

Scroll Column Delay h m s s [0ms - +inf]

Change Delay h m s s [0ms - +inf]

Inactivity Time h m s [0ms - +inf]

Status Beep

Arming Pin Required

Status Pin Required

Point Display

Default Page

In Alarm Beep


In Alarm Max Beep h m 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.

Figure 295 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.

Alerts

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.

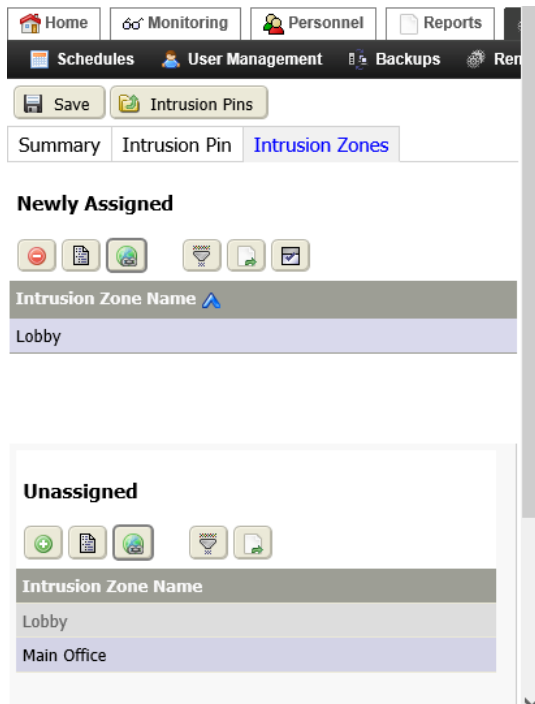
Alert properties


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.

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..

Figure 296 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.

Buttons

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	Displays the name that identifies the intrusion zone/display association.
Zone Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}
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.

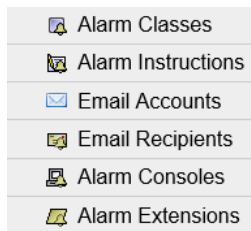
Chapter 11 Controller (System) Setup–Alarm Setup

Topics covered in this chapter

- ◆ Alarm Classes views
- ◆ Add New (or edit) Alarm Class view
- ◆ Alarm Instructions view
- ◆ Alarm Relays view (Alarm Count Relays)
- ◆ Add New (or edit) Alarm Count To Relay view
- ◆ EmailService view (Email Accounts)
- ◆ Email Recipients view
- ◆ Add New (or edit) Email Recipient view
- ◆ Alarm Consoles view
- ◆ Add (or edit) Alarm Console view, Alarm Classes tab
- ◆ Video Alarm Classes (Video Alarm Recipient) view
- ◆ Station Recipients views
- ◆ Add New (or edit) Station Recipient view
- ◆ Power alarm Setup (PlatformServices) view
- ◆ Alarm Extensions view
- ◆ Edit Alarm Extension properties (Alarm Source Info tab)

Setup views include displays that are related to configuring system components and network properties, as well as user preferences and other variables.

Figure 297 Alarm Setup menu



Alarm Classes views

Alarm classes allow you to group alarms into categories and assign them alarm priority levels.






Figure 298 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 73 Alarm Class columns

Column	Description
Display Name	Displays the name associated with the priority.
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	Displays 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 299 Add New Alarm Class

The screenshot shows the 'Alarm Class' configuration page in the Niagara Enterprise Security Reference web interface. The page is titled 'Alarm Class' and includes a 'Save' button and an 'Alarm Classes' link. The configuration fields are:

- Ack Required:** Normal (checkbox), Offnormal (checkbox), Fault (checkbox), Alert (checkbox)
- Priority:** Offnormal (255), Fault (255), Normal (255), Alert (255)
- Total Alarm Count:** 0
- Open Alarm Count:** 0
- In Alarm Count:** 0
- Unacked Alarm Count:** 0
- Time of Last Alarm:** 31 Dec 1969 07:00 PM EST
- Escalation Level1 Enabled:** false
- Escalation Level1 Delay:** 00000 h 05 m [1min - +inf]
- Escalation Level2 Enabled:** false
- Escalation Level2 Delay:** 00000 h 15 m [2mins - +inf]
- Escalation Level3 Enabled:** false
- Escalation Level3 Delay:** 00000 h 30 m [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.
Priority	number for each component state transition from 1-255 (defaults to 255, which is the lowest priority)	Defines 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, and from offnormal, fault and alert to Normal). The lower the number, the more significant the alarm. The highest priority alarm is number 1.
Total Alarm Count	read-only	Reports the total number of alarms assigned to the alarm class from all sources.
Open Alarm Count	read-only	Reports 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.

Property	Value	Description
In Alarm Count	read-only	Reports the total number of alarm sources.
Unacked Alarm Count	read-only	Reports the total number of unacknowledged alarms.
Time of Last Alarm	read-only	Reports the time that the system generated the last alarm assigned to this alarm class.
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 minuetts (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.

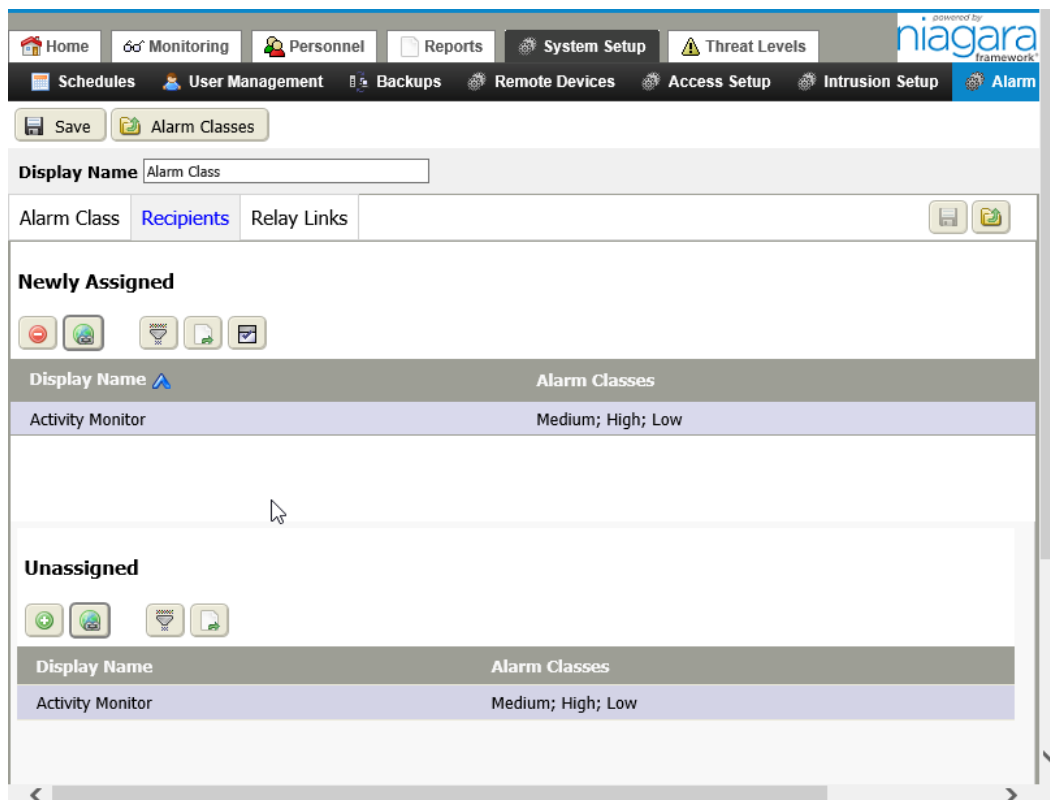
Recipients tab

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 300 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 buttons open and close the **Unassigned** pane.

Columns

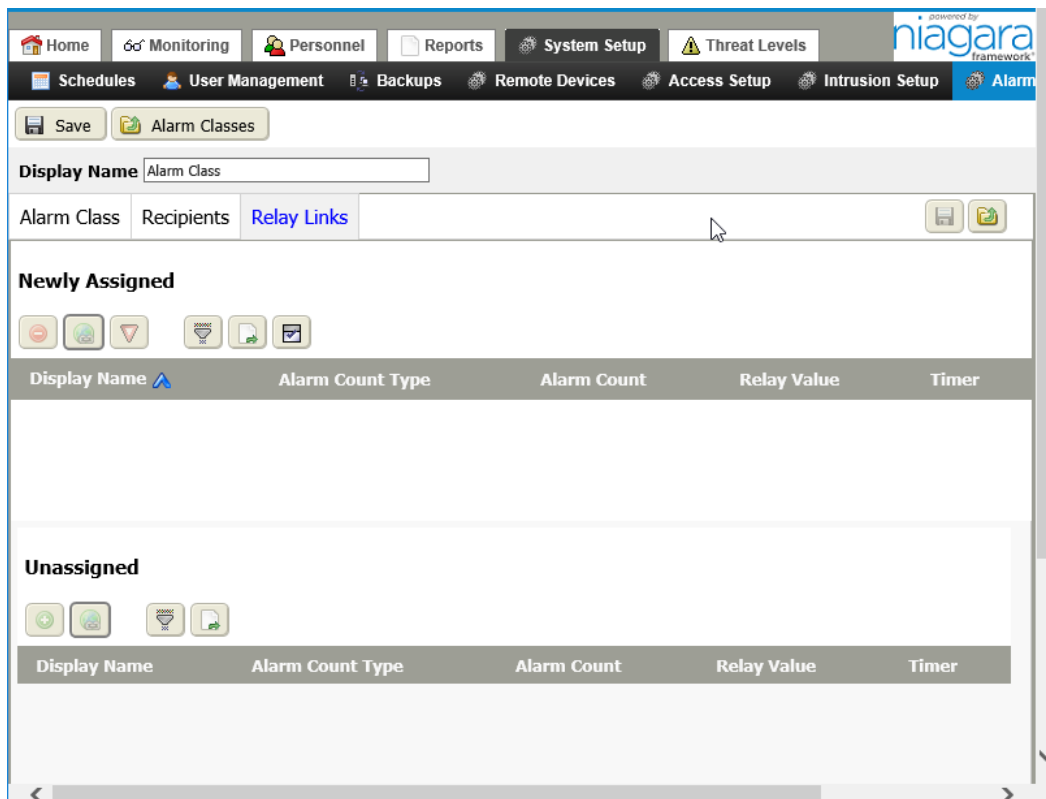
Table 74 Recipients tab columns

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 301 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.

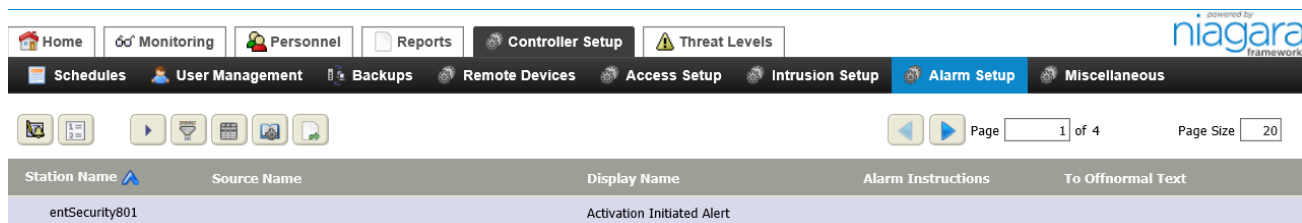
Columns

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.

Figure 302 Alarm Instructions view



Station Name	Source Name	Display Name	Alarm Instructions	To Offnormal Text
entSecurity801		Activation Initiated Alert		

This view opens when you click the **Alarm Instructions** submenu, under the **Controller (System) Setup→Alarm Setup** menu.

Buttons

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.

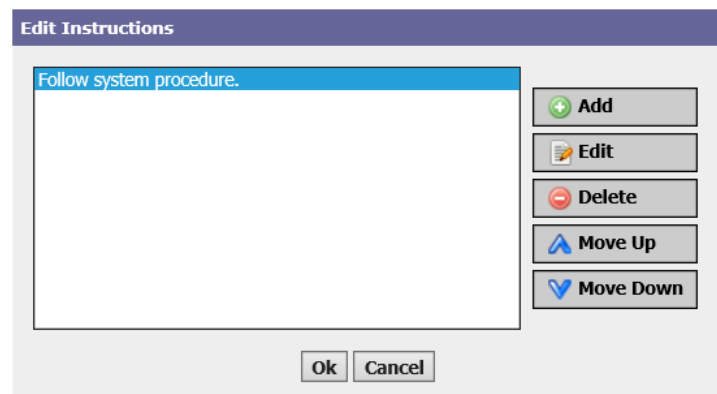
Columns

Column	Description
Station Name	Identifies the station where the alarm point source is located.
Source name	Identifies the name of the alarm source.
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 303 Edit Instructions window



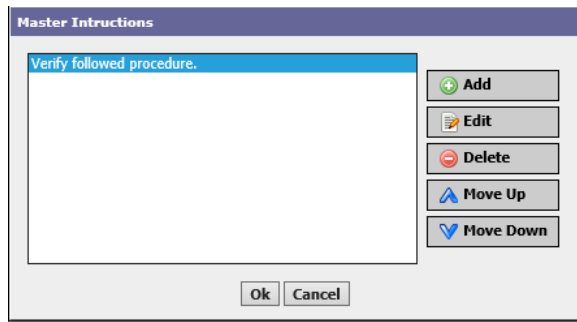
Access this view by selecting **Controller Setup→Alarm Setup→AlarmInstructions**. Then select a row and right click Or select a row and click on edit button on left above the table

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 304 Master Instructions window

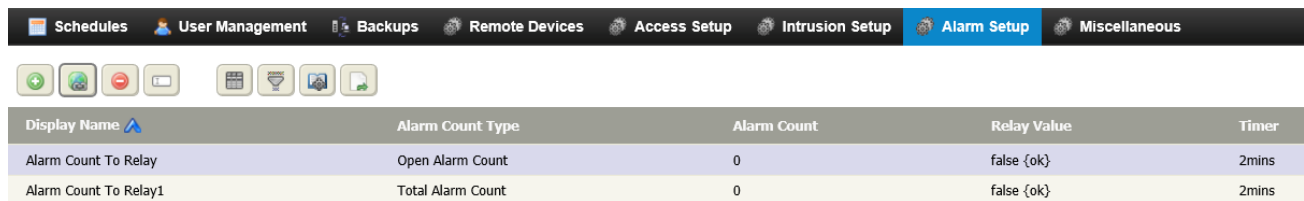


Use the **Add**, **Edit**, **Delete**, **Move Up**, and **Move Down** buttons to edit, arrange, and add alarm instructions to the desired alarm extensions.

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.

Figure 305 Alarm Relays view



This view opens when you select the **Alarm Count Relays** submenu, under the **System Setup**→**Alarm Setup** menu.

Buttons

This view displays standard controls across the top and a table of all alarm relay configurations in the lower part.

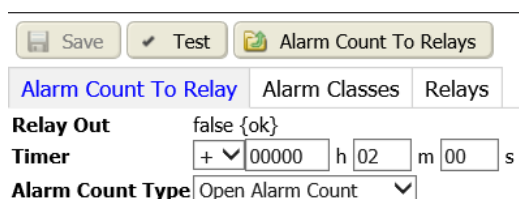
Columns

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.

Figure 306 Add New Alarm Count to Relay view



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.

Links

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.

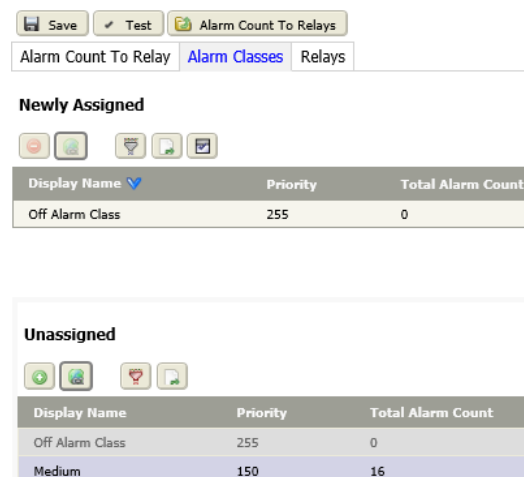
Properties

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. Unacked Alarm Count counts alarms that have not been acknowledged. Open Alarm count counts alarms that have not been cleared from the console. In Alarm Count counts alarms that have not yet returned to normal. Total Alarm Count counts all alarms regardless of state.

Alarm Classes tab

This tab manually assigns and unassigns alarm classes to the current alarm-count-to-relay action.

Figure 307 Add New Alarm Count To Relay view Alarm Classes tab




Newly Assigned

Display Name	Priority	Total Alarm Count
Off Alarm Class	255	0

Unassigned

Display Name	Priority	Total Alarm Count
Off Alarm Class	255	0
Medium	150	16

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.

Buttons

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.

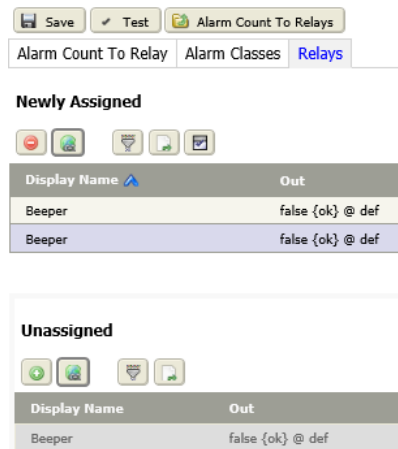
Columns


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 <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	Displays 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.


Figure 308 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.

Buttons

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 of the Relay name.
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.

Figure 309 EmailService view

This view opens when you select the **Email Accounts** menu item under the **System Setup→Alarm Setup** menu.

Links

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 entity is licensed and polling successfully. {down} indicates that the last poll was unsuccessful, perhaps because of an incorrect property. {disabled} indicates that the Enable property is set to false. {fault} indicates another problem. Depending on conditions, multiple status flags may be set including {fault} and {disabled}, combined with {down}, {alarm}, {stale}, and {unackedAlarm}.
Fault Cause	read-only	Reports the reason why a network, component, or extension is in fault. Fault Cause is blank unless a fault exists.
Enabled	true or false	Turns the feature on (true) and off (false).

Outgoing Account tab

This tab displays all the properties for the outgoing account associated with the EmailService.

Figure 310 Outgoing Account properties

The screenshot shows the configuration interface for an outgoing email account. At the top, there are buttons for 'Save' and 'Manage Accounts'. Below that are tabs for 'Email Service', 'Outgoing Account' (which is selected), and 'Incoming Account'. The configuration fields include:

- Hostname: A text input field.
- Port: A numeric input field with a range of [-1 - +inf].
- Account: A text input field.
- Password: A text input field with masked characters (dots).
- Pollrate: A time-based input field with units for hours (00000), minutes (01), and seconds (00).
- Enabled: A dropdown menu set to 'false'.
- Status: A dropdown menu set to '{disabled}'.
- Last Poll Success: A date and time selector (31 Dec 1969 07:00 PM EST).
- Last Poll Failure: A date and time selector (31 Dec 1969 07:00 PM EST).
- Last Poll Failure Cause: A text input field.
- Debug: A dropdown menu set to 'false'.
- Use Ssl: A dropdown menu set to 'false'.
- Use Start Tls: A dropdown menu set to 'false'.
- Transport: A dropdown menu set to 'Smtp'.
- Connection Timeout: A time-based input field (00000 h 00 m 10 s).
- Use Authentication: A dropdown menu set to 'false'.
- Reply To: A text input field.
- Persistent: A dropdown menu set to 'false'.
- Persistence Directory: A text input field with the value 'file:^email'.
- Allow Disabled Queuing: A dropdown menu set to 'false'.
- Queue Size: A numeric input field set to 0.
- Max Queue Size: A numeric input field with a range of [1 - +inf].
- Number Sent: A numeric input field set to 0.
- Max Sendable Per Day: A numeric input field with a range of [1 - +inf].
- Number Discarded: A numeric input field set to 0.
- Last Discard: A date and time selector (31 Dec 1969 07:00 PM EST).
- Last Discard Cause: A text input field.

To access this view, click **Controller (System) Setup**→**Alarm Setup**→**Email Accounts**, followed by clicking the **Outgoing Account** tab.

Properties

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 to 25	Identifies the port number 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 Hostname 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 Hostname 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.

Property	Value	Description
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 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.

Figure 311 Incoming Account tab

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.

Properties

In addition to the standard properties (**Enabled** and **Status**), these properties support an incoming account.

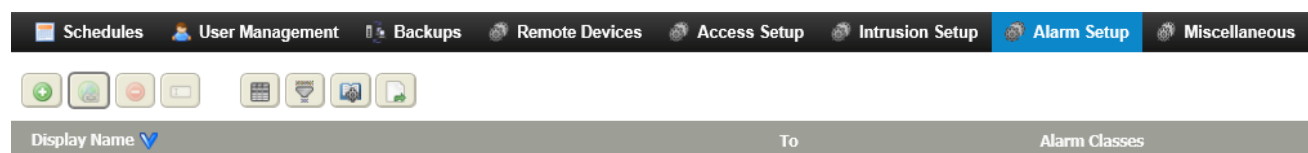
Property	Value	Description
Hostname	text	Identifies the name of the mail server. For example, mail.acme.com could be a Hostname.
Port	number from -1 to infinity; defaults to 110	Identifies the port associated with the email account. Typically, this number is 110, however, to set -1 the system searches for and uses a valid port.
Account	text	Identifies the name of the distinct account that is authorized for access to the Hostname mail server. For example, if you are using an email account named <code>controls@acme.com</code> on

Property	Value	Description
		the host described above, the account name is <code>controls</code> . The <code>Hostname</code> in this case could be <code>mail.acme.com</code> .
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 for 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.
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	Selects how the incoming email account handles incoming emails at the mail server. 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 Mark As Read marks all emails as read on the mail server when it checks the account to retrieve new email. Mark As Unread marks all emails as unread on the mail server when it checks the account to retrieve new email.

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 312 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 313 Add New Email Recipient view

The screenshot shows the configuration form for an email recipient. At the top, there are 'Save' and 'Email Recipients' buttons. Below them is the 'Display Name' field with the value 'Email Recipient'. There are two tabs: 'Email Recipient' (selected) and 'Alarm Classes'. The 'Time Range' section includes 'Start Time' (12:00:00 AM EDT) and 'End Time' (12:00:00 AM EDT). 'Days of Week' has checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked. 'Transitions' has checkboxes for Normal, Offnormal, Fault, and Alert, all checked. 'Route Acks' is set to 'true'. The 'To', 'Cc', and 'Bcc' fields are empty. 'Language' is empty. 'Email Account' is set to 'None'. The 'Subject' field contains the text: 'Niagara Alarm From %alarmData.sourceName%'. The 'Body' field contains a template: '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 seconds	Set a limited period of time during a 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: http://www.loc.gov/standards/iso639-2/langcodes.html
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 Email body, page 341

Email body

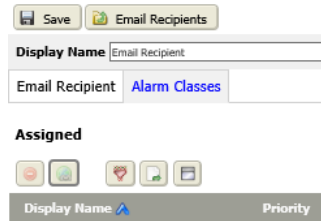
This property has the following editable default additional properties.

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 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.



Figure 314 Edit Email Recipient view



To access this view, click **Controller (System) Setup**→**Alarm Setup**→**Email Recipients**, and click the **Alarm Classes** tab.

Buttons

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.
Time of Last Alarm	Displays 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.

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 315 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.

Buttons

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.

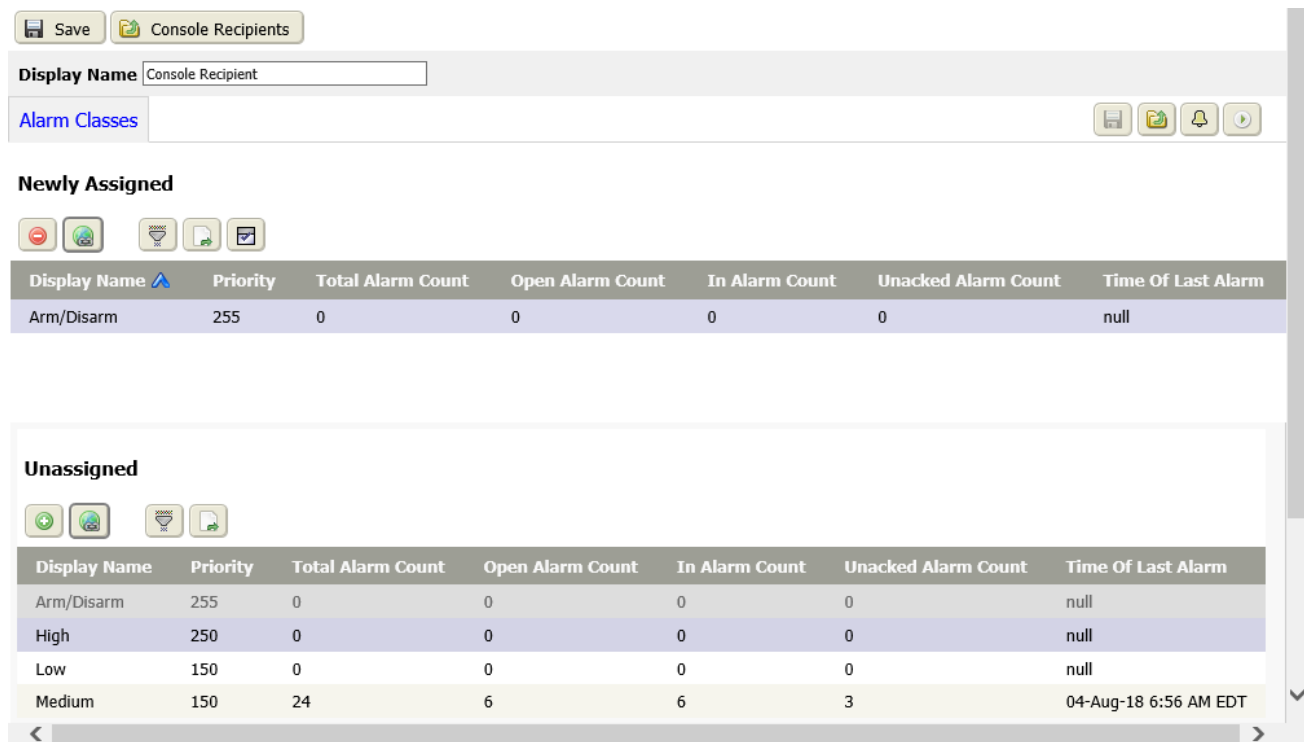
Columns

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.

Figure 316 Console Recipients Alarm Classes tab



This tab opens when you click **Controller (System) Setup→Alarm Setup→Alarm Consoles**, and click the plus button (+).

Buttons

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 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.

Column	Description
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Displays 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.

Figure 317 Video Alarm Recipient view

The screenshot shows the 'Video Alarm Recipient' configuration page. At the top, there are 'Save' and 'Alarm Setup' buttons. Below them are two tabs: 'Video Alarm Recipient' (selected) and 'Alarm Classes'. The main area contains the following fields:

- Time Range:** A section containing 'Start Time' and 'End Time' fields, each with a time and zone selector (e.g., 12:00 AM EDT).
- Days Of Week:** A row of checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked.
- Transitions:** A row of checkboxes for Normal, Offnormal, Fault, and Alert, all of which are checked.
- Route Acks:** A dropdown menu set to 'true'.
- Status:** A text input field containing '{ok}'.
- Fault Cause:** An empty text input field.
- Default Time Range:** A dropdown menu set to 'Time Range' with a help icon.
- Preset On Normal:** A dropdown menu set to '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*.

Properties

In addition to the standard properties (**Status** and **Fault Cause**), these properties support an video alarm recipients.

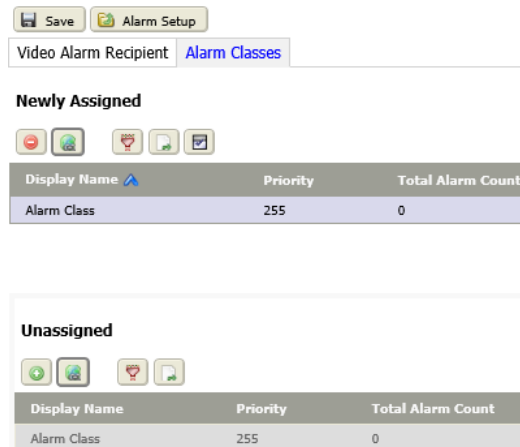
Property	Value	Description
Time Range	Start Time, End Time	Specifies when the Video Alarm Recipient is active in terms of time and day.
Start Time	Check boxes	
End Time	Check boxes	
Days of Week	check boxes	Defines the days of the week when the Video Alarm Recipient is active.
Transitions	check boxes	Provides option boxes to allow selection of specific alarm transitions to display. Only those transitions that are selected will be displayed - even though the alarms are still saved into the alarm history.
Route Acks	true or false (default)	true routes alarm acknowledgments (Acks) to this recipient; false does not route Acks to the recipient.

Property	Value	Description
Default Time Range	drop-down list and additional properties	Suggests a variety of pre-defined time ranges.
Preset on Normal	true (default) or false	true moves the camera to a preset position when a video alarm returns to normal.

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.



Figure 318 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.

Buttons

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

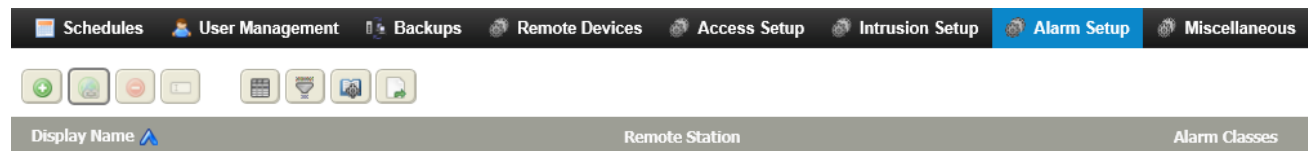
Column	Description
Display Name	Reports the name that describes the event or function.
Priority	Reports the priority level assigned to the alarm class for each component state transition (from normal to Offnormal, from normal to Fault, from offnormal, fault or alert to Normal, and from normal to Alert).The 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.

Column	Description
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Displays 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.




Figure 319 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.

Buttons

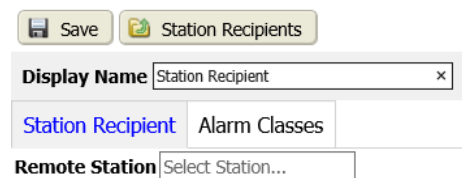
In addition to the standard buttons (Delete, Rename, Filter, Manage Reports, and Export), these buttons support station recipients:


-  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 320 Add New Station Recipient view



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.

Figure 321 Add New Station Recipient Alarm Classes tab

Newly Assigned

Display Name	Priority	Total Alarm Count
Alarm Class	255	0

Unassigned



Display Name	Priority	Total Alarm Count
Alarm Class	255	0
Alarm Class1	255	0

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.

Buttons

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 <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.

Column	Description
Unacked Alarm Count	Displays the total number of unacknowledged alarms.
Time of Last Alarm	Displays 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.

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.

Links

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	drop-down list	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.
Source Name	BQL script	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, to display here.
Alert Text	text	Defines a description that is associated with an alert.
To Fault Text	text	Defines the text to display when the alarm source transitions to a fault state.
To Offnormal Text	text	Defines the text to display when the alarm source transitions to an offnormal state.
To Normal Text	text	Defines the text to display when the alarm source transitions to a normal state.
Hyperlink Ord	ORD	Defines an ORD, a BQL query or a path to associate with an alarm status on the point you are configuring. When an alarm is reported in the console, the Hyperlink button activates using this path. Click the folder icon to browse to the file to link to. Click the arrow icon to the right of the folder icon to test the ORD.
Sound File	file path	Defines the path to a sound file that executes when the current point is in an alarm state. In <i>Wb Web Profile</i> mode (non <i>Hx</i> mode) you can browse to the file, and click an 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.
Meta Data	read-only	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 322 Alarm Source Exts view with Edit Alarm Class window



Station Name	Source Name	Display Name	Alarm Class	Alarm State	Status
entSecurity901		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 Display Name 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}, {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.

Figure 323 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.

Properties

Property	Value	Description
Alarm Class	drop-down list	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.
Source Name	BQL script defaults to <code>%parent.displayName%</code>	Displays the name of the alarm source. If you use the default, the this property shows the display name of the alarm extension parent. You can edit this script or type in a literal string to display.
To Fault Text	text	Defines the text to display when the alarm source transitions to a fault state.
To Offnormal Text	text	Defines the text to display when the alarm source transitions to an offnormal state.
To Normal Text	text	Defines the text to display when the alarm source transitions to a normal state.
Hyperlink Ord	ORD	Defines an ORD, a BQL query or a path to associate with an alarm status on the point you are configuring. When an alarm is reported in the console, the Hyperlink button activates using this path. Click the folder icon to browse to the file to link to. Click the arrow icon to the right of the folder icon to test the ORD.
Sound File	file path	Defines the path to a sound file that executes when the current point is in an alarm state. In <i>Wb Web Profile mode</i> (non <i>Hx mode</i>) you can browse to the file, and click an 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	read-only	Displays additional information about the alarm source when available.

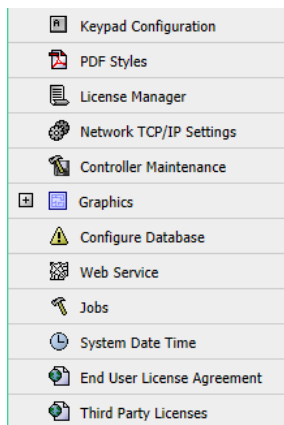
Chapter 12 Controller (System) Setup–Miscellaneous

Topics covered in this chapter

- ◆ Keypad Formats (Keypad Configuration) view
- ◆ Add New (or edit) Keypad Format view
- ◆ Pdf Styles view
- ◆ Add New (or edit) PDF Styles view
- ◆ License Manager view
- ◆ Network TCP/IP Settings view
- ◆ Maintenance view (Server)
- ◆ Configure Database view, Database Services tab
- ◆ Web Service view
- ◆ Job Service view
- ◆ System Date Time Editor view
- ◆ End User Licenses Agreement view
- ◆ Third Party Licenses view
- ◆ Controller TimeServers Settings
- ◆ Supervisor TimeServers Settings

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.

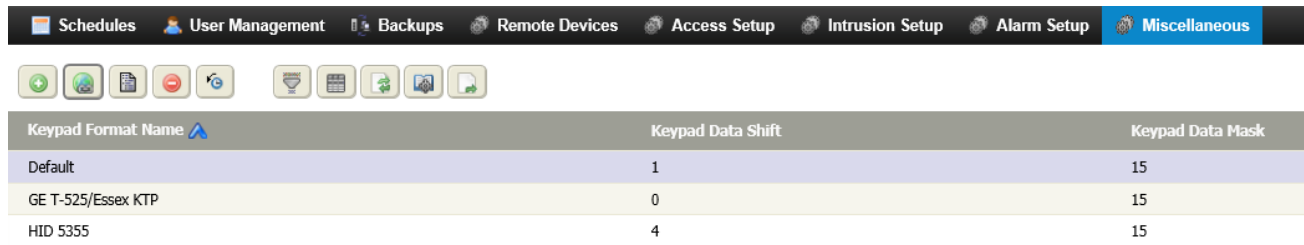
Figure 324 Miscellaneous menu



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.

Figure 325 Keypad Formats view



To access this view, select **Keypad Configuration** from the **Controller (System) Setup→Miscellaneous** menu.

Buttons

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 326 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.

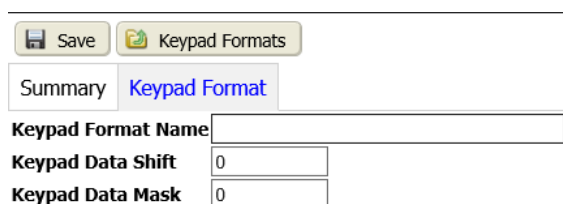
Table 75 Keypad Format columns

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 327 Add New Keypad Format view



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.

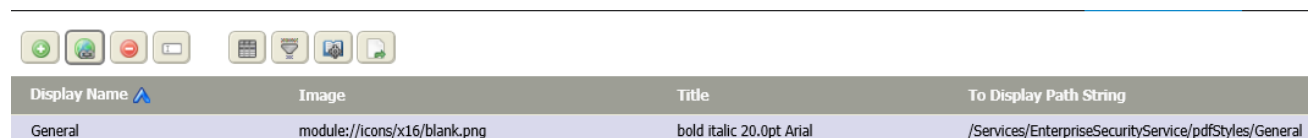
Summary tab

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.

Figure 328 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/General

This view opens when you click the **Pdf Styles** menu item, under the **Controller (System) Setup→Miscellaneous** menu.

Buttons

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.

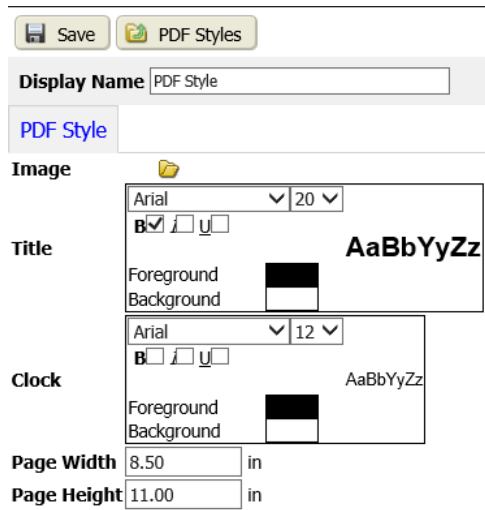
Columns


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.

Figure 329 Add Pdf Style view



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).

Links

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.

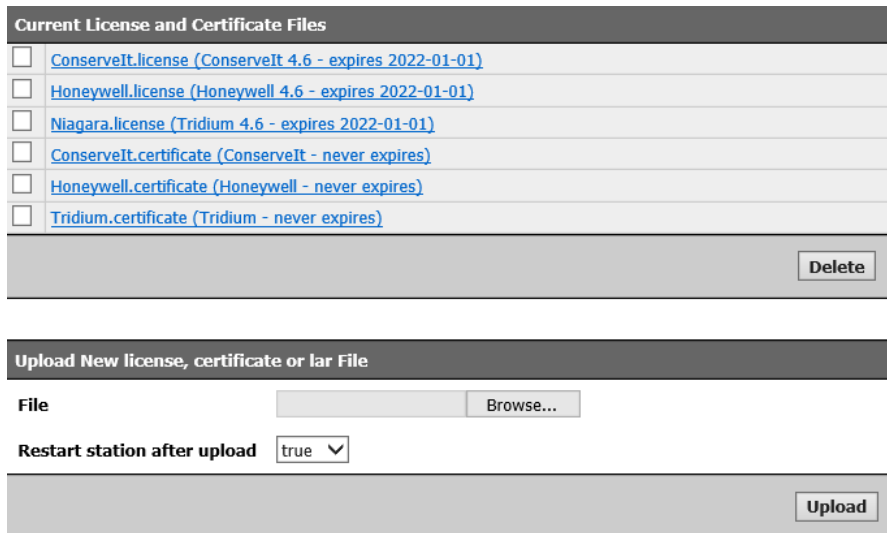
Properties

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.
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.

Figure 330 License Manger view



This view opens when you select **Controller (System) Setup→Miscellaneous→License Manager** from the main menu.

License view sections

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 331 Display Names and Network Settings (Supervisor view)

Display Names

Station Display Name

System Display Name

Station Name Settings (Changes to these settings require a restart the station to take effect)

Station Name

Network Settings (Changes to these settings require a reboot to take effect)

Host Name

Use IPv6

Domain

IPv4 Gateway

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	<input type="text" value="Enabled"/>
DHCPv4	<input type="text" value="Disabled"/>
IPv4 Address	<input type="text" value="172.31.66.10"/>
IPv4 Subnet Mask	<input type="text" value="255.255.252.0"/>
IPv6 Support	Yes
IPv6 Enabled	<input type="text" value="Enabled"/>
Obtain IPv6 Settings Automatically	<input type="text" value="Yes"/>
IPv6 Address	<input type="text" value="fe80::ee11:27ff:fea8:fa0"/>
IPv6 Network Prefix Length	<input type="text" value="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 332 Display Names view

Display Names

Station Display Name

System Display Name

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 System Display Name . The Station Display Name is unique for each controller. NOTE: This name takes priority over the Station Name and displays in the interface when both names are defined. The station n displays if no Station Display Name 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 Station Display Name . 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 333 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 334 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"/>

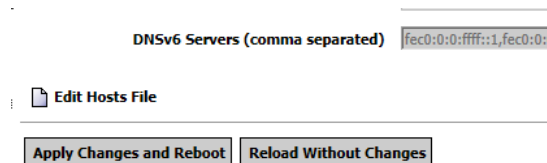
Property	Value	Description
ID, Description, Physical Address	read-only	Report identifying information about the interface.
Adapter Enabled	Enabled (default) or Disabled	Brings the adapter on line and takes it offline.
DHCPv4	Enabled or Disabled (default)	Turns use of this protocol (Dynamic Host Configuration Protocol), version 4, on and off.
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 (,).

Property	Value	Description
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.
IPv6 Network Prefix Length	defaults to zero (0)	Defines the node in an 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 335 Final Network Settings properties

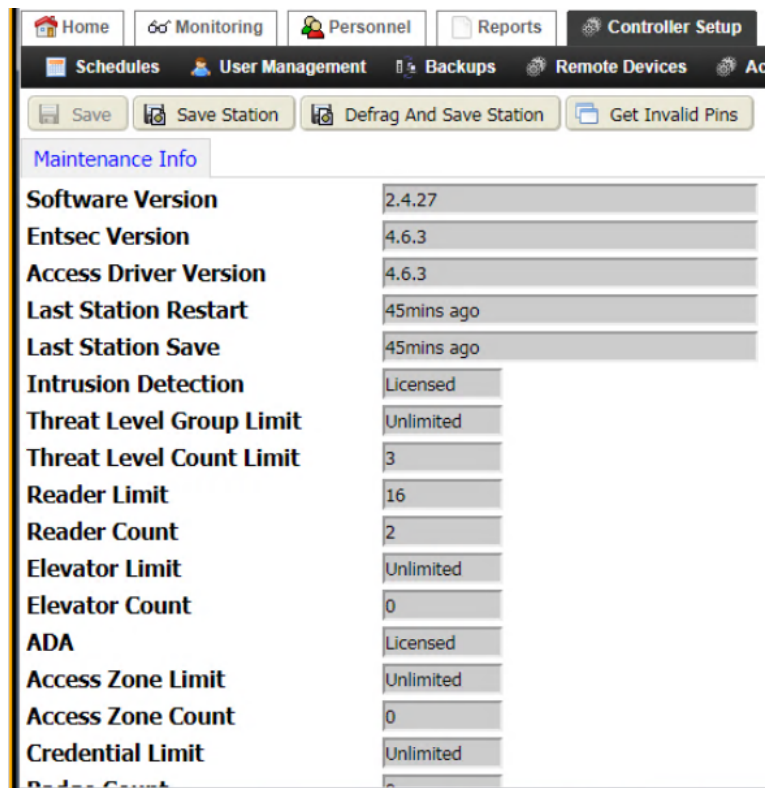


Property	Value	Description
Edit Hosts File	icon; when you click it opens a blank text file	Opens the Hosts File editor. The operating system uses this plain text file to map host names to IP addresses. It is stored in the Windows folder. This utility provides an easy way to edit it. You can type directly into this view to edit the hosts file and click the Save button at the bottom of the view to save changes.
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.

Figure 336 Server Maintenance view



Open this view by selecting **Controller Setup**→**Miscellaneous**→**Server Maintenance**.

Links

- **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 re-starts 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).

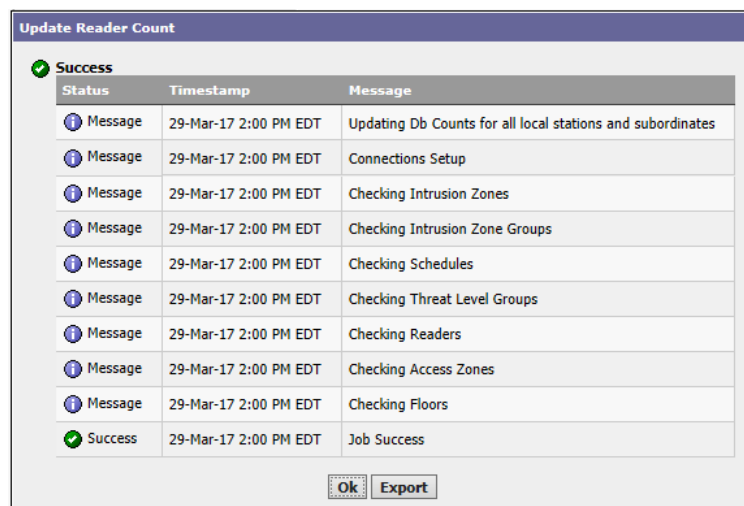
Property	Value	Description
Last Station Restart	read-only	Displays the time, in days and hours, since the last station restart.
Last Station Save	read-only	Displays the time, in hours and minutes, since the last station save.
Intrusion Detection	read-only	Indicates if the Intrusion Detection feature 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.
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	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. NOTE: If you happen to be over the license limit, the following error message displays: <code>javax.baja.license.LicenseException: Credential License Limit Reached: <limit></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.
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.

Property	Value	Description
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 true is selected and saved, this property causes the Guided Tour to display at the top of the interface when a user logs on the system. When false is selected and saved, the Guided Tour does not display.
Coalesce Alarms	true or false	When true 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 false. When false is selected and saved, the Coalesce Alarms does not combine the alarms, but sends individual alarm notifications. NOTE: 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.

Update Reader Count window

This window displays the received messages.

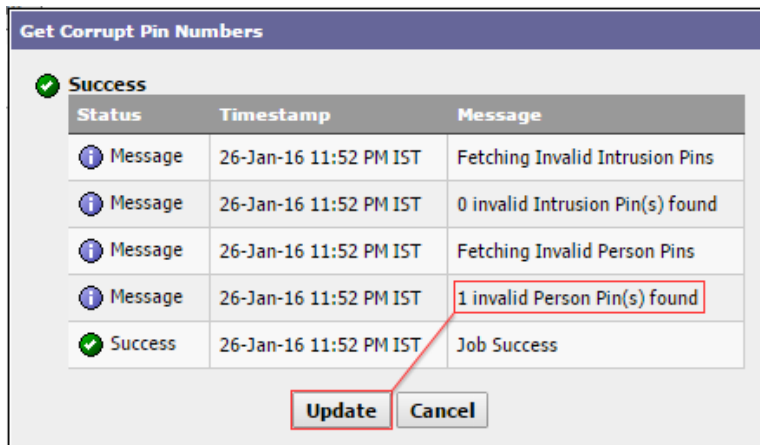
Figure 337 Update Reader Count window



Get Corrupt Pin Numbers window

This window displays a list of corrupt PIN numbers.

Figure 338 Get Corrupt Pin Numbers window

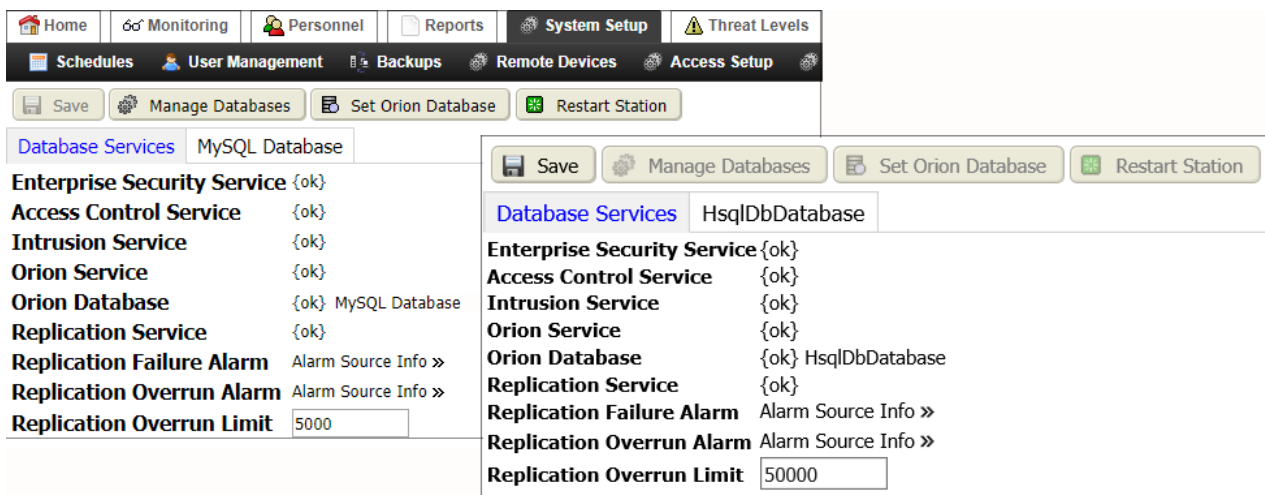


This window shows job status with time stamped messages that indicate if any invalid PINs are found. If one or more invalid PINs are found, then the window displays an **Update** button that you can click to launch a job that updates any PINs that are identified as invalid.

Configure Database view, Database Services tab

This view displays the station's database and network configuration settings.

Figure 339 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.

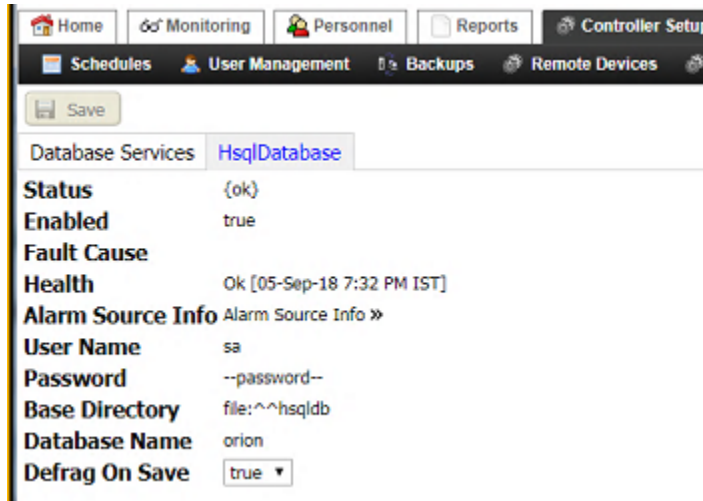
- **Restart Station** starts the current stations. This is necessary after configuring or reassigning a station database.

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 <i>Alarm Setup</i> topic of the PDF and in the help system (search for Alarm Source Info).
Replication Overrun Alarm (This alarm occurs when the deletion table record count is greater than the Replication Overrun Limit 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 340 HsqlDbDatabase properties



You access this view from the main menu by clicking **Controller Setup**→**Miscellaneous**→**Configure Database**, followed by clicking the **HsqlDbDatabase** tab.

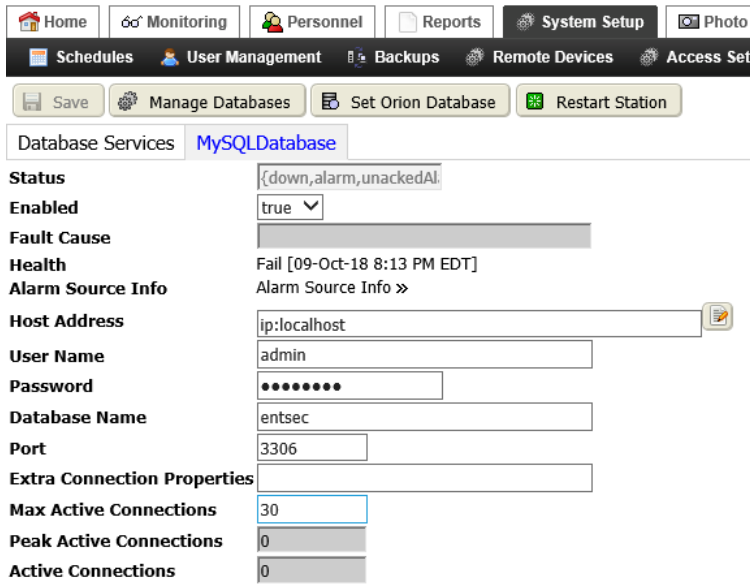
In addition to the standard properties (Status, Enabled, Fault Cause, Health, and Alarm Source Info), these properties support an HSQL database.

Property	Value	Description
User Name	read-only	Defines the user name credential with which to log in to the database.
Password	read-only	Defines the password credential required to log in to the database.
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 <code>hsqldb</code> , the path would be: <code>file:^^hsqldb</code> .
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 Base Directory and Database Name .
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.

Figure 341 MySQL database properties



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.

Properties

In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support the MySQL database.

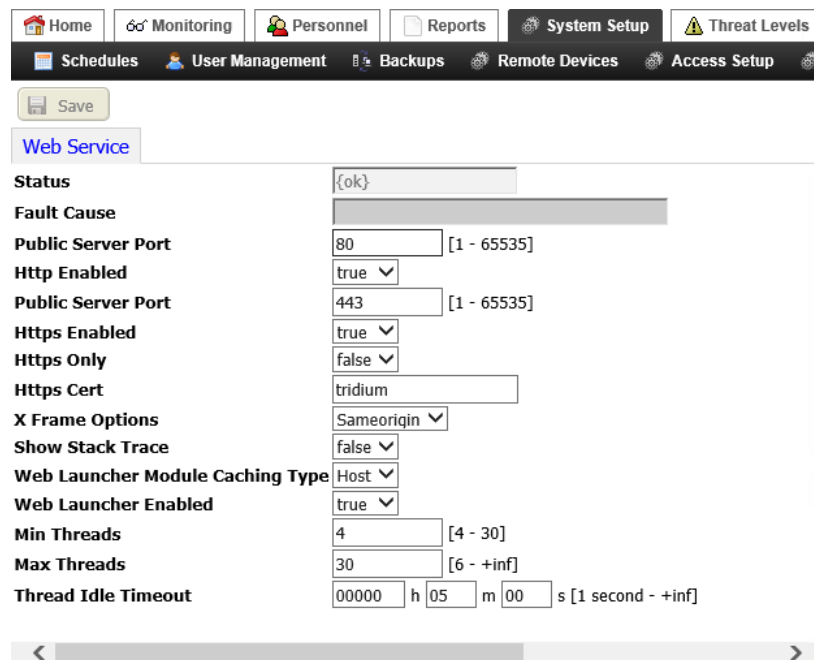
Property	Value	Description
Host Address	IP address	Defines the IP address of the computer platform where the database resides.
User Name	text	Defines the user name credential with which to log in to the database. For MySQL databases, this should be a name other than the default, "root," which only connects to a database hosted on localhost.
Password	two properties	The Password property defines a password that is used to log in to the database. The Confirm property must be an exact match to the Password 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 Base Directory and Database Name .
Port	number	Specifies the port to use when connecting to the database. Common default values are: HsqlDbDatabase - no port is specified because this rdb is for local database use only. MySQLDatabase - Port 3306 SqlServerDatabase - Port 1433

Property	Value	Description
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.

Figure 342 Web Service view



You select this view by choosing **Controller (System) Setup**→**Miscellaneous**→**Web Service** from the main menu.

Properties

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)	Defines the port that the HTTP service listens on.
Http Enabled	true or false	Turns the processing of HTTP requests on (true) and off (false).

Property	Value	Description
Public Server Port	number (defaults to 443)	Defines the port that the HTTPS service listens on.
Https Enabled	true (default) or false	
Https Only	true or false (default)	true redirects any attempt to connect using a connection that is not secure (Http alone) to Https. false, does not redirect attempts to connect using Http alone.
Https Cert	text	Sets the certificates that the user wants to use. By default the certificate is set to tridium.
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 <frame> or <iframe>, 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 only if the top-level origin FQDN (fully-qualified-domain-name) does not exactly match FQDN of the subframe page that demanded the Sameorigin restriction. This is considered a safe practice.</p> <p>Any allows XFS and Cross-Site Scripting (XSS). This is the least safe choice.</p>
Show Stack Trace	true or false	true shows exception stack traces in error responses when available. false disables exception stack traces in error responses.
Web Launcher Module Caching Type	drop-down list; defaults to Host	<p>Determines how a client using the Web Launcher caches modules.</p> <p>Host results in a folder and the downloading of installation modules to the module folder. This creates multiple folders of downloaded modules that negatively affect platform memory usage.</p> <p>User results in one cache per host visited (user)- one shared cache per user. This option results in the creation of a .share-dModuleCache folder. The system then downloads to a sub-folder at this location. This option minimizes the memory required when running in a controller.</p>
Web Launcher Enabled	true (default) or false	Enables (true) and disables (false) the use of the Web Launcher.
Min Threads	number (defaults to 4)	Ensures that at least four threads process at a time.

Property	Value	Description
Max Threads	number (defaults to 30)	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 large-job scalability and allows the local station's thread pool to grow uncapped.
Thread Idle Timeout	hours minutes seconds (defaults to five hours)	Configures the amount of idle time to elapse before a thread times out.

Job Service view

This view shows a table listing of all the jobs that have run on the local station.

Figure 343 view

The screenshot shows the 'JobService' view. At the top, there is a navigation bar with tabs for Home, Monitoring, Personnel, Reports, Controller Setup, and Threat Levels. Below this is a secondary menu with Schedules, User Management, Backups, Remote Devices, Access Setup, Intrusion Setup, Alarm Setup, and Miscellaneous. The 'JobService' section has a title and a set of control buttons: a document icon, a triangle, a red circle with a slash, a pause icon, a funnel, and a download icon. Below these buttons is a table with the following data:

Job Name	Progress	Job State	Start Time	End Time
✓ Replication	100	Success	22-Aug-18 2:00 AM EDT	22-Aug-18 2:00 AM EDT
✓ Station Save	100	Success	21-Aug-18 6:03 PM EDT	21-Aug-18 6:03 PM EDT
✓ Replication	100	Success	21-Aug-18 2:00 AM EDT	21-Aug-18 2:00 AM EDT
✓ Station Save	100	Success	20-Aug-18 6:04 PM EDT	20-Aug-18 6:04 PM EDT
✓ Replication	100	Success	20-Aug-18 2:00 AM EDT	20-Aug-18 2:00 AM EDT
✓ Station Save	100	Success	19-Aug-18 6:04 PM EDT	19-Aug-18 6:04 PM EDT
✓ N Discovery	100	Success	16-Aug-18 11:58 AM EDT	16-Aug-18 11:58 AM EDT
✓ N Discovery	100	Success	16-Aug-18 11:56 AM EDT	16-Aug-18 11:57 AM EDT

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.

Buttons

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.

Column	Description
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 344 System Data Time Editor view

System Time EDT

Time Zone

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.

Figure 345 NTP view in a controller station

The screenshot shows the 'Controller Setup' interface with the 'Time Servers Settings' view. The 'Settings' section contains five dropdown menus: 'Enabled' (false), 'Sync Local Clock to NTP' (true), 'Sync Time At Boot' (false), 'Use Local Clock as Backup' (false), and 'Generate NTP Statistics' (false). The 'Time Servers' section features a table with columns: 'Address', 'Peer Mode', 'Burst', 'Preferred', 'Min. Poll Interval', and 'Max. Poll Interval'. A single row is visible with an empty 'Address' field, 'Peer Mode' set to 'Server', 'Burst' set to 'false', 'Preferred' set to 'false', 'Min. Poll Interval' set to '6 log2 s', and 'Max. Poll Interval' set to '10 log2 s'. 'Refresh' and 'Save' buttons are located at the bottom right of the table area.

To access this view, click **Controller Setup**→**Miscellaneous**→**TimeServers Settings**

Settings properties

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 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)	If true, 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. A true 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.
Generate NTP Statistics	true or false (default)	If true, 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 Views SpyRemote . Keep in mind that the ntpd is a QNX process; thus Niagara has no control over what it reports.

Time Servers properties

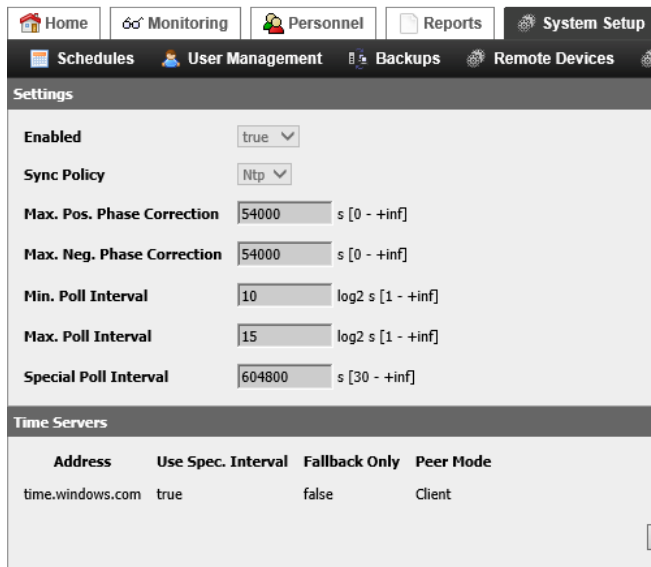
These properties become available when you click the Add button.

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	Defines the type of server: <i>Server</i> indicates that the controller platform is in a subordinate role to the server with regard to time synchronization. <i>Peer</i> indicates that the platform functions as an equal with the server with regard to time synchronization.
Burst	Drop-down list, <i>true</i> or <i>false</i> (default)	<i>false</i> by default. If <i>true</i> , 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, <i>true</i> or <i>false</i> (default)	If <i>true</i> , 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).

Supervisor TimeServers Settings

This view configures NTP (Network Time Protocol) properties in a Supervisor PC.

Figure 346 NTP view in a Supervisor station



To access this view, click **System Setup**→**Miscellaneous**→**TimeServers Settings**

Settings properties

NOTE:

The Windows 32 time service supports two registry entries, the Max. Pos. Phase Correction and the Max. Neg. Phase Correction (listed below). These entries restrict the samples that the time service accepts on a local computer when those samples are sent from a remote computer. When a computer that is running in a steady state receives a time sample from its time source, the sample is checked against the phase correction boundaries that the MaxPosPhaseCorrection and MaxNegPhaseCorrection registry entries impose. If the time sample falls within the limits that the two registry entries enforce, this sample is accepted for additional processing. If the time sample does not fall within these limits, the time sample is ignored.

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 Policy	read-only drop-down list	Reports that the system uses Ntp (Network Time Protocol) to synchronize the time.
Max. Pos. Phase Correction	seconds (defaults to 54000)	See note, above.
Max. Neg. Phase Correction	seconds (defaults to 54000)	See note, above.
Min. Poll Interval	seconds (defaults to 10)	Minimum poll interval for NTP messages, from 4 to 16. Note 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).

Property	Value	Description
Max. Poll Interval	seconds (defaults to 15)	Maximum poll interval for NTP messages, from 10 to 17. Note 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).
Special Poll Interval	seconds (defaults to 604800)	To change the period at which Windows attempts to synchronize with the NTP reference, modify the parameter Special Poll Interval . This allows you to specify a period at which the operating system attempts to synchronize with the NTP reference. It specifies the synchronization period in seconds. The default is 604800 seconds, or 7 days. A generally accepted polling period of once every hour, or 3600 seconds, is reasonable.

Time Servers properties

These properties become available when you click the Add button.

Property	Value	Description
Address	domain	Fully qualified domain name, IP address, or host files alias for the NTP time server.

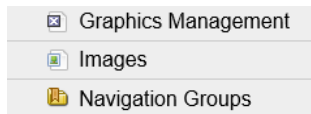
Chapter 13 Controller (System)–Miscellaneous Graphics

Topics covered in this chapter

- ◆ Graphics view (Graphics Management)
- ◆ View Graphic
- ◆ Graphic Editor view
- ◆ Images view
- ◆ Add New Image view
- ◆ Display Image view
- ◆ Navigation Groups view
- ◆ Add New (or edit) Nav Group view

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 347 Graphics menu



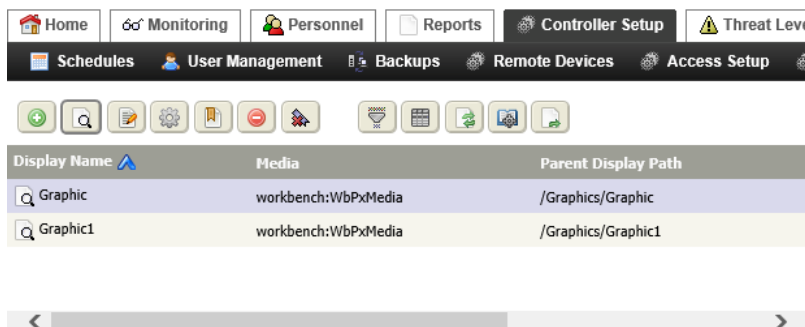
You access this menu by clicking the **Controller (System) Setup→Miscellaneous→Graphics** menu item.

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.







Figure 348 Graphics view



This view opens when you select **Controller (System) Setup→Miscellaneous→Graphics→Graphics Management** from the main menu.

Buttons

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.

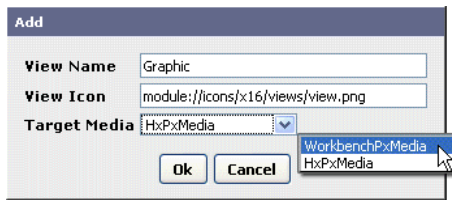
Columns

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 349 Add a new graphic window

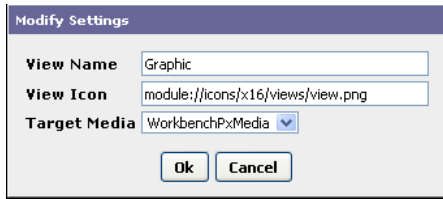


Property	Value	Description
View Name	text	Identifies the name of the graphic.
View Icon	file path	Defines the location of an icon to represent the graphic.
Target Media	drop-down list	Identifies where the graphic will be used: Workbench or the web (HxPxMedia).

Modify Settings window

This window configures graphics properties.

Figure 350 Modify Settings window properties



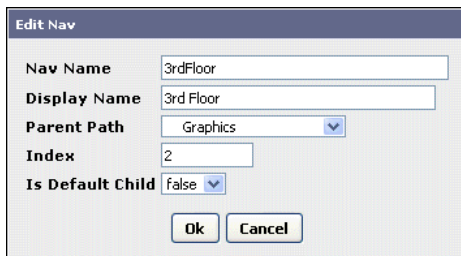
You access these properties by selecting a row in the **Graphics** view table followed by clicking the Modify Settings button (⚙️).

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 351 Edit Nav window properties



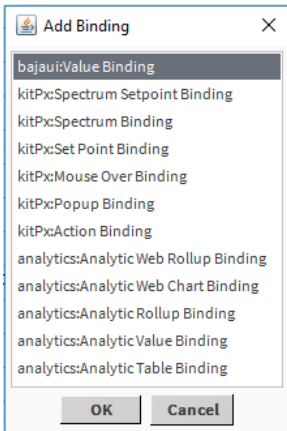
You access these properties by selecting a row in the **Graphics** view table followed by clicking the Edit Nav button (📁).

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 352 Types of bindings

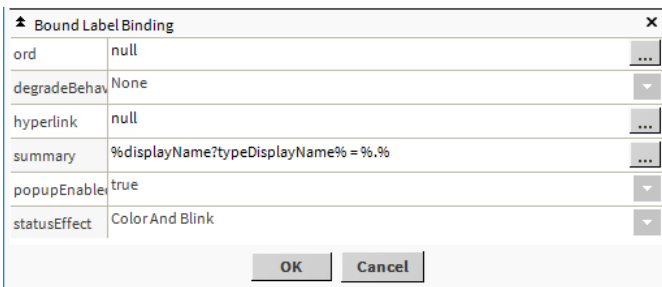


To access this menu in the Graphic Editor, open the Widget Tree side bar, double-click the object in the Widget Tree or on the canvas.

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 353 Bound label binding properties



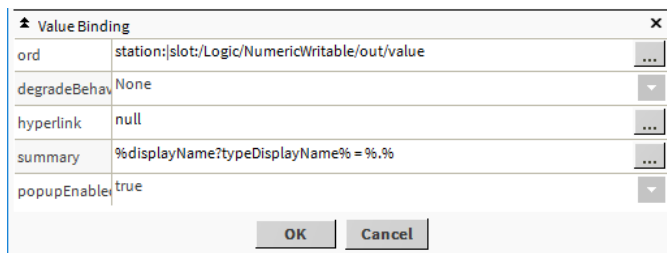
To access these properties after dragging a **BoundLabel** from the **kitPx** palette to the Px Editor, double-click the bound label. These properties are toward the bottom of the list.

Property	Value	Description
Ord	Defaults to <code>null</code>	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound. In a Popup binding this path that designates the component view to display in the popup window.
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	Specifies a display name for the widget as text or by means of a script.

Property	Value	Description
	%displayName%= %.%	
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.
Status Effect	three options	Configures what happens when the status of a bound value changes: Color changes the background color. Color and blink changes the background color and causes the value to blink. None disables any effects when the status of a bound value changes.

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.



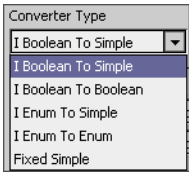
This pop-up opens when you right-click an object on a PX grid.

Property	Value	Description
Ord	Chooser; defaults to 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	drop-down list; de- faults to None	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 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.

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 354 Types of converters



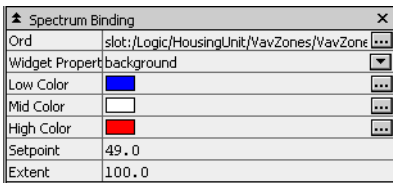
The following types of converters are available when using a value binding:

- 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 355 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 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 Mid Color property.

Property	Value	Description
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 High Color property. As the value decreases below the setpoint, the color changes, approaching the color set by the Low Color 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 Mid Color 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 Mid Color 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 356 Set Point Binding properties

Property	Value
Ord	station:/slot:/Logic/HousingUnit/AirHandler/SetpointTer...
Hyperlink	null
Summary	%displayName% = %%,%
Popup Enabled	true
Widget Event	actionPerformed
Widget Property	value

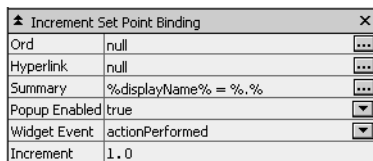
Property	Value	Description
Ord	Chooser; defaults to <code>null</code>	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Hyperlink	Chooser; defaults to <code>null</code>	Links to another object. When used, the link is active in the browser 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.

Property	Value	Description
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 357 Increment set point binding properties

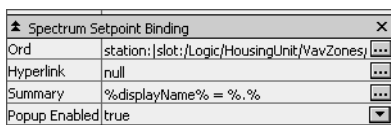


Property	Value	Description
Ord	Chooser; defaults to null	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Hyperlink	Chooser; defaults to null	Links to another object. When used, the link is active in the browser or in the graphic view.
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.
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 358 Spectrum set point binding properties

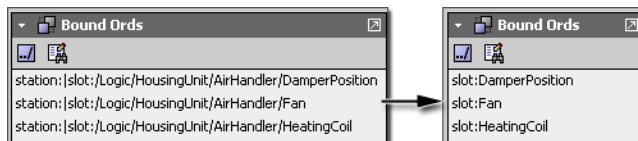


Property	Value	Description
Ord	Chooser; defaults to null	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Hyperlink	Chooser; defaults to null	Links to another object. When used, the link is active in the browser or in the graphic view.
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 359 Absolutely bound ORDs and relatively bound ORDs



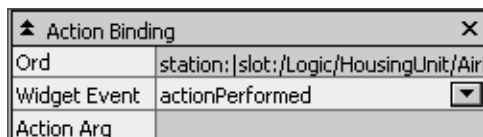
An absolute ORD, such as: `station:|slot:/Logic/HousingUnit/AirHandler/DamperPosition` defines the absolute path to a single unique DamperPosition regardless of where the Graphic file or the parent component is located. If the same Graphic file is attached to a view that belongs to a different component, 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 360 Action Binding properties

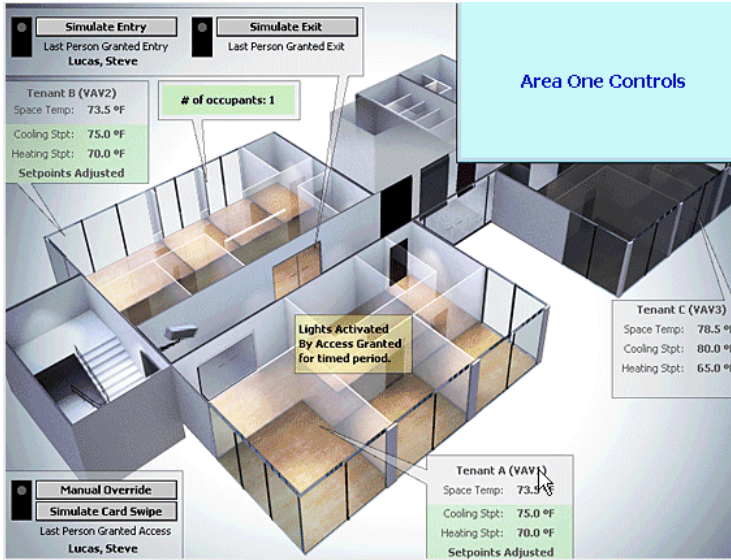



Property	Value	Description
Ord	Chooser; defaults to null	Defines the location of the data value to bind to the widget. This is a required property for the widget to be bound.
Widget Event	drop-down list	Defines the action to perform on the binding of the target component when an event is fired by the parent widget.
Action Arg	read-only	

View Graphic

This view represents the inside of a building.

Figure 361 Example graphic view



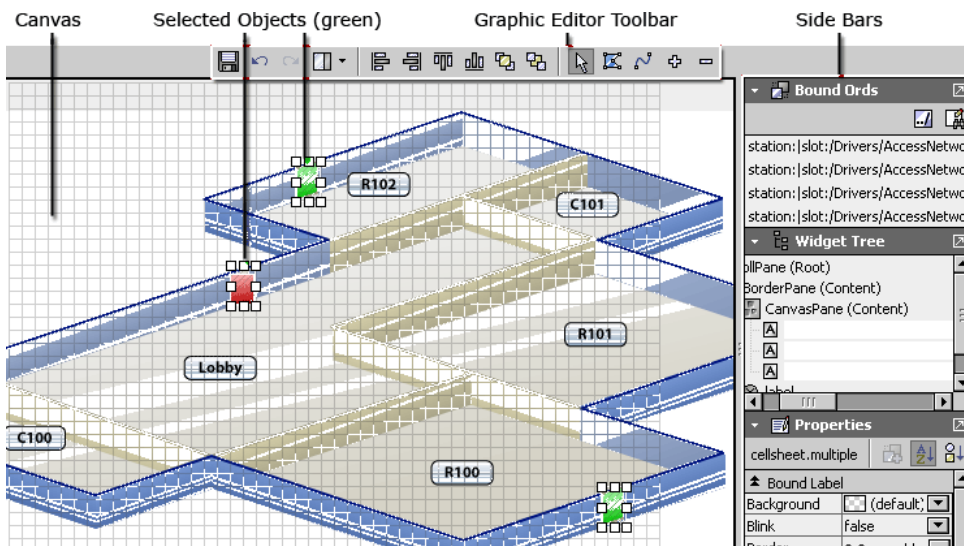
You access this view from the Graphics view by double-clicking the Display Name record in the Graphics view or by selecting the record and clicking the View Graphic button ().

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 362 Graphic Editor view



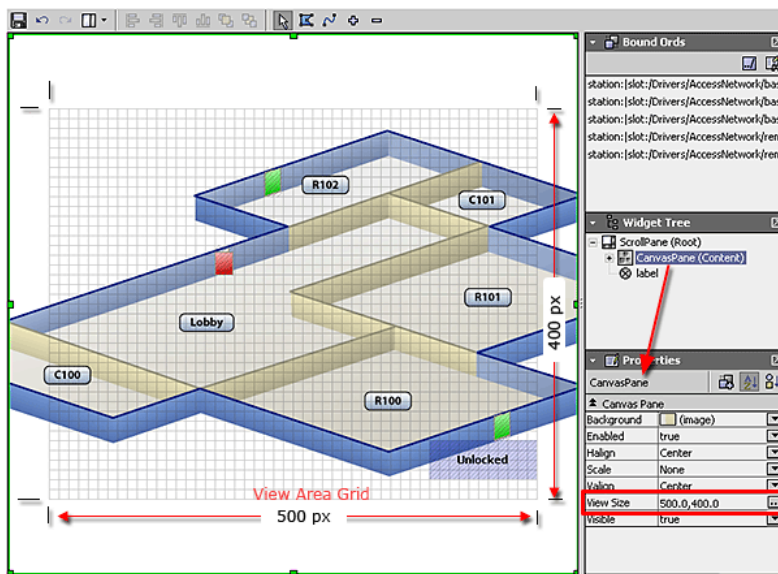
You access this view from the main menu by clicking **Controller (System) Setup→Miscellaneous→Graphics→Graphics Management** followed by clicking the New button (🟢) or selecting an existing graphic and clicking the Graphic Editor button (📄)

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 363 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.

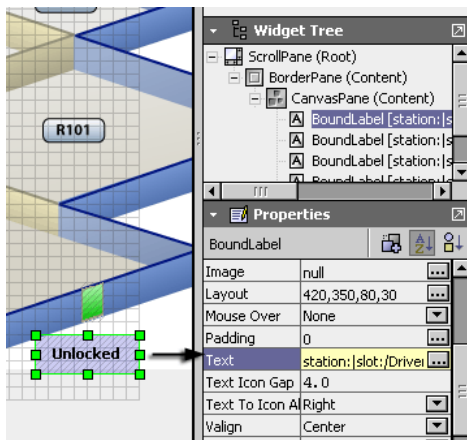
Property	Value	Description
Scale	drop-down list, defaults to <code>None</code>	Increases and decreases the background image proportionally.
Valign	drop-down list, defaults to <code>Center</code>	Aligns the background image vertically.
View Size	Chooser	Defines the dimensions of the background graphic.
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 364 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 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: <code>Right</code> , <code>Left</code> , <code>Center</code>
Valign	drop-down list	Defines vertical alignment: <code>Top</code> , <code>Bottom</code> , <code>Center</code>

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 365 Default Graphic Editor Toolbar buttons

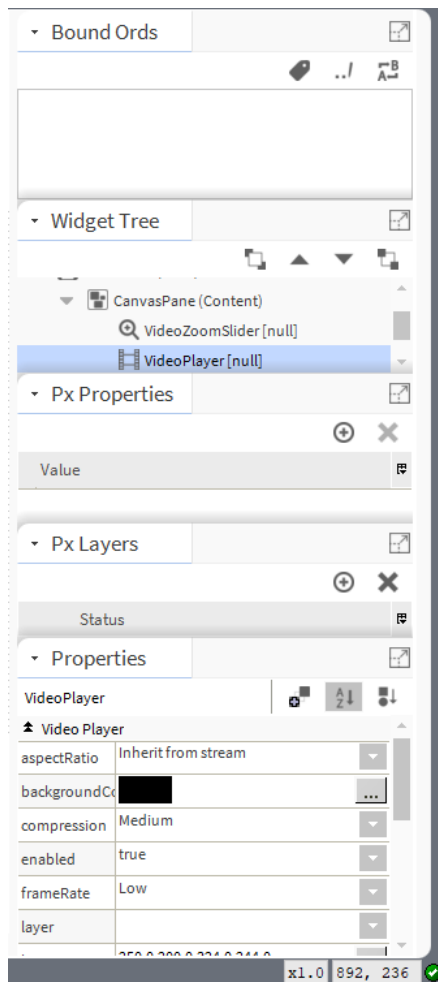


-  Save saves the graphic in the station database.
- Undo and Redo perform the tasks their names imply.
- Right side bar menu opens a drop-down menu of side bar options for the Graphic Editor.
- Alignment options align the selected widgets and objects at their left, right, top and bottom edges.
- The 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 366 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 367 Graphic Editor popup menu - available video cameras

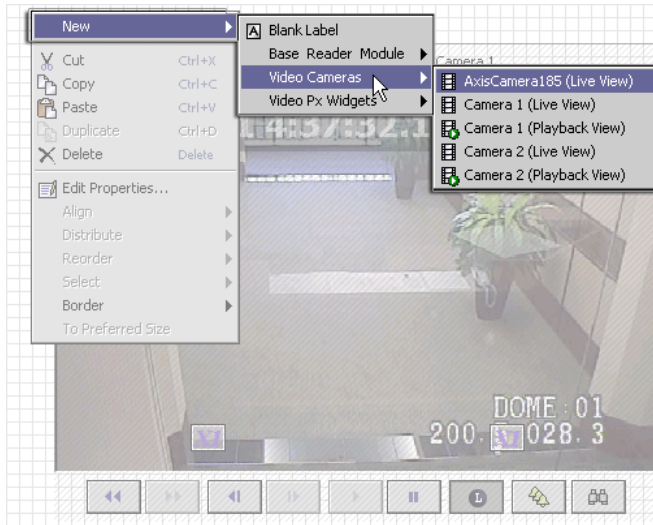


Figure 368 New menu items

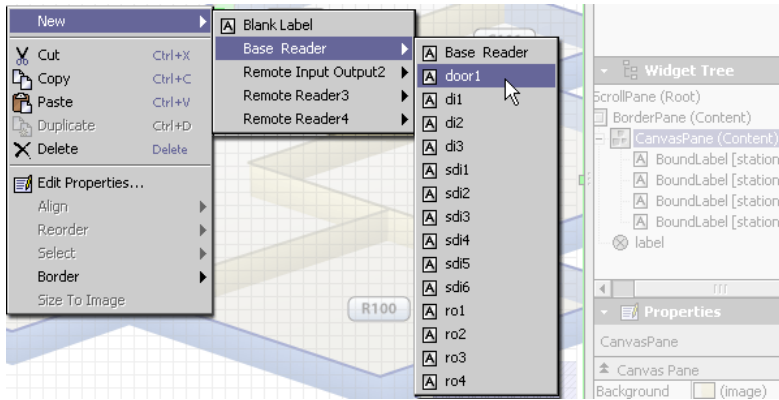
Menu item	Description
Blank Labels	Selects a standard Px label widget, which you use to annotate the graphic.
Base Reader Module, Remote Reader Module	These menus are context sensitive and list widgets that represent the devices available under each module. Adding one to the graphic adds a representation of the device to the graphic.
Video Cameras	This list of widgets represents the camera(s) connected to your 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 Player-Control 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 369 Graphics Editor popup menus



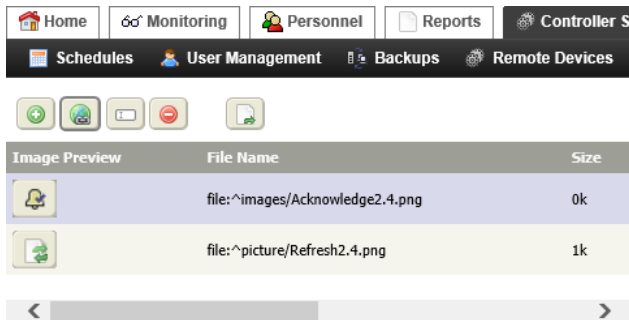
The popup menu also provides many other context-sensitive commands, including the ability to add a border pane to a selected object.

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.

Figure 370 Images view



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

Buttons

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 371 Add New Image view



Property	Value	Description
File Path	file path (defaults to <code>^images</code>)	Defines the folder under the station for storing uploaded image files. The <code>^</code> 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 372 Display Image view

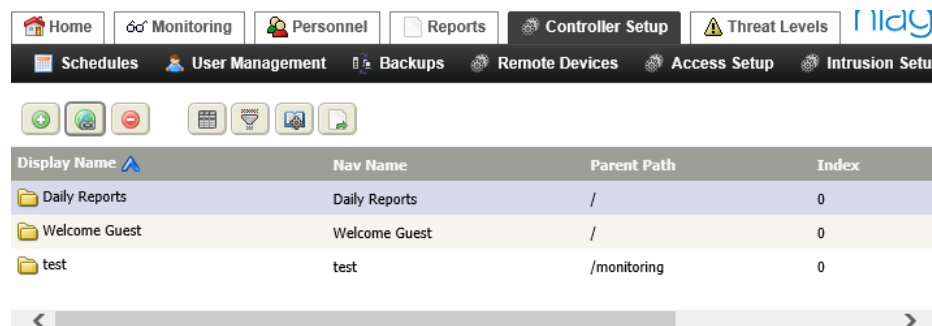
file:^graphics/edit.png



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 373 Navigation Groups view



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 374 Add New Nav Group view

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 Display Name is specified. You may want to use this property for a design-logical name and use the Display Name as a more user-friendly name.
Display Name	text	Defines a name that describes the event or function.
Parent Path	drop-down list	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. For example, to place a menu item under the Remote Devices submenu, choose the Remote Devices option in this property.
Icon	file path	Assigns an appropriate icon to the menu view for the nav group. This requires that you point to an existing icon in your For example, using the following path: module://icons/x16/folder.png displays a folder icon in a new nav group menu .
Index	number	Defines where, in the parent to display this menu item. The first position (from left to right, or top to bottom) is "0", then "1", "2", and so on.

Chapter 14 Threat Levels

Topics covered in this chapter

- ◆ Threat level groups view
- ◆ Add New (or edit) Threat Level Group view
- ◆ Threat Level Setup view

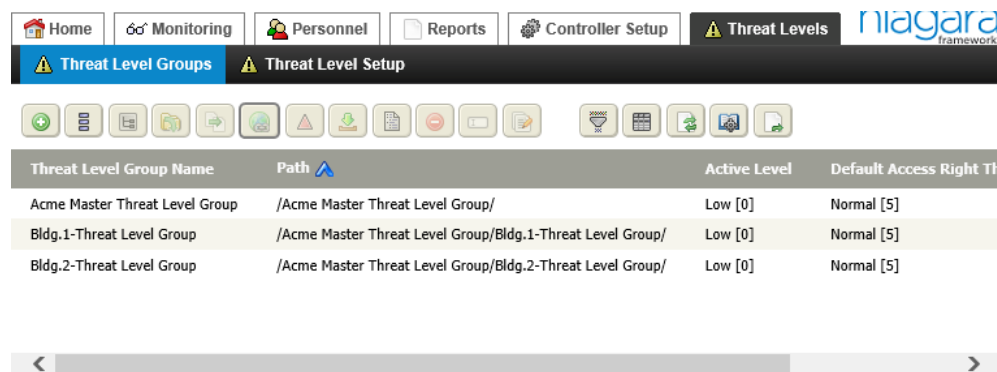
A threat level defines a range of operational values (threat levels) related to overall building security. Threat level groups define facility spaces for the purpose of managing perceived threats.

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.

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 375 Threat Level Groups view




To open this view, expand the **Threat Levels** node in the menu and click **Threat Level Groups**.

Buttons

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.

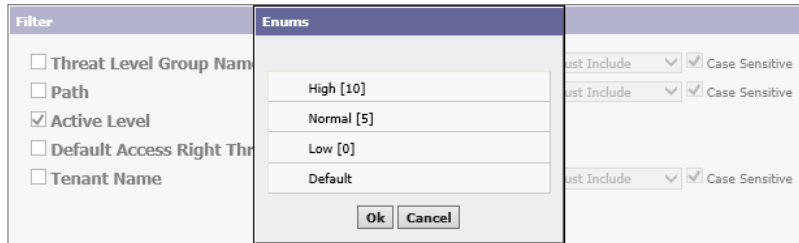
Figure 376 Threat Level Groups filter

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 377 Activate Threat Level window



The drop-down list levels default to:

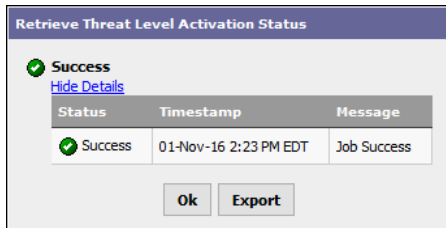
- Low [0]
- Normal [5]
- High [10]

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 378 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 76 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.

Figure 379 Add New Threat Level Group view

To open this view, click the **Add** button on the **Threat Level Groups** view.

Links

- **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:




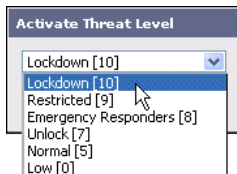



-  Save updates the database with the current information.
-  Threat Level Groups returns to the **Threat Level Groups** view.
-  Activate Threat Level opens a drop-down list of threat level group options. Choosing one of these options, followed by clicking **Ok** turns the threat level on.

Figure 380 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	Defines a name that describes the event or function.
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 Ref Chooser 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.
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	optional 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 381 Threat level group summary

The screenshot shows the 'Summary' tab of a Threat Level Group configuration. At the top, there is a toolbar with buttons for 'Save', 'Threat Level Groups', 'Activate Threat Level', 'Retrieve Active Status', 'Manage Devices', and 'Add Child'. Below the toolbar, the 'Summary' tab is selected, and the following properties are displayed:

- Threat Level Group** (Warning icon)
- Type:** Threat Level Group (Warning icon)
- Threat Level Group Name:** Threat Level Group
- Path:** /Threat Level Group/
- Active Level:** Low [0]
- Default Access Right Threat Level:** Normal [5]
- Tenant:**
- Hierarchy** (Link icon)
 - Threat Level Group** (Link icon)

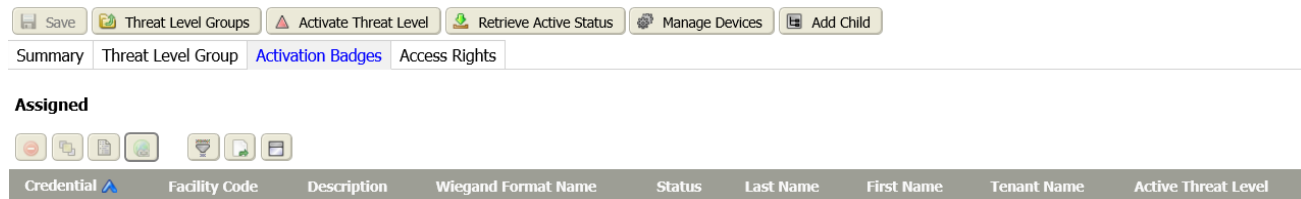
Some properties are not populated until you save the group. In the edit threat level group view, these properties display current information, including links to the appropriate edit view for a specific piece of information. For example, **Hierarchy**, **Remote Stations**, and **Activation Badges** properties 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.
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 382 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.

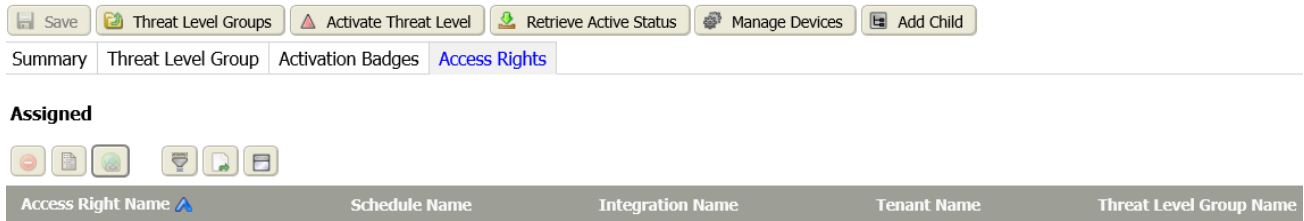
Table 77 Activation Badges table columns

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	Indicates the type or purpose of the badge.
Wiegand Format Name	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	Identifies the family name of the badge holder.
First Name	Identifies the given name of the badge holder.
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 383 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.

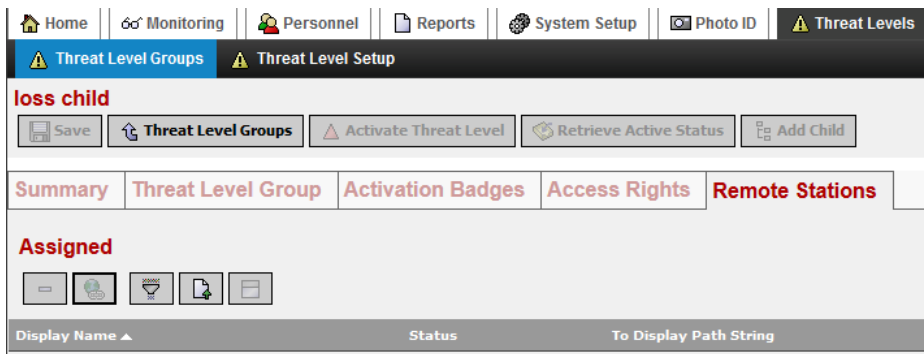
Table 78 Access rights tab table columns

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	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 assigned to this threat level group.

Remote Stations tab

This tab provides standard assign-mode controls for adding remote stations to a threat level group.

Figure 384 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.

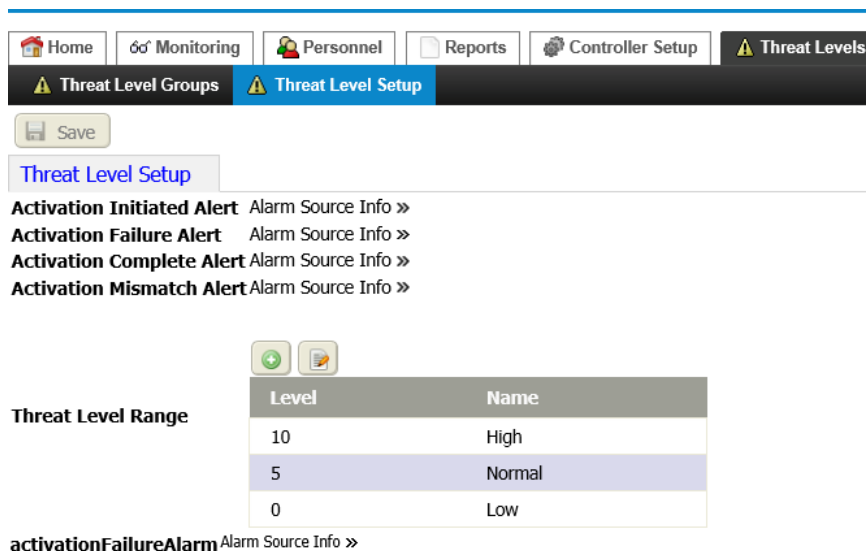
Table 79 Remote Stations table columns

Column	Description
Display Name	Reports the station name, which is usually its IP address.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}
To Display Path String	Reports the system path to the remote station. For example: /Drivers/Niagara/MyStation1.

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.

Figure 385 Threat Level Setup tab



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.

Activation alert and alarm links

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 Alert** 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.

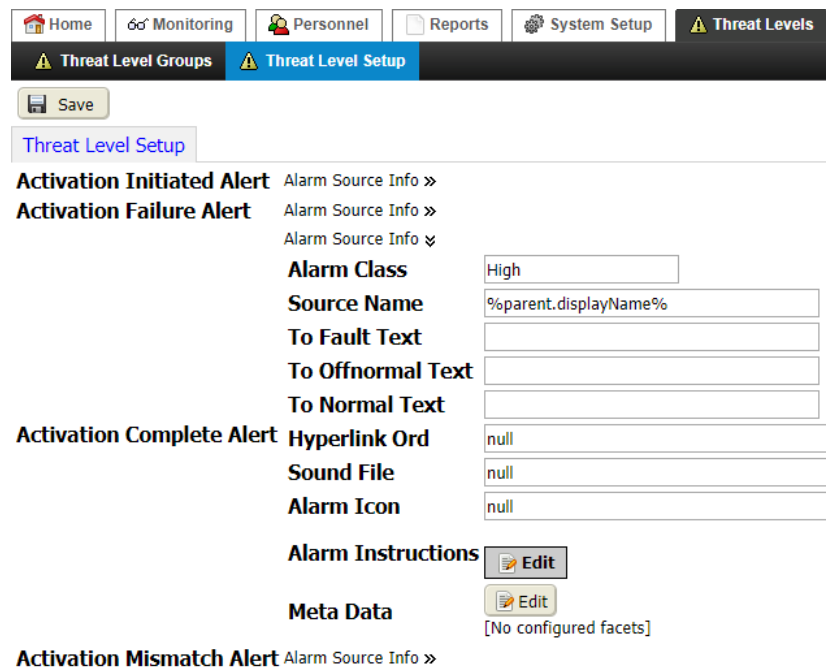
Column	Description
Level	Assigns an arbitrary number to create a threat level.
Name	Provides a description of the level.

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 386 Alarm Source Info adapted to threat levels



Home Monitoring Personnel Reports System 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 »
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.
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 387 Add threat level window

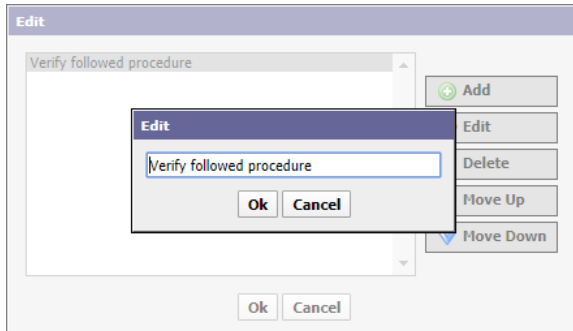
You access this window from the main menu by clicking **System setup**→**Threat Levels**→**Threat Level Setup**, and clicking the add button (🟢).

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 388 Edit alarm instructions windows

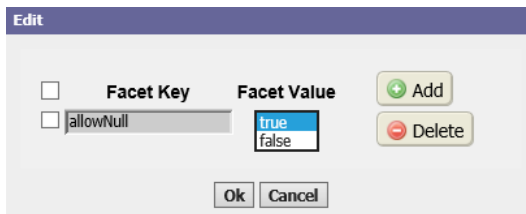


To access this window from the main menu, click **Threat Levels**→**Threat Level Setup**, expand an activation alert and click the **Edit** button next to **Alarm Instructions**.

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 389 Edit alarm metadata window



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 15 LDAP network driver views, tabs and windows

Topics covered in this chapter

- ◆ LDAP Network view
- ◆ Ldap Server view
- ◆ LDAP Audit History view
- ◆ Periodic Purge Schedule

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:

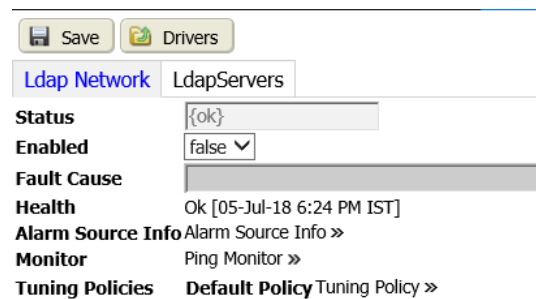
- Attribute discovery
- Attribute mapping to system properties
- The ability to ping the LDAP server.
- Import from the LDAP server

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.

Figure 390 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.

LDAP Network tab

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 Ping Monitor, page 408 .
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 Tuning Policy, page 408 .

Ping Monitor

Figure 391 Ping Monitor properties

Ping Monitor ▾

Monitor **Ping Enabled**

Ping Frequency h m s

Alarm On Failure

Startup Alarm Delay h m s

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.

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 392 LDAP Network Tuning Policy properties

Tuning Policy ▾

Min Write Time h m s [0 ms - +inf]

Max Write Time h m s [0 ms - +inf]

Tuning Policies **Default Policy** **Write On Start**

Write On Up

Write On Enabled

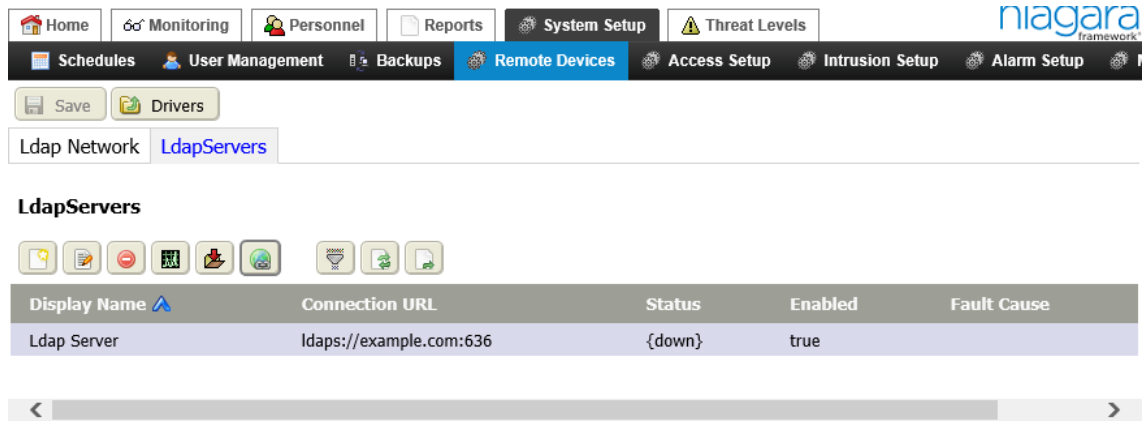
Stale Time h m s [0 ms - +inf]

Property	Value	Description
Min Write Time	hours minutes seconds	Specifies the minimum amount of time allowed between writes to writable proxy points, thus providing a method to throttle rapidly changing values so that only the last value is written. A value of zero (0) disables this rule causing all value changes to attempt to write.
Max Write Time	hours minutes seconds	If nothing else triggers a write to a proxy point, this property specifies the maximum amount of time to wait before rewriting the value. Any write action resets this timer. The default (zero) disables this rule resulting in no timed rewrites.
Write on Start	true (default) or false	Defines a writeable proxy point's behavior at station startup. true initiates a write when the station first reaches a steady state. false prevents a write when the station first reaches a steady state.
Write on Up	true (default) or false	Defines a writeable proxy point's behavior when the point and its parent device transition from down to up. true initiates a write when the transition occurs. false prevents a write when the transition occurs.
Write on Enabled	true (default) or false	Defines a writeable proxy point's behavior when its status transitions from disabled to enabled. true initiates a write when the transition occurs. false prevents a write when the transition occurs.
Stale Time	hours minutes seconds (defaults to 0 (zero))	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). 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}. The default value (zero) disables the stale timer causing points to become stale immediately when unsubscribed. Do not configure an amount of time shorter than the poll cycle time. If you do, points will go stale in the course of normal polling. Instead, set this time to be longer than the largest expected poll cycle time.

Ldap Servers tab

This tab lists one or more Ldap server.

Figure 393 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 80 LDAP server view columns


Column	Description
Display Name	Indicates the name of the server.
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 (true) or off (false).
Fault Cause	Reports the reason for an undesirable status.

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 394 New LDAP server window

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	Defines the name of the server.
Status	read-only	Reports "Issueable" until the badge is assigned, then it may be Active, Disabled, Lost or Unknown.
Connection Host	URL	Defines 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	number (defaults to 636)	Defines the port over which the computer communicates with the server.
Enable Connection TLS	true or false (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	text	Defines 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	text	Defines the password the LDAP server requires for this user.
Enable connection Pooling	true (default) or false	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

Property	Value	Description
		performance. 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.
Connection Timeout	milliseconds	Defines the number of milliseconds that an idle connection may remain in the pool without being closed and removed from the pool.
User Search Base	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 Search Filter	text	Defines the objectClass (metadata) associated with each personnel record that identifies it as a personnel record versus a system or other record type in the server database.
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 395 Import Preferences window

The screenshot shows the 'Import Preferences' dialog box. The title bar reads 'Import Preferences'. Below the title bar, it says 'The following configurations are used for Ldap Import..'. The dialog contains several labeled fields:

- User SearchBase**: An empty text input field.
- User SearchFilter**: A text input field containing '(objectclass=*)'.
- Search Scope**: A dropdown menu currently set to 'Object Scope'.
- Group Attribute**: An empty text input field.
- Allow New InactiveUsers**: A dropdown menu currently set to 'true'.
- Status Attribute**: An empty text input field.
- Active Status Values (Comma Separated)**: An empty text input field.

At the bottom of the dialog are 'Ok' and 'Cancel' buttons.

This window opens when you click **System Setup**→**Remote Devices**→**Remote Drivers**, followed by double-clicking the LdapNetwork driver row in the table.

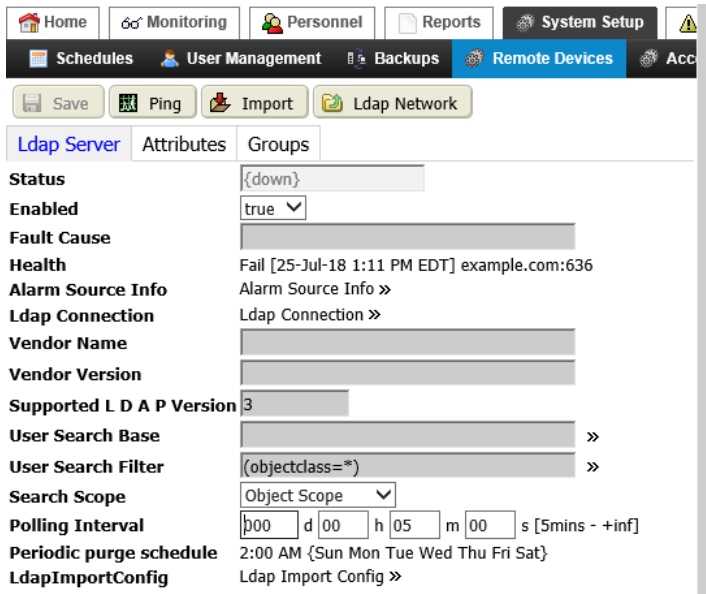
Another way to open this window is to click the **Import** button on the **Ldap Server** view. You access this view by clicking **System Setup**→**Remote Devices**→**Remote Drivers**, followed by double-clicking the LdapNetwork driver row in the table, clicking the **Ldap Servers** tab, selecting the 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 SearchFilter	text	Defines the objectClass (metadata) associated with each personnel record that identifies it as a personnel record versus a system or other record type in the server database.
Search Scope	drop-down list	Defines how much of the User Search Base to actually search:
Group Attribute	text	Defines the LDAP server attribute that provides the LDAP group Distinguished Name. Each LDAP user belongs to a group.
Allow New Inactive Users	true (default) or false	Indicates that users may be added before they are activated in the system.
Status Attribute	text	Reports LDAP user status: active or inactive.
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.

Figure 396 Ldap Server view and tab



To access this view, click **System Setup** → **Remote Devices** → **Remote Drivers**, double-click your LDAP network device driver 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.

Properties

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 LDAP Connection properties, page 415 .
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 Search Base	String chooser	Opens the String chooser window. Refer to User Search Base string chooser, page 416 .
User Search Filter	String chooser	Opens the String chooser window. Refer to User Search Filter string chooser, page 417 .
Search Scope	drop-down list	Defines how much of the User Search Base to actually search:

Property	Value	Description
Polling Interval	plus or minus hours minutes and seconds	Defines how frequently to poll the LDAP server.
Periodic purge schedule	read-only	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 Workbench.
Ldap Import Config	additional properties	Refer to Ldap Import Config, page 418 .

LDAP Connection properties

These properties configure the physical connection between the Supervisor PC and the LDAP server.

Figure 397 Ldap Connection properties

The screenshot shows the 'Ldap Connection' configuration window. The properties and their values are as follows:

- Connection Host: localhost
- Connection Port: 10389
- Enable TLS: false
- Authentication Mechanism: Simple
- Connection User: uid=admin,ou=system
- Connection Password: [masked]
- Enable Connection Pooling: true
- Initial Size: 0
- Max Size: 10
- Pref Size: 0
- Connection Timeout (in milli seconds): 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	text; defaults to the connection already made	Defines 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	number; defaults to 10389	Defines the port over which the computer communicates with the server.
Enable TLS	true or false (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.
Authentication Mechanism	drop-down list; defaults to None	Identifies the method used to verify the identity of the LDAP server to its client, the system database.: Simple Cram Md5 Digest Md5

Property	Value	Description
		For information about these options, refer go the <i>Niagara Station Security Guide</i>
Connection User	text	Defines 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	text	Defines the password the LDAP server requires for this user.
Enable Connection Pooling	true (default) or false	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	number; defaults to 0 (zero)	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.
Perf Size	number; defaults to 0 (zero)	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.

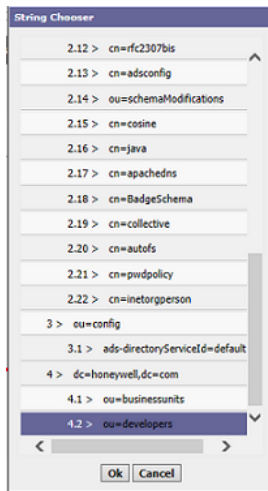
dc stands for domain controller.

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 398 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 399 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 400 Ldap Import properties

Ldap Import Config ▾

Import Frequency

Last Import Time IST

Group Attribute

Allow New Inactive Users

Status Attribute

Active Status Values

Account Expiry Date Time Attribute

Property	Value	Description
Import Frequency	drop-down menu	Defines when to import properties.
Last Import Time	read-only	Reports the last time the system imported data.
Group Attribute	text	Defines the LDAP server attribute that provides the LDAP group Distinguished Name. Each LDAP user belongs to a group.
Allow New Inactive Users	true (default) or false	Indicates that users may be added before they are activated in the system.
Status Attribute	text	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.

Attributes tab

LDAP attributes map to system properties.

Figure 401 Attributes tab

Save Ping Import Ldap Network

Ldap Server **Attributes** Groups

LDAP Attributes Manager

Display Name	Mandatory	Parent Class	Data Type	Description	MappedORD	isRDN
	<input checked="" type="checkbox"/>					

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 81 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 82 Discovered columns

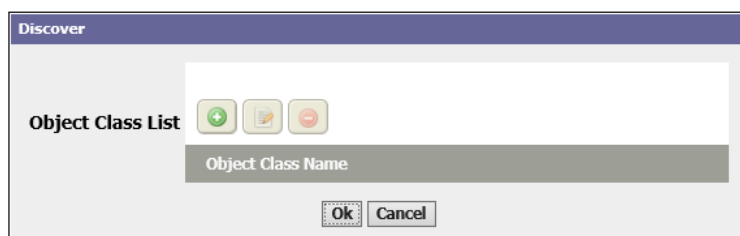
Column	Description
attrName	Reports the name of the attribute.
isMandatory	Indicates if this attribute is required or not.
parentClass	Identifies the owner of this attribute.
dataType	Identifies the type of data: Boolean, numeric, enum or string.
description	Provides additional information.

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 402 Discover attributes window with two object classes



This window opens when you click the Discover button under **LDAP Attributes Manager**.

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 Object Class Name 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 83 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 84 LDAP Discovered columns



Column	Description
attrName	Identifies the attribute in the LDAP server.
isMandatory	Indicates if the property is required by the LDAP server.

Column	Description
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 403 Add Attribute window

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: String identifies the attribute as text. Binary identifies the attribute as a Boolean value.
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 404 Groups tab



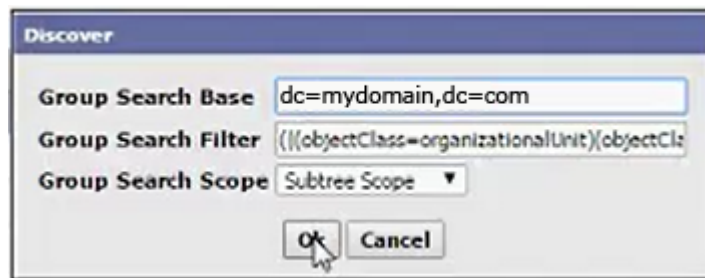
You access this tab by navigating to **Controller (System) Setup**→**Remote Devices**→**Remote Drivers**, double-clicking the LdapNetwork driver row in the table, clicking the **Ldap Server** tab, double-clicking the Ldap Server row, and clicking the **Groups** tab. To view the **Discovered** pane, click 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 405 Discover groups window



This window opens when you click the Discover button (🔍) on the **Ldap Server Groups** tab.

Property	Value	Description
Group Search Base	expression	Defines from which node in the LDAP server to begin searching for groups (access rights).
Group Search Filter	expression	Defines the groups (access rights) to use for the search.
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 85 LDAP Group Manager columns

Column	Description
GroupName	Identifies the system name for this group.
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.

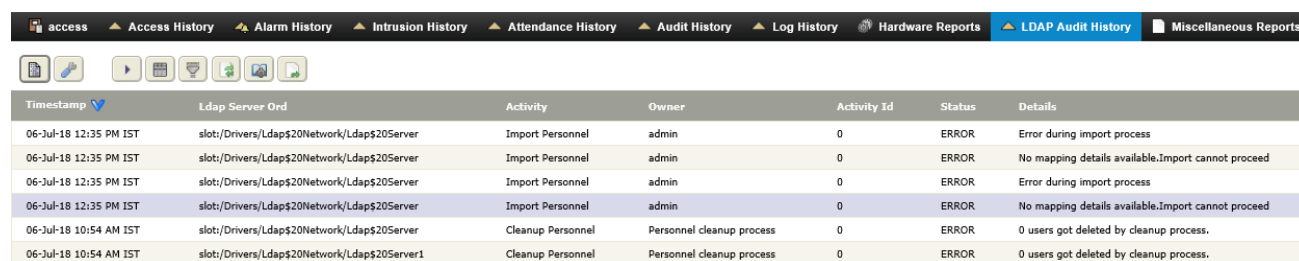
Table 86 LDAP group Discovered columns

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 406 LDAP Audit History view



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 87 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 407 Periodic Purge Schedule properties

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 Trigger Mode properties, page 424
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.

Chapter 16 Nrio Driver views, tabs and windows

Topics covered in this chapter

- ◆ Nrio Device Manager view
- ◆ Nrio Module view
- ◆ Nrio Point Manager, Analog Points tab
- ◆ Nrio Point Edit view
- ◆ History Extension view

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 408 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 88 Nrio Device Manager database columns

Column	Description
Display Name	Reports the name of the Nrio module.
Enabled	Reports if the function is turned on (true) or off (false).
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 89 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 409 Nrio module view

The screenshot shows the 'Nrio16 Module' configuration view. At the top, there is a toolbar with buttons for 'Save', 'Point Manager', 'Clear Totals', 'Go to Module', and 'Nrio Network'. Below the toolbar, the 'Nrio16 Module' title is displayed. The main area is divided into several sections:


- Status:** A text field containing '{disabled,fault}'.
- Enabled:** A dropdown menu set to 'false'.
- Fault Cause:** A text field containing 'Invalid UID: Do Discover and Match.'
- Health:** A text field containing 'Fail [null]'. Below it is an 'Alarm Source Info' section with a dropdown arrow.
- Alarm Source Info:** A series of text fields: 'Alarm Class' (Medium), 'Source Name' (%parent.parent.displayName% %parent.dis), 'To Fault Text', 'To Offnormal Text' (%lexicon(driver:pingFail)%), and 'To Normal Text' (%lexicon(driver:pingSuccess)%).
- Alarm Source Info Hyperlink Ord:** A text field containing 'null'.
- Sound File:** A text field containing 'null'.
- Alarm Icon:** A text field containing 'null'.
- Alarm Instructions:** A button labeled 'Edit'.
- Meta Data:** A button labeled 'Edit' and a text field containing '[No configured facets]'.
- Address:** A text field containing '0' with a range indicator '[0 - 16]'. Below it is an 'Nrio16 Status' section with a dropdown arrow.
- To Status:** A table of status values:

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

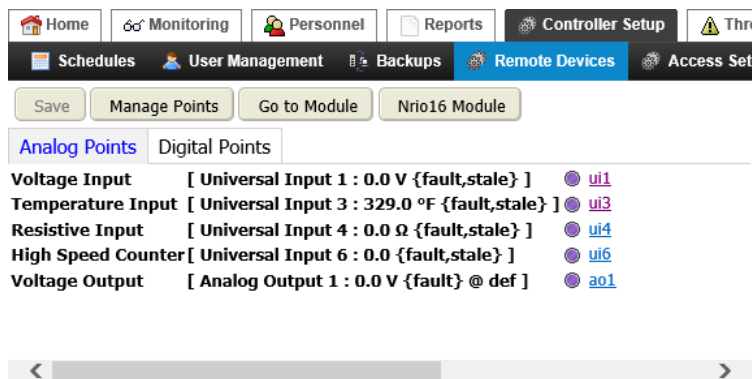
In addition to the standard properties (**Status**, **Fault Cause**, and **Enabled**, **Health** and **Alarm Source Info**), these properties specifically support the **Nrio Module** view.

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.

Figure 410 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.

Links

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.

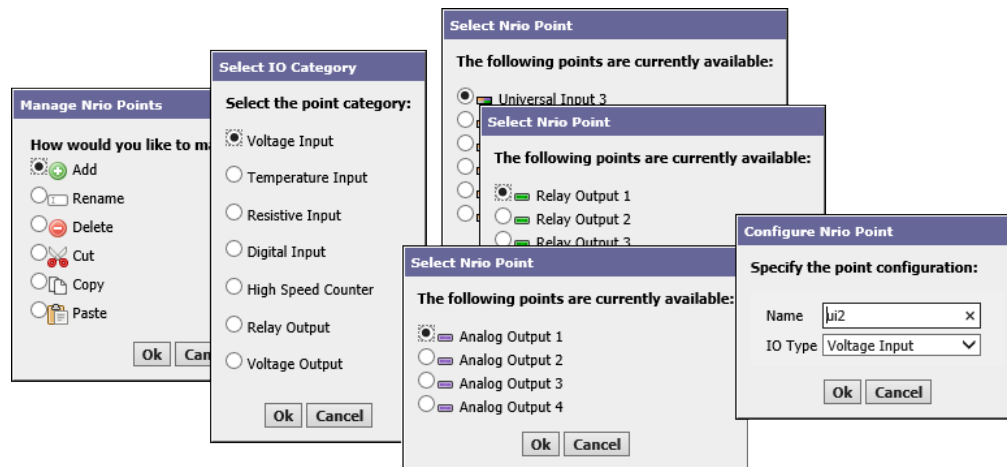
The system creates or adds to this tab when you add an analog point (voltage, temperature, resistive, or high speed counter) by clicking the **Manage Points** button and selecting **Add** in the **Nrio Point Manager** view.

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 411 Manage Nrio Points window



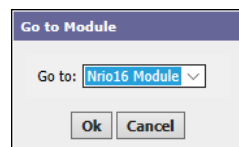
You open these windows from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers**, double-clicking the NrioNetwork row in the table, double-clicking the module name in the table, clicking the **Point Manager** link, followed by clicking the **Manage Points** link.

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.

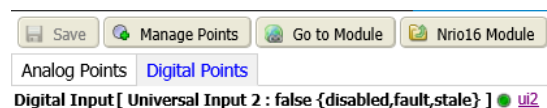
Figure 412 Go to Module window



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.



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.

Links

In addition to **Save**, these links support the point manager:

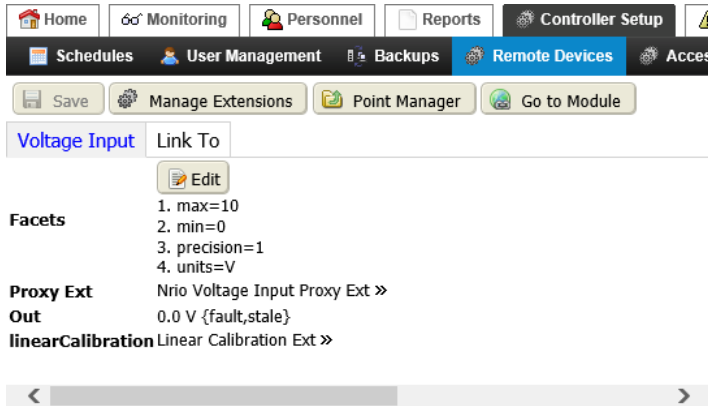
- **Manage Points** opens the **Manage Nrio Points** windows, which add, rename, delete, cut, copy, and paste analog and digital point information.
- **Go To Module** opens the **Go to Module** window for navigating to another set of Nrio module points. The system populates this window only when there 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.

Figure 413 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.

Links

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.

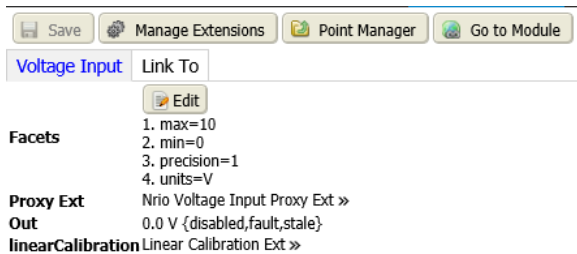
Properties

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 414 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 Voltage Input Facets, page 431 .
Proxy Ext	additional properties	Refer to .
Out	read-only	Reports the current value of the proxy point and its status.
linearCalibration	additional properties	Refer to .

Voltage Input Facets

Facets determine how a point's value displays in the station. Voltage Input facets include voltage numbers and decimal precision.

Figure 415 Voltage Input Facets and Edit facets window

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 416 Voltage Proxy Ext properties

Nrio Voltage Input 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 <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>NOTE: 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 "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 <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> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. <code>Generic Tabular</code> 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 requests.</p>
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 input value. The network's Poll Service defines these rates in hours, minutes and seconds. For example:</p> <p><code>Fast</code> may set polling frequency to every second.</p>

Property	Value	Description
		Normal may set poll frequency to every five seconds. Slow may set poll frequency to every 30 seconds.
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.

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 417 Linear Calibration properties

Linear Calibration Ext ▾

Scale

Offset

Units **Quantity** **Unit**

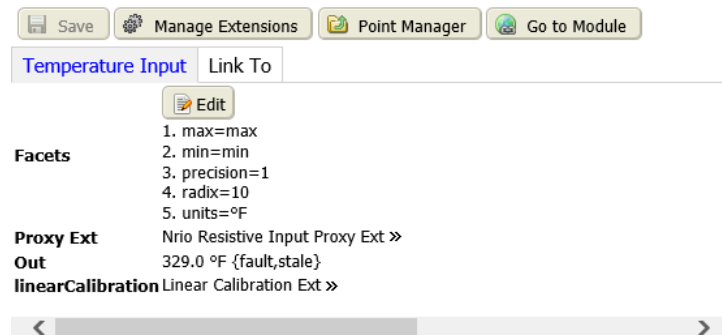
Fault Cause

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	Reports the reason why a network, component, or extension is in fault. Fault Cause is blank unless a fault exists.

Temperature Input points

Configures a temperature input point.

Figure 418 Temperature Input tab



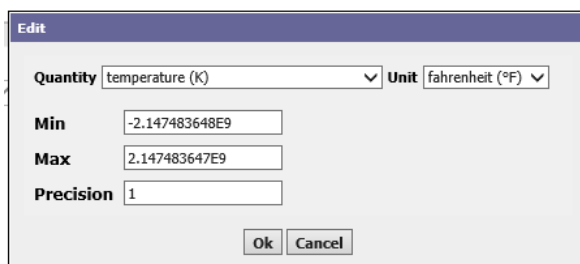
You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers**, double-clicking the **NrioNetwork** driver, double-clicking a module, clicking the **Point Manager** link, followed by clicking the hyperlink to the right end of the `Temperature Input` point.

Property	Value	Description
Facets	additional properties	Refer to Temperature Input Facets, page 435 .
Proxy Ext	additional properties	Refer to Temperature Proxy Ext properties, page 436 .
Out	read-only	Reports the current temperature of the proxy point and its status.
linearCalibration	additional properties	Refer to Temperature Input, Linear Calibration Ext properties, page 438 .

Temperature Input Facets

Facets determine how a point’s value displays in the station. Temperature facets include a minimum, maximum, and decimal precision.

Figure 419 Temperature Input Facets and Edit facets window



The Edit window opens when you click the **Edit** button.

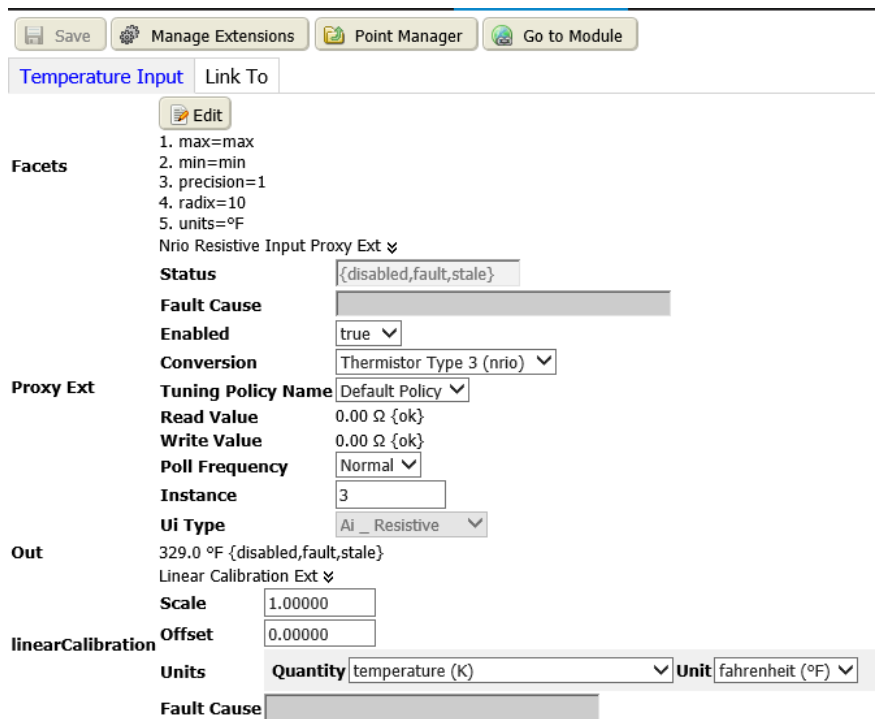
Property	Value	Description
Quantity	drop-down list	Defines the units used to measure temperature.
max	number	Defines the maximum temperature value.

Property	Value	Description
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 de-grees Fahrenheit	Configures the default unit.

Temperature Proxy Ext properties

These properties configure the proxy point extension.

Figure 420 Temperature Proxy Ext properties



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 <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>NOTE: 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 "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 <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> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. <code>Generic Tabular</code> 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 requests.</p>
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 input value. The network's Poll Service defines these rates in hours, minutes and seconds. For example:</p> <p><code>Fast</code> may set polling frequency to every second.</p>

Property	Value	Description
		Normal may set poll frequency to every five seconds. Slow may set poll frequency to every 30 seconds.
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 421 Linear Calibration properties

linearCalibration

Scale

Offset

Units **Quantity** **Unit**

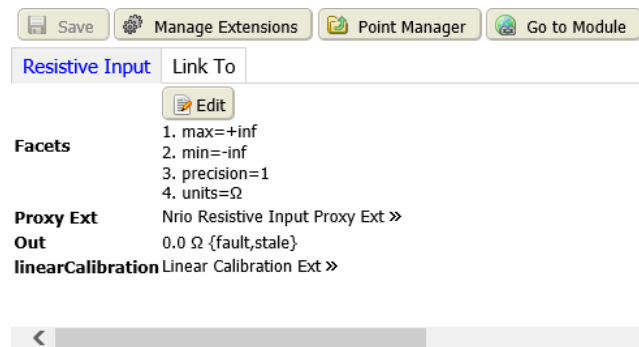
Fault Cause

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 (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	Reports the reason why a network, component, or extension is in fault. Fault Cause is blank 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 422 Resistive Input tab



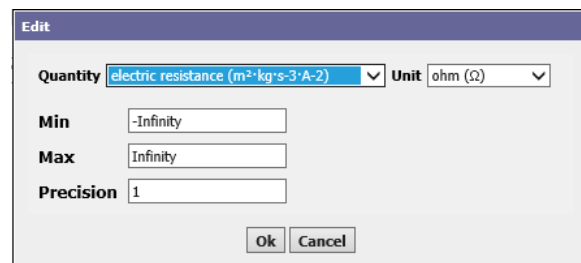
You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers**, followed by double-clicking the NrioNetwork driver, selecting and double-clicking a module, clicking the **Point Manager** link, followed by clicking the hyperlink to the right end of the Resistive Input point.

Property	Value	Description
Facets	additional properties	Refer to Resistive Input Facets, page 439 .
Proxy Ext	additional properties	Refer to Resistive Input Proxy Ext properties, page 440 .
Out	read-only	Reports the current value of the proxy point and its status.
linearCalibration	additional properties	Refer to Resistive Input, Linear Calibration Ext properties, page 442 .

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 423 Resistive Input Facets and Edit facets window



The Edit window opens when you click the **Edit** button.

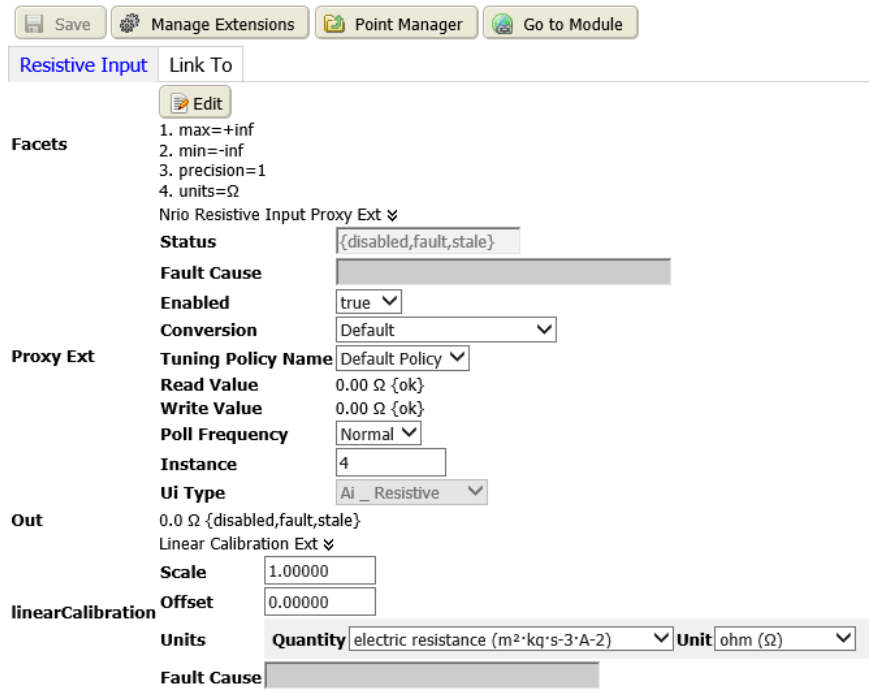
Property	Value	Description
Quantity	drop-down list	Defines the formula.
Unit	defaults to ohm	Configures the default unit.
Max	number, defaults to Infinity	Defines the maximum ohm value.

Property	Value	Description
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 424 Resistive Input Proxy Ext properties



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 <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>NOTE: 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 "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 <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> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. <code>Generic Tabular</code> 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 requests.</p>
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 input value. The network's Poll Service defines these rates in hours, minutes and seconds. For example:</p> <p><code>Fast</code> may set polling frequency to every second.</p>

Property	Value	Description
		Normal may set poll frequency to every five seconds. Slow may set poll frequency to every 30 seconds.
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.

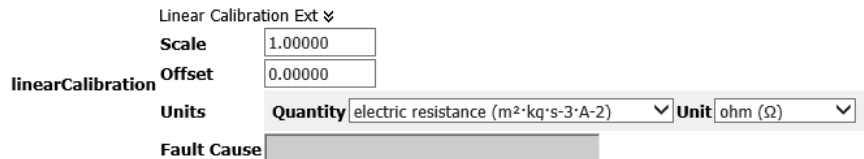
Resistive Input, Linear Calibration Ext properties

These properties calibrate the calculated resistance value before it is applied to the Out slot, where $[(\text{calculatedValue} \times \text{Scale}) + \text{Offset}] = \text{Out value}$. 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 425 Resistive Input Linear Calibration properties

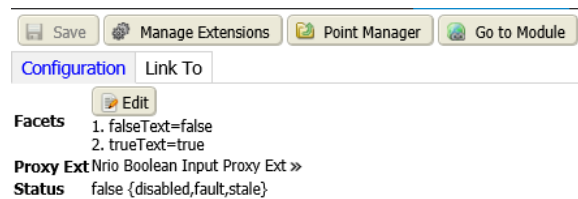


Property	Value	Description
Scale	number, defaults to 1.0	Defines a scale value. Usually you leave this value set to the default. One exception is if you copied this extension under a <code>CounterInputPoint</code> for the purpose of returning a scaled total.
Offset	positive or negative number, defaults 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	Reports the reason why a network, component, or extension is in fault. Fault Cause is blank unless a fault exists.

Digital input points

Configures a Boolean Input proxy point.

Figure 426 Digital Input, Configuration tab



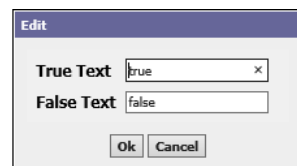
You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers**, followed by double-clicking the NrioNetwork driver, selecting and double-clicking a module, clicking the **Point Manager** link, clicking the **Digital Points** tab, followed by clicking the 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 .
Proxy Ext	additional properties	Refer to .
Status	read-only	Indicates the condition of the network, device or component at the last check. {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. {disabled} indicates that the Enable property is set to false. {fault} indicates another problem. Refer to Fault Cause for more information.

Edit window

Figure 427 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 Status for the point is true.
False Text	text	Sets up the text to appear when Status for the point is false.

Digital Proxy Ext properties

Figure 428 Digital Proxy Ext properties

Status	<input data-bbox="462 304 656 331" type="text" value="{fault,stale}"/>
Fault Cause	<input data-bbox="462 338 810 365" type="text"/>
Enabled	<input data-bbox="462 371 526 399" type="text" value="true"/>
Conversion	<input data-bbox="462 405 680 432" type="text" value="Default"/>
Proxy Ext Tuning Policy Name	<input data-bbox="462 438 591 466" type="text" value="Default Policy"/>
Read Value	<input data-bbox="462 472 537 499" type="text" value="false {ok}"/>
Write Value	<input data-bbox="462 506 537 533" type="text" value="false {ok}"/>
Poll Frequency	<input data-bbox="462 539 545 567" type="text" value="Normal"/>
Instance	<input data-bbox="462 573 576 600" type="text" value="4"/>
Ui Type	<input data-bbox="462 606 612 634" type="text" value="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	<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>NOTE: 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 "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 <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> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. <code>Generic Tabular</code> 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 requests.</p>
Read Value	read-only true or false	
Write Value	read-only true or false	
Poll Frequency	drop-down list	Configures how frequently the system polls proxy points.

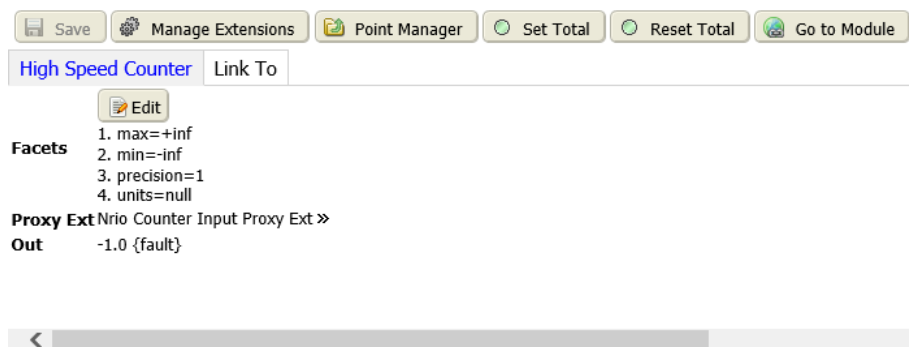
Property	Value	Description
Instance	number	Defines the point's I/O terminal address based on its hardware type. If duplicated (same instance as same hardware type, same board), the point reports a fault status. If an edit attempt is made to an instance already in use by another proxy point, the system discards the edit, and retains the previous instance value.
Ui Type	drop-down list	

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 429 High Speed Counter tab



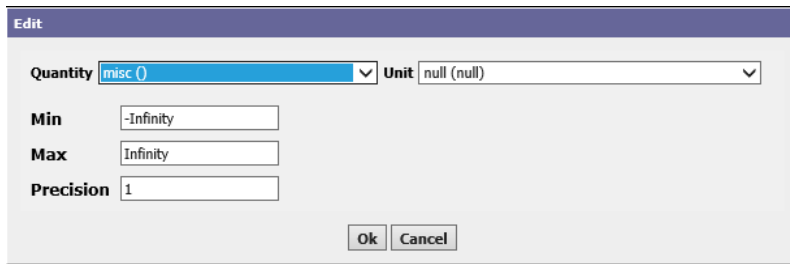
You access this view from the main menu by clicking **Controller Setup**→**Remote Devices**→**Remote Drivers**, double-clicking the **NrioNetwork** driver, double-clicking a module, clicking the **Point Manager** link, followed by clicking the hyperlink to the right end of the High Speed Counter point.

Property	Value	Description
Facets	additional properties	Refer to High Speed Counter Facets, page 446 .
Proxy Ext	additional properties	Refer to High Speed Counter Proxy Ext properties, page 447 .
Out	read-only	Reports the current value of the proxy point and its status.

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 430 High Speed Counter Facets and Edit facets window

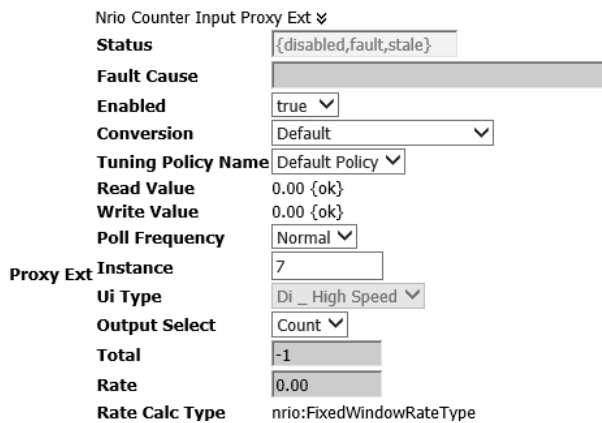


The Edit window opens when you click the **Edit** button.

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 431 High Speed Counter Proxy Ext properties



In addition to the standard properties (Status, Fault Cause, and Enabled), these properties support high speed counter proxy extensions.

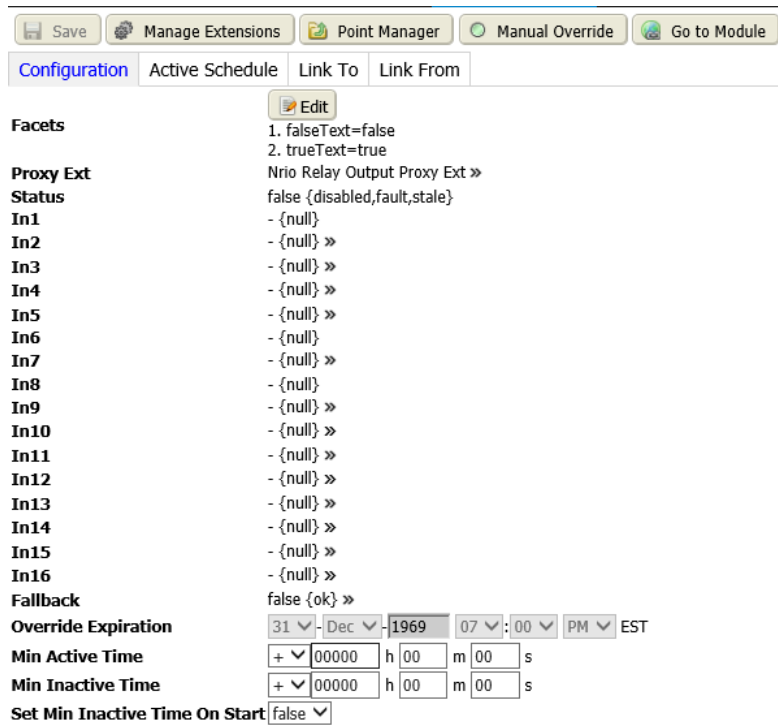
Property	Value	Description
Conversion	drop-down list, defaults to <code>Default</code>	<p>Defines how the system converts proxy extension units to parent point units.</p> <p><code>Default</code> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p>NOTE: 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 "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 <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> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. <code>Generic Tabular</code> 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 requests.</p>
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 input value. The network's Poll Service defines these rates in hours, minutes and seconds. For example:</p> <p><code>Fast</code> may set polling frequency to every second.</p>

Property	Value	Description
		Normal may set poll frequency to every five seconds. Slow may set poll frequency to every 30 seconds.
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.
Output Select	drop-down list, defaults to Count	Specifies if count total (Count) or count rate (Rate) 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 Rate Calc configuration.
Rate Calc Type	drop-down list	Defines the type of rate calculation: The purpose of these calculations is to report a meaningful value: <code>FixedWindowRateType</code> waits for the interval defined under the Rate Calc slot to elapse. Then it recalculates the rate based on the interval. <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. <code>TriggeredRateType</code> adds a <code>recalculateRate</code> action to the parent point.
Rate Calc	additional properties	Provides one to three properties to use in the rate calculation: <code>Scale</code> (defaults to 1) depends on the item quantity/pulse and desired rate units. <code>Interval</code> (not available if <code>Rate Calc Type</code> is <code>TriggeredRateType</code>) defaults to one (1) minute. <code>Windows</code> (available only if <code>Rate Calc Type</code> is <code>SlidingWindowRateType</code>) 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 432 Relay Output, Configuration tab



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.

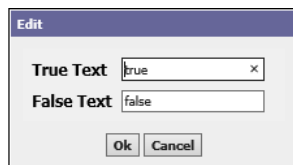
Property	Value	Description
Facets	additional properties	Refer to Relay Out Facets, page 451 .
Proxy Ext	additional properties	Refer to Relay out Proxy Ext properties, page 451 .
Status	read-only	Indicates the condition of the network, device or component at the last check. {ok} indicates that the component 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. {disabled} indicates that the Enable property is set to false. {fault} indicates another problem. Refer to Fault Cause for more information.
In2-5, 7, and 9-16	true or false, defaults to false	Configures the amount of voltage coming from each of 16 inputs. 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 In value.

Property	Value	Description
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. 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 433 Relay Output Configuration Facets

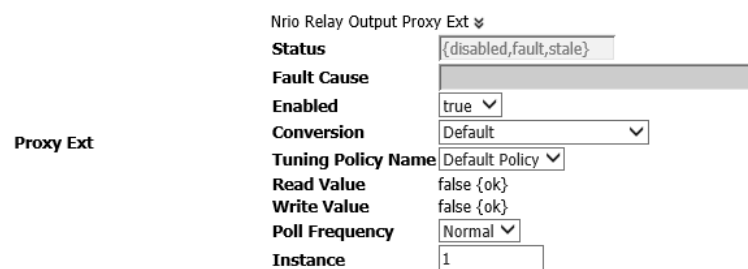


You use this window to configure different text (other than `true` and `false`) when the station writes this Boolean value.

Relay out Proxy Ext properties

The proxy extension properties are the same as those documented for other Nrio proxy points.

Figure 434 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>)	<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>NOTE: 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 "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 <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> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. <code>Generic Tabular</code> 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>)	Defines the assigned tuning policy. During polling, the system uses the network driver's 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.

Property	Value	Description
Poll Frequency	drop-down list	Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its input value. The network's Poll Service defines these rates in hours, minutes and seconds. For example: Fast may set polling frequency to every second. Normal may set poll frequency to every five seconds. Slow may set poll frequency to every 30 seconds.
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.

Voltage Output points

This is a NumericWritable point that represents a 0-to-10Vdc analog output (AO).

Figure 435 Voltage Output tab

Voltage Output | Link To | Link From

[Edit](#)

Facets

- max=10
- min=0
- precision=1
- 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

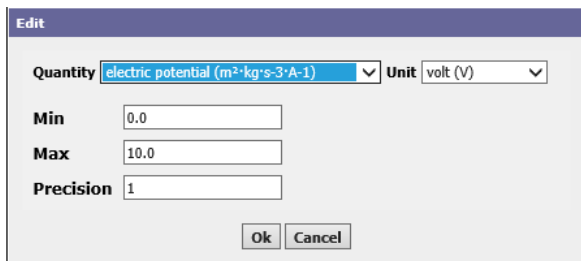
You access it from the **Nrio Point Manager, Analog Points** tab by clicking the hyperlink on a Voltage Output point.

Property	Value	Description
Facets	additional properties	Refer to Voltage Output Facets properties, page 454.
Proxy Ext	additional properties	Refer to Voltage Output Proxy Ext properties, page 454.
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 10.0, defaults to 0.0	Creates a pre-defined output value in 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 436 Voltage Output facets and Edit facetw window



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 437 Voltage Output Proxy Ext properties

Nrio Voltage Input Proxy Ext	
Status	{disabled,fault,stage}
Fault Cause	
Enabled	true
Conversion	Default
Proxy Ext	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.

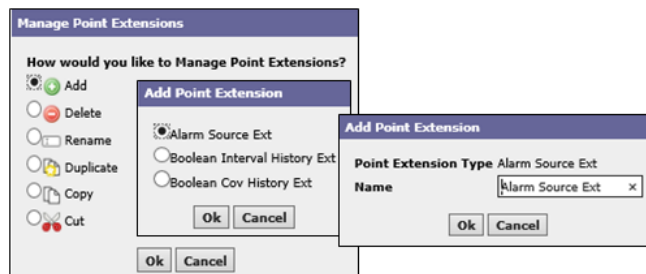
Property	Value	Description
Conversion	drop-down list, defaults to <code>Default</code>	<p>Defines how the system converts proxy extension units to parent point units.</p> <p><code>Default</code> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p>NOTE: 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 "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 <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> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. <code>Generic Tabular</code> 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 requests.</p>
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.

Property	Value	Description
Poll Frequency	drop-down list (defaults to <code>Normal</code>)	Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its input value. The network's Poll Service defines these rates in hours, minutes and seconds. For example: Fast may set polling frequency to every second. Normal may set poll frequency to every five seconds. Slow may set poll frequency to every 30 seconds.
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.

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 438 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**:

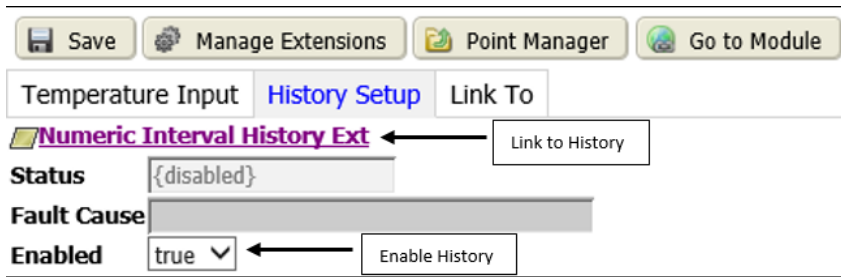
You can add Alarm Source extensions, History Extensions, and create links between appropriate points using standard assign Mode features.

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.

Figure 439 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.

Links

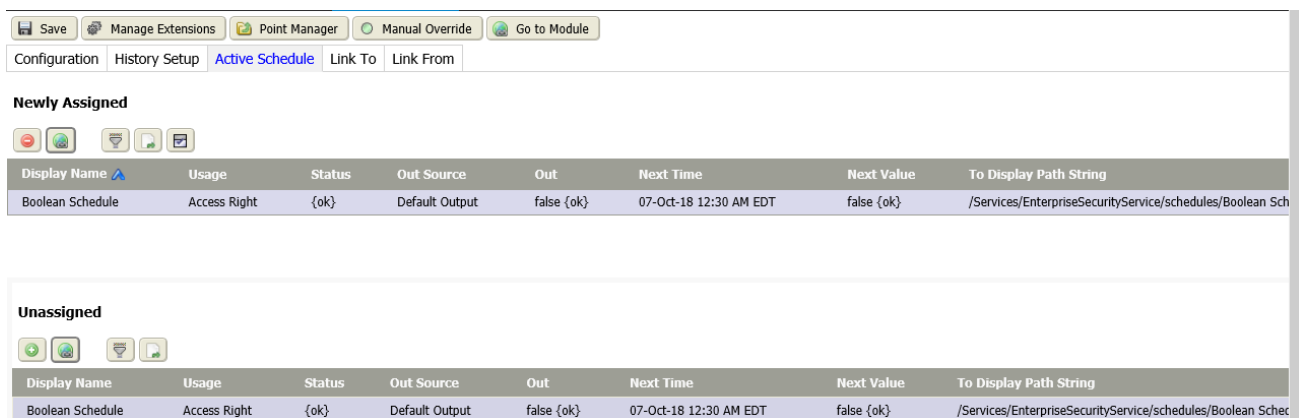
The links at the top of this tab provide these functions:

- **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.

Figure 440 Active Schedule tab



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.

Columns

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 441 Nrio edit point view (showing Link To error)

Configuration
History Setup
Active Schedule
Link To
Link 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

Page of 2

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 90 Link To columns

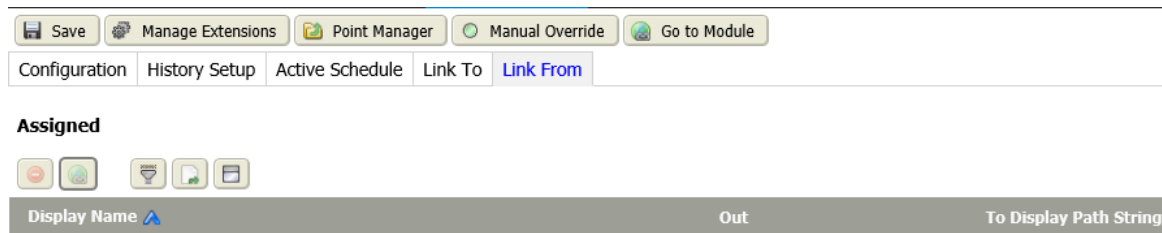
Column	Description
Display Name	Identifies the name of the point.
Out	Reports the Out value.

Column	Description
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.

Figure 442 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 91 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.

Figure 443 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
- Change Tolerance
- Precision
- Min Rollover Value
- Max Rollover Value

Interval: irregular, Record Type: numeric trend record, Capacity: 500 records, Full Policy: Roll >>

Id / /

Source 0 Ords

Time Zone NULL (+0) ▾

Record Type history:NumericTrendRecord

Capacity Record Count ▾ 500 records

Full Policy Roll ▾

Interval irregular ▾

System Tags

valueFacets

- max=10
- min=0
- precision=1
- units=V

minRolloverValue null 0.00

maxRolloverValue null 0.00

precision 32 bit ▾

Edit

Facet Key	Facet Value
<input type="checkbox"/> max	10
<input type="checkbox"/> min	0
<input type="checkbox"/> precision	1
<input type="checkbox"/> units	volt (V) >>

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.

Properties

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 Active Period properties.
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 History Name property. An error string here indicates that the History Name property is incorrectly defined.

Property	Value	Description
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. <code>Unlimited</code> 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 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 Change Tolerance 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 444 Set COM Port for Nrio devices

This window opens from the **Nrio Device Manager** when you click the Set COM Port button ().

Property	Value	Description
Port Name	text	Defines the communication port to use: none, COM2 or COM3.
Trunk	number	Each RS-485 connection is called a trunk. If your network has multiple RS-485 trunks, a separate network and remote I/O module is required to support each. This property specifies which trunk the port is connected to.

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 445 Upload window

This window opens from the **Nrio Device Manager** when you click the Upload button (.

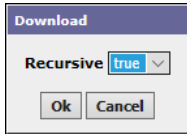
Typically, you leave the upload properties at their default settings of `true`.


Property	Value	Description
Recursive	<code>true</code> or <code>false</code>	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 run-time requirements. The uploading of recursive data is always recommended.
Upload Transient	<code>true</code> or <code>false</code>	Transient data typically store current session information, which the system clears when it resets the device.
Upload Persistent	<code>true</code> or <code>false</code>	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 446 Download window



This window opens from the **Nrio Device Manager** when you click the Download button ().

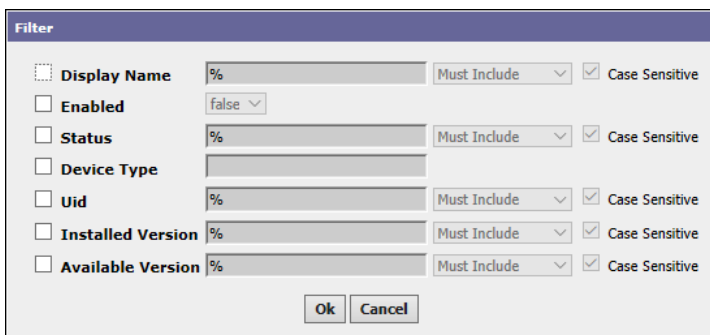
The single download property turns the download function off (`false`) and on (`true`).

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 447 Nrio Device Manager Filter window



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.

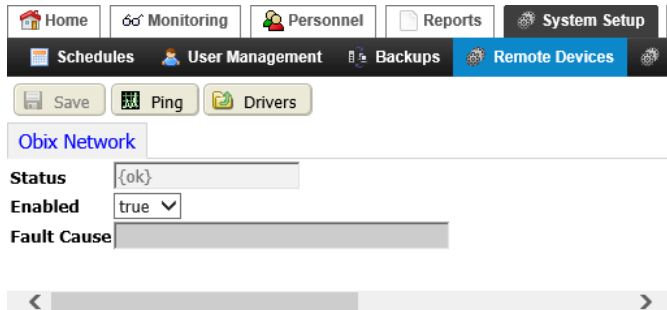
Chapter 17 Obix Network view

Topics covered in this chapter

◆ Obix links

The Obix Network view includes tabs for configuring the Obix Network and Obix clients.

Figure 448 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.

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 18 Photo ID management

Topics covered in this chapter

- ◆ Photo ID Network view
- ◆ Azure ID Client Device view
- ◆ Azure ID Device.[template] view
- ◆ Edit Photo ID Template Data view
- ◆ Photo ID Viewers view
- ◆ Photo ID Viewer (surveillance) view

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.



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**

Database pane

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:



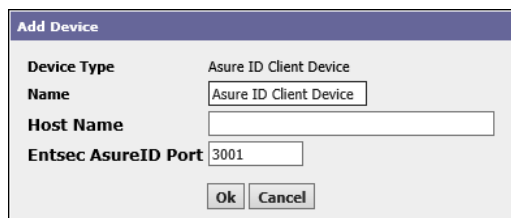

-  Add discovered item(s) moves one or more discovered items from the **Discovered** pane to the **Database** pane. It is available when items are selected (highlighted) in the **Discovered** pane. Before the item(s) are added, a window opens with properties to configure them.
-  Match initiates an action 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 449 PhotoID Add Device window

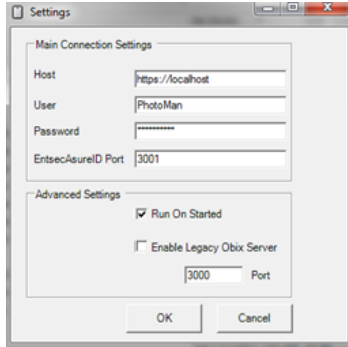


You access this view from the Supervisor’s main menu by clicking **Photo ID** followed by clicking the Manage Devices button () , clicking Add, selecting the Asure Id Client Device, and clicking **Ok**.

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 platform host name or the IP address of the computer that is running EntsecAsureID.
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.

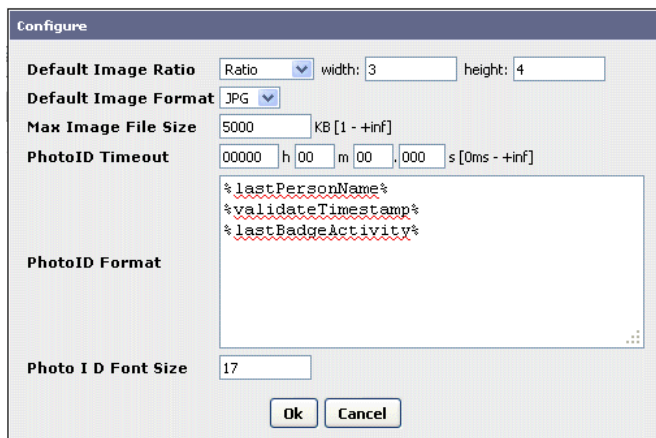



To open this window on the Photo ID workstation, right-click the EntsecAsureID icon (📷) in the system tray, and select the Settings menu option.

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 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.



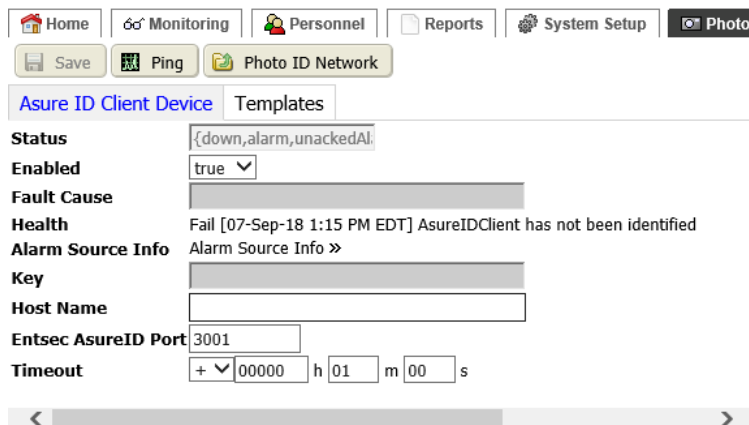
This window opens when you click the Settings button () on the **Photo ID Network** view.

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 photos created to conform to the photo property defined by the Asure ID template. Free-hand 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).

Figure 450 Asure ID Client Device tab



The screenshot shows the 'Asure ID Client Device' configuration tab. At the top, there is a navigation bar with buttons for Home, Monitoring, Personnel, Reports, System Setup, and Photo. Below this is a sub-navigation bar with Save, Ping, and Photo ID Network buttons. The main configuration area includes:

- Status:** A text field containing '{down,alarm,unackedAl:'.
- Enabled:** A dropdown menu set to 'true'.
- Fault Cause:** A greyed-out text field.
- Health:** A text field displaying 'Fail [07-Sep-18 1:15 PM EDT] AsureIDClient has not been identified'.
- Alarm Source Info:** A text field with a link 'Alarm Source Info »'.
- Key:** A greyed-out text field.
- Host Name:** An empty text field.
- Entsec AsureID Port:** A text field containing '3001'.
- Timeout:** A time picker set to '+ 00000 h 01 m 00 s'.

At the bottom of the configuration area, there are left and right navigation arrows.

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.

Links

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

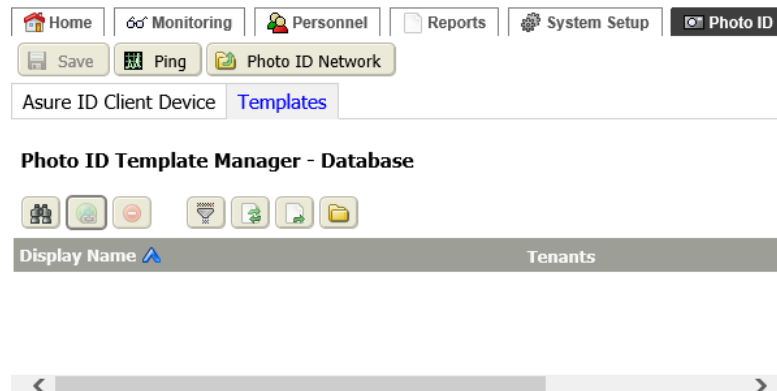
In addition to the standard properties (**Status**, **Enabled**, **Fault Cause**, **Health**, and **Alarm Source Info**), these properties support an Azure ID client device.

Property	Value	Description
Key	read-only	Displays a unique identifier for a particular EntsecAzureID (non-legacy) device and is provided automatically during discovery. After manually adding the EntsecAzureID device, you match with the discovered device in order to populate this property.
Host Name	text	Defines the platform host name or the IP address of the computer that is running EntsecAzureID.
EntsecAzureID Port	text	Identifies the port used for the EntsecAzureID 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 Azure ID templates to add to the database.

Figure 451 Templates tab



You access this view from the Supervisor's main menu by clicking **Photo ID**, double-clicking the Azure ID Client Device row in the table and clicking the **Templates** tab.

Use this tab to discover the template(s) created using the Azure 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.



Links


In addition to the Save link, these links support the Azure 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 Azure 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.

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.

Buttons

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.

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.

Buttons

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.

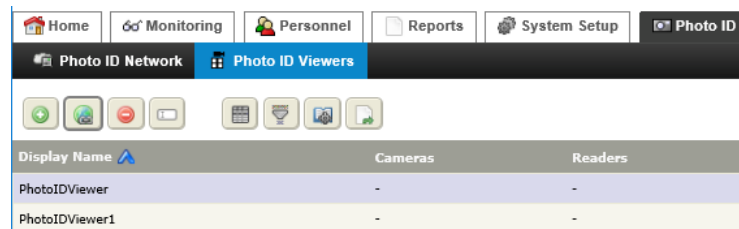
You access this view from the Supervisor's main menu by clicking **Photo ID** followed by double-clicking the **Asure ID Client Device** row in the **Photo ID Network** table, clicking the **Templates** tab, and double-clicking a template row in the **Template Data** view table.

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.



You access this view from the main Supervisor menu by clicking **Photo ID** → **Photo ID Viewers**.

Buttons

In addition to the standard buttons (Delete, Rename, Column Chooser, Filter, Manage Reports, and Export), these buttons support Photo ID viewers.

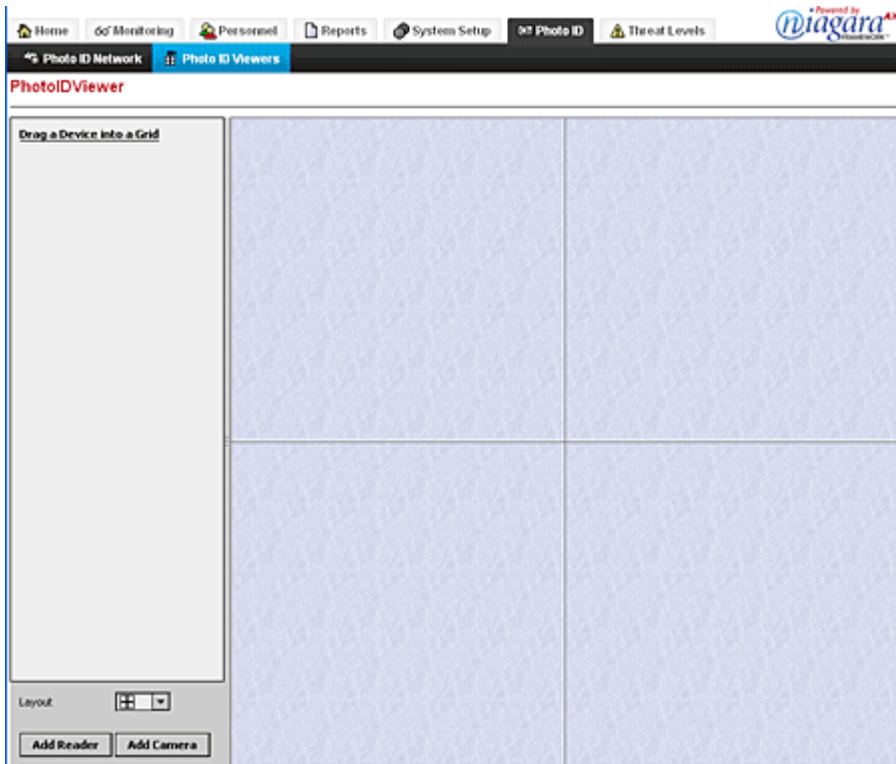
-  Add adds a new Photo ID viewer.
-  Hyperlink opens the viewer.

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 19 Workbench components in the entsec module

Topics covered in this chapter

- ◆ entsec-SecurityActivityMonitor (AX Alarm Console)
- ◆ entsec-SecurityAlarmConsoleOptions
- ◆ entsec-EnterpriseSecurityService
- ◆ entsec-AccessControlService (AX Property Sheet)
- ◆ entsec-ReplicationService (AX Property Sheet)

Components include services, folders and other model building blocks. You may drag them onto a property or Wire Sheet from a palette. These components configure system stations using Workbench.

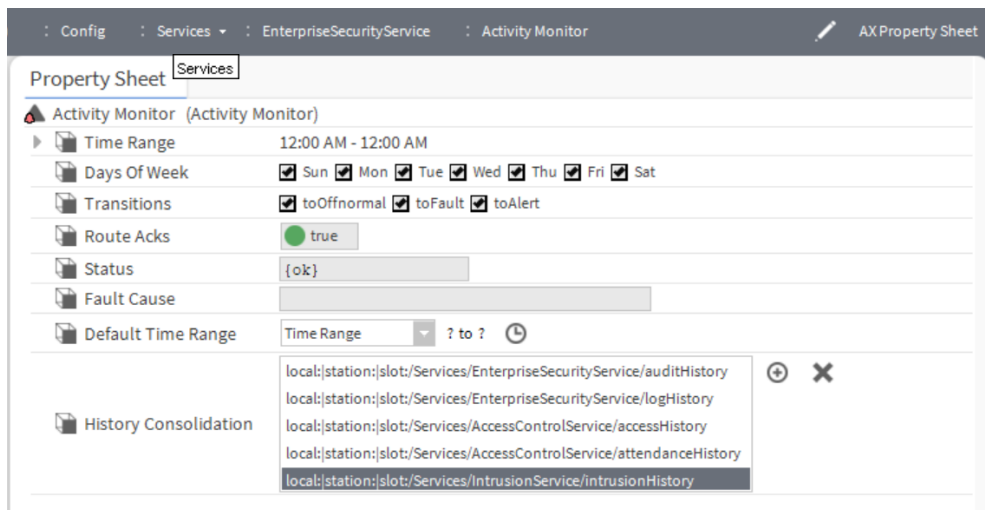
The descriptions included in the following topics appear as headings in documentation. They also appear as context-sensitive help topics when accessed by:

- Right-clicking on the component and selecting **Views→Guide Help**
- Clicking **Help→Guide On Target**.

entsec-SecurityActivityMonitor (AX Alarm Console)

This 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 452 Security Alarm Monitor properties



You can access these property by double-clicking the **Services→EnterpriseSecurityService** in Nav tree.

In addition to the standard properties (Status and Fault Cause). This property is unique to this service:

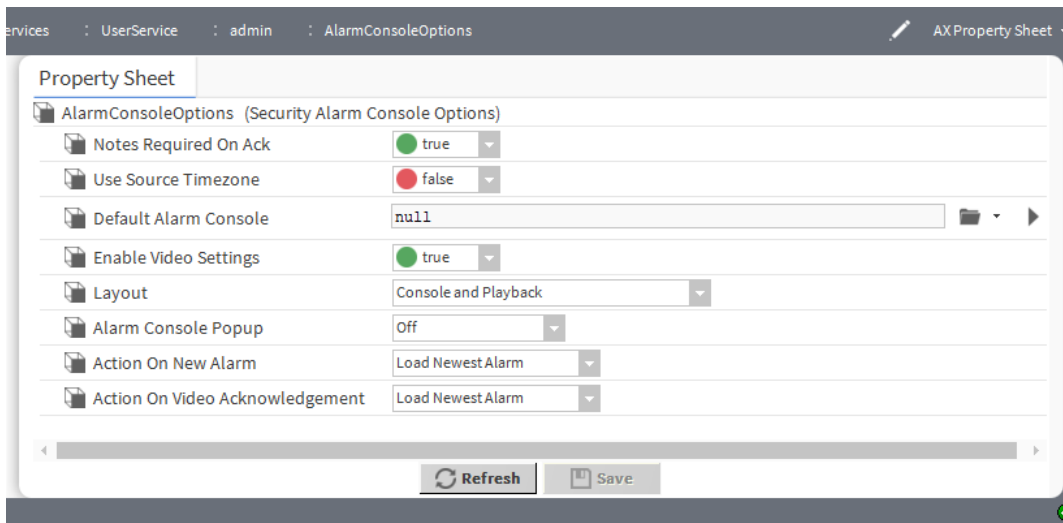
Property	Value	Description
Time Range	Start Time and End Time	Start Time sets the time of day to begin the function (for example, trigger schedule, alarm event)
Days of Week	check mark	Specifies the days of the week.

Property	Value	Description
Transitions	toOffnormal, toFault, toNormal, toAlert	Allows selection of specific alarm transitions to display in the console. Only those transitions that are selected will be displayed in the console - even though the alarms are still saved into the alarm history.
Route Acks	true (default) or false	Enables and disables the routing of alarm acknowledgements to the recipient. Enable this property by selecting "true". Trap acknowledgements are not routed if "false" is selected.
Default Time Range	drop-down	Allows selection of Time Range for ActivityMonitor .
History Consolidation	text	

entsec-SecurityAlarmConsoleOptions

This component configures the alarm console assigned to a specific user.

Figure 453 Security Alarm Console Options properties



You access these properties by double-clicking the **Video Alarm Console Options** node under **Service-s→UserService→admin** (or other user name) in the Nav tree.

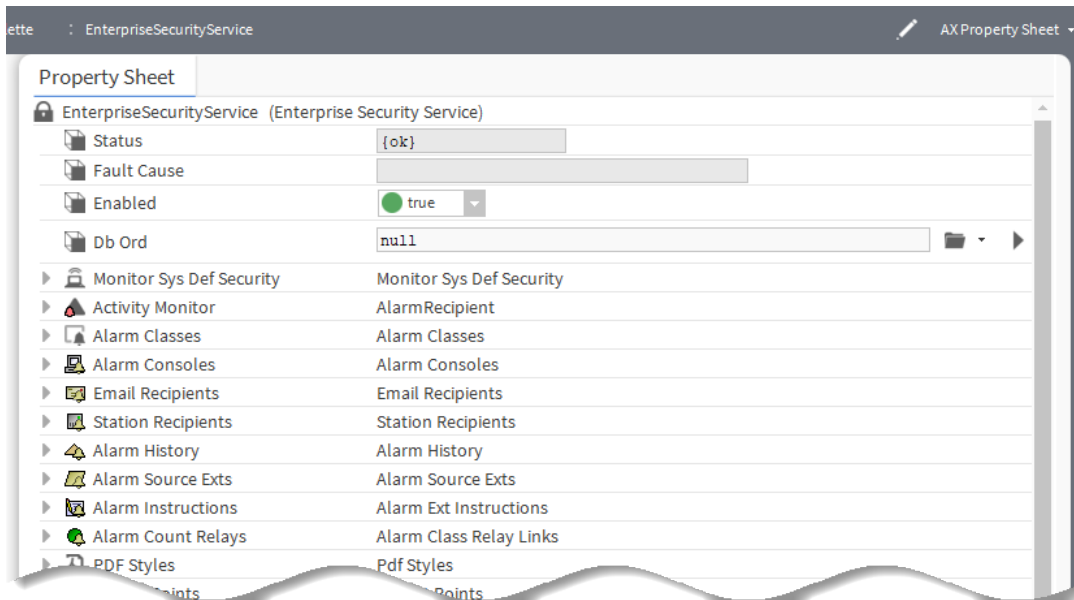
Property	Value	Description
Notes Required On Ack	true (default) or false	Configures the requirement to add a note when the operator acknowledges an alarm. true opens the Notes window when the operator initiates an alarm acknowledgment from the alarm console. false does not require a note.
Use Source Timezone	true or false (default)	For time reporting, configures the console to report the time zone at the source of the alarm rather than at the location of the Supervisor station.

Property	Value	Description
Default Alarm Console	Ord selector	In cases where you have more than one Alarm Console, this property selects the console that displays initially when an alarm console view opens.
Enable Video Settings	true (default) or false	Displays and hides the video setting properties. When set to false, the following properties do not display in the view: Layout , Alarm Console Popup , Action on New Alarm , and Action On Video Acknowledgment .
Layout	drop-down list	Lists the display options that are available for the Alarm Console - Live view. The options determine what information the live console view displays. Some layouts include one or more video feeds.
Alarm Console Popup		Enables and disables the alarm console popup feature. When enabled (on), new alarms open an alarm popup window.
Action On New Alarm	drop-down list (defaults to Load Newest Alarm)	For video alarms, determines alarm console behavior when a new alarm (with video) occurs. Load Newest Alarm automatically displays video associated with the latest alarm. Manual Alarm Selection displays no video until you select an alarm in the console.
Action on Video Acknowledgment	drop-down list (defaults to Load Video)	Determines the video alarm console behavior when a video alarm is acknowledged from the video alarm controls. Load Newest Alarm automatically displays the video associated with the acknowledged alarm. Manual Alarm Selection displays no video until you select the alarm in the console.

entsec-EnterpriseSecurityService

This component serves as the parent for a long list of components

Figure 454 EnterpriseSecurityService properties



You access this **Property Sheet** by double-clicking the **EnterpriseSecurityService** under the **Services** folder in the Nav tree.

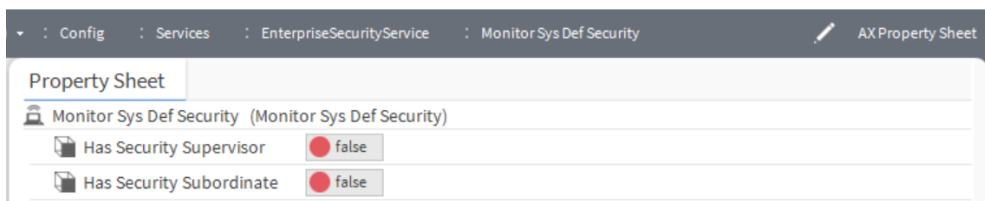
In addition to the standard properties (Status, Fault Cause and Enabled). this property is unique to this service:

Property	Value	Description
Db Ord	ORD	Identifies the location of the Orion database in the station.

entsec-MonitorSysDefSecurity (AX Property Sheet)

This component defines the role of Niagara station, Whether it will work as a Supervisor or Controller.

Figure 455 Security Monitor Sys Def Security



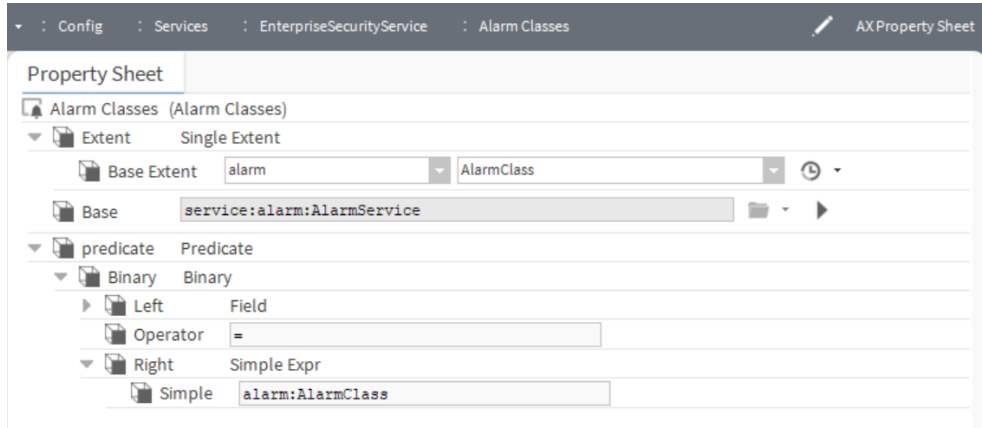
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Has Security Supervisor	true or false	When it displays true then station works as a Security Supervisor. It does not work when displays false.
Has Security Subordinate	true or false	When it displays true then station works as a Security Subordinate. It does not work when displays false.

entsec-AlarmClasses (Wb Query Table View)

This component may route alarms to one or more alarm recipients. The routing process involves notifying the recipient of the alarm and receiving back from the recipient an alarm acknowledgement

Figure 456 Security Alarm Classes properties



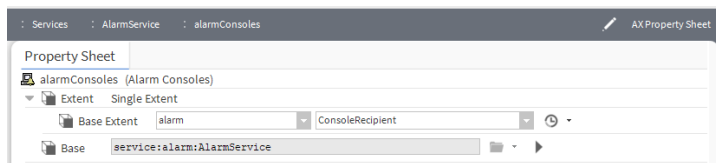
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree. In addition to the standard properties (Enabled). This property is unique to this service:

Property	Value	Description
Extent	Single Extent	
Base	drop-down	
Predicate	Predicate	
Binary	Binary	
Left	Field	
Field path	text	
Operator		Its a user name who is going to operate.
Right	Simple Expr	
Simple	text	

entsec-AlarmConsoles (WB Query Table View)

This component links the **AlarmClass** components into whatever alarm recipient objects are needed.

Figure 457 Security Alarm Consoles properties



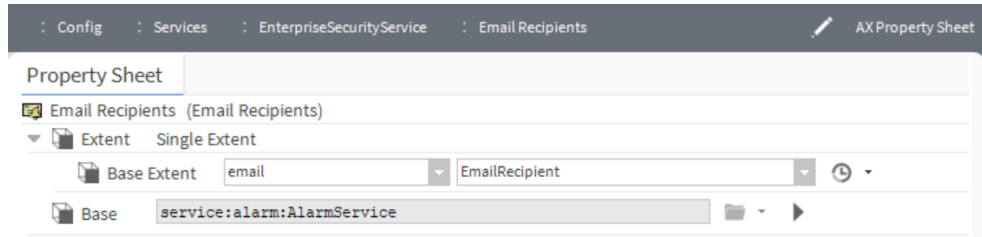
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
Base	Path	User can select a file location.

entsec-EmailRecipients (WB Query Table View)

This component is used to route the alarms to get the notification by E-mail.

Figure 458 Security Email Recipients properties



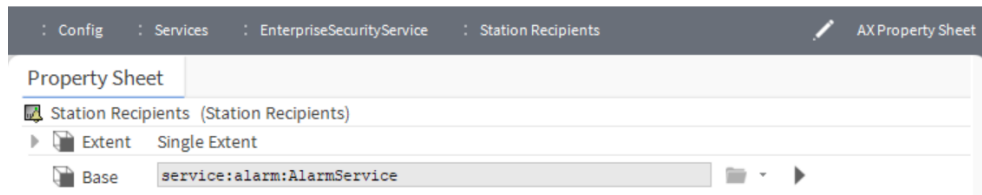
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
Base Extent	drop-down	
Base		

entsec-StationRecipients (WB Query Table View)

This component is used to route the alarms to get the notification.

Figure 459 Security Station Recipients properties



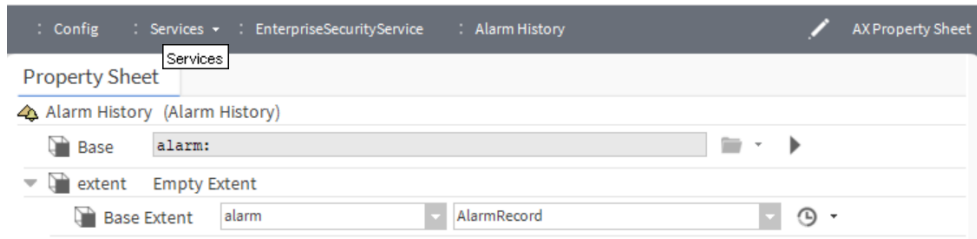
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
Base	text	

entsec-AlarmHistory (Wb Query Table View)

This component gives the information of routed **AlarmClass** to **AlarmConsole**.

Figure 460 Security Alarm History properties



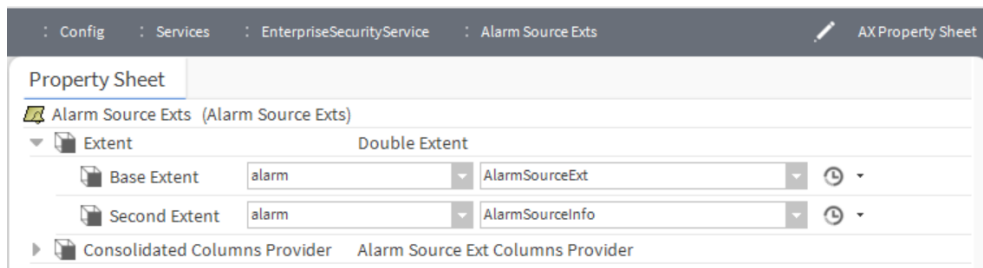
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Base	text	
Extent	drop-down	

entsec-AlarmSourceExts (Wb Query Table View)

This component

Figure 461 Security Alarm Source Exts properties



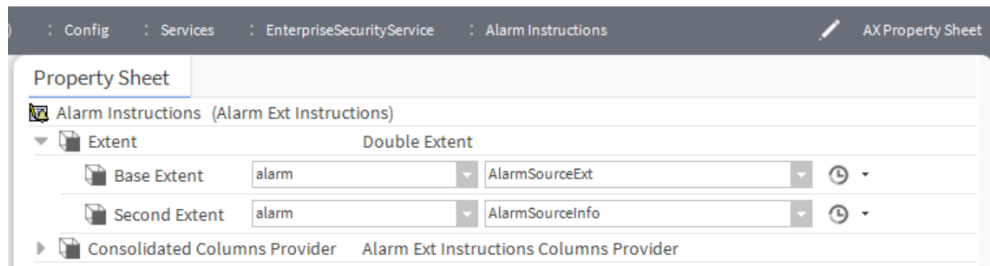
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent, Base Extent	drop-down	
Extent, Second Extent	drop-down	
Consolidated Columns Provider	separate slot	A separate topic documents this property.

entsec-AlarmExtInstructions (Wb Query Table View)

Each alarm can have customized instructions assigned to it so that any time an alarm is generated, the instructions are presented with the alarm notification (in the Alarm Record window). Alarm instructions provide information for the system operator. Instructions are created, assigned, and edited from the Instructions view.

Figure 462 Security Alarm Ext Instructions properties



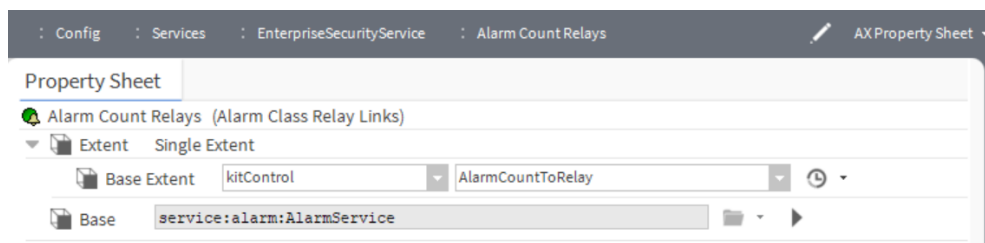
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
Base Extent	drop-down	
Second Extent	drop-down	
Consolidate Columns Provider	Alarm Ext Instructions Columns Provider	

entsec-AlarmClassRelayLinks (Wb Query Table View)

This component allows you to link from an **Alarm Class** component to monitor alarm count and send an associated boolean output to a relay whenever there is an increase in the alarm count.

Figure 463 Security Alarm Count Relays properties



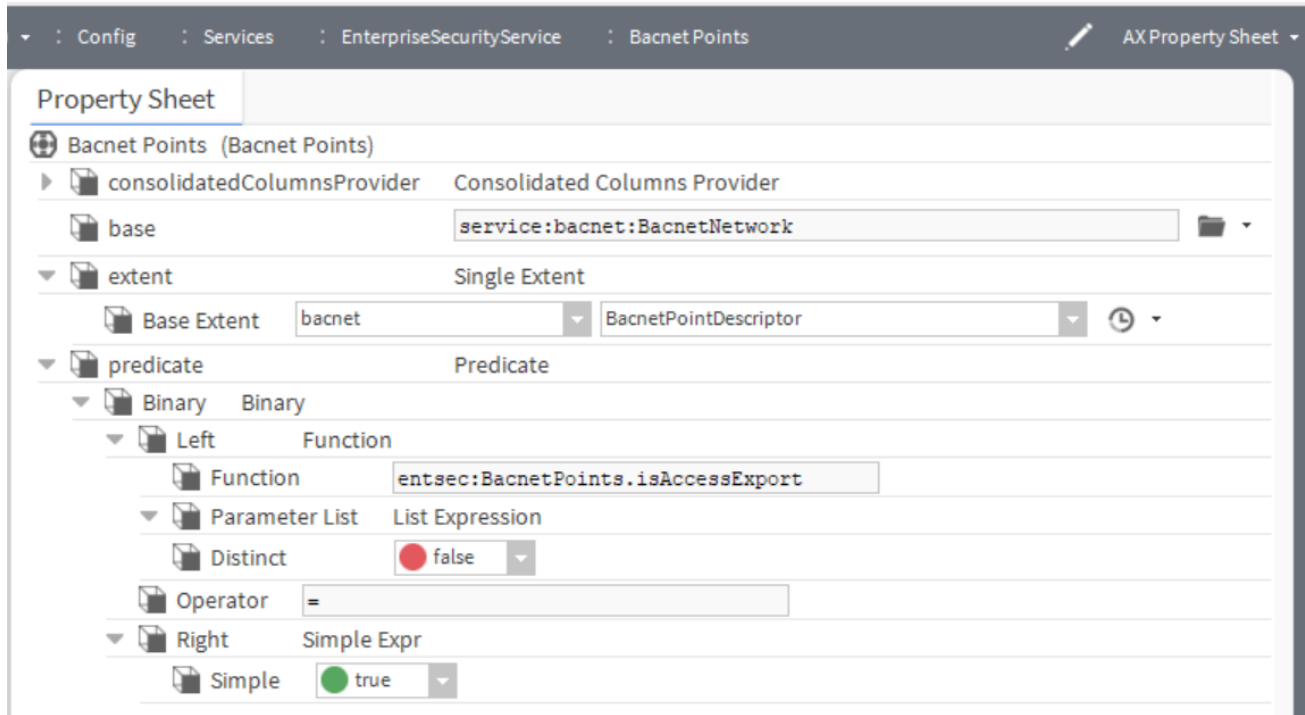
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
Base Extent		
Base	Path	

entsec-BacnetPoints (WB Query Table View)

The **BacnetPoints** component

Figure 464 Security Bacnet Points properties



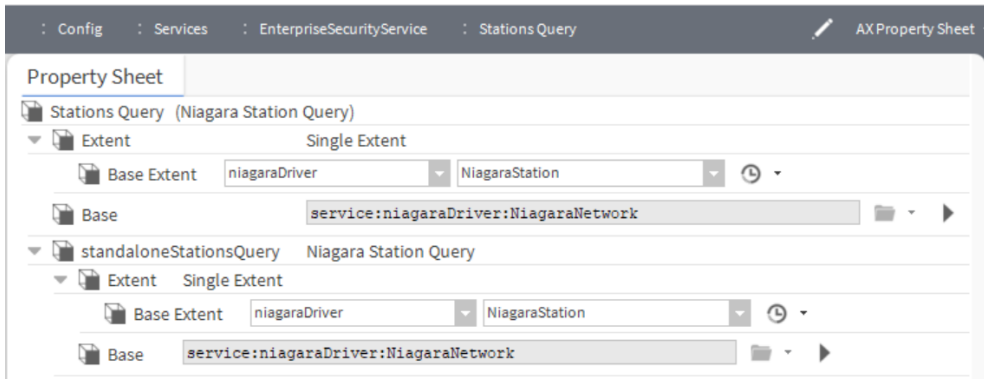
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
base	path	
extent	Single Extent	
Base Extent	drop-down	
Predicate	Predicate	
Function	path	
Parameter List	List Expression	
Distinct	true or false	
Operator		
Simple	true or false	

entsec-NiagaraStationQuery (WB Query Table View)

The `NiagaraStationQuery` component

Figure 465 Security Niagara Station Query properties



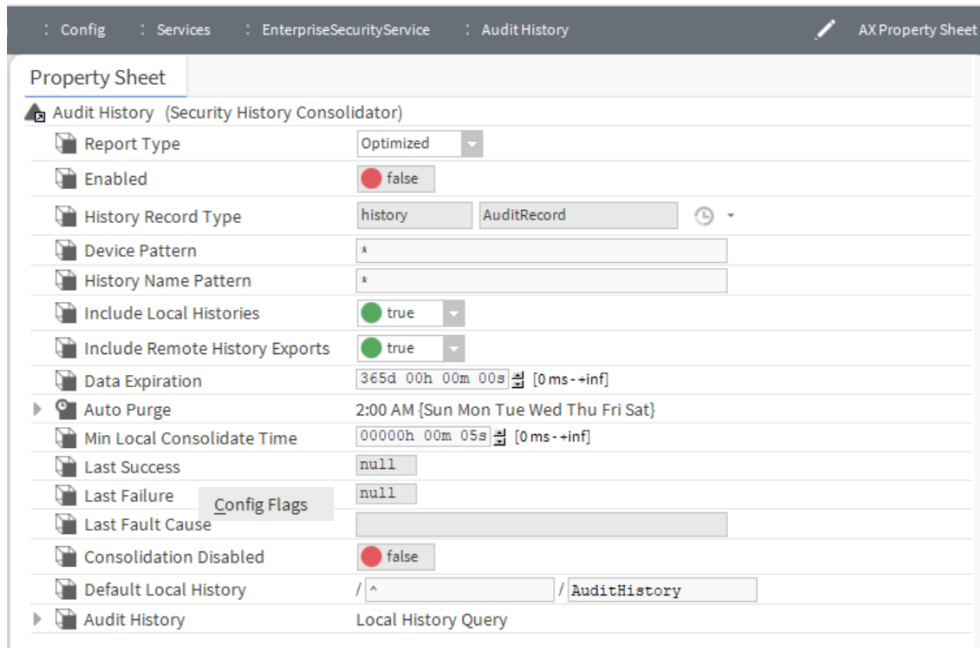
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
Base Extent	text	
Base	drop-down	
StandAloneStation-Query	Niagara Station Query	
Extent	Single Extent	
Base	drop-down	

entsec-SecurityAuditHistory (Orion History View)

This Service keeps a history of the changes that are made by users. When service starts it is register itself as the auditor for the system.

Figure 466 Security Audit History properties



You can access these property by double-clicking the **Services**→**AuditHistoryService** in Nav tree.

In addition to the standard properties (Enabled), this property is unique to this service:

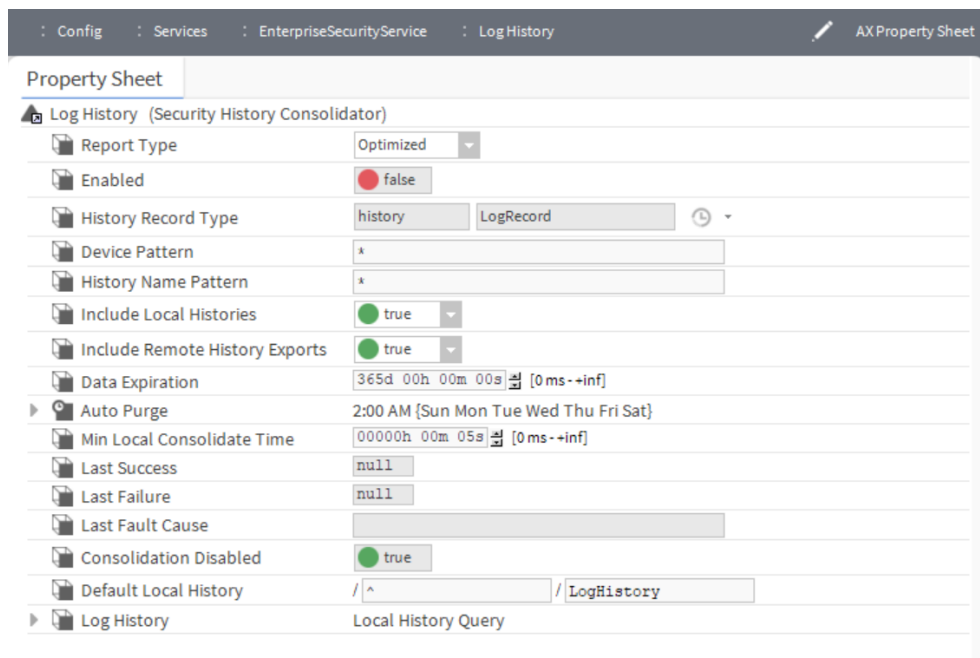
Property	Value	Description
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.
History Record Type	read-only	Reports the type of record.
Device pattern	text (defaults to *)	String matching to device names, meaning name of station(s) that are exporting histories Default value is a wildcard ("*"), meaning all station names are matched.
History Name Pattern	text (defaults to *)	String matching to history names of histories being exported. Again, default value is a wildcard ("*"), meaning all named histories are matched. NOTE: Both Device Pattern and History Name Pattern must apply for the rule to be used—otherwise the next rule down (in order) in History Policies is evaluated.
Include Local Histories	true (defaults) or false	
Include Remote History Exports	true (defaults) or false	
Data Expiration	days, hrs, mins, seconds	

Property	Value	Description
Auto Purge	all days of week	Specifies the days of the week.
Min Local Consolidate Time		
Last Success	null	
Last Failure	null	
Last Fault Cause	text	
Consolidation Disabled	true (defaults) or false	
Default Local History	text	
Audit History	default	

entsec-SecurityLogHistory (Orion History View)

This Service keeps a history of framework log records when it is enabled. This service maintains a buffered history ("LogHistory") of some of the messages seen in the station's standard output. This can be very helpful when you are troubleshooting problems with a station. If a station has Log History Service enabled, you can check the log history for recent error messages.

Figure 467 Security Log History properties



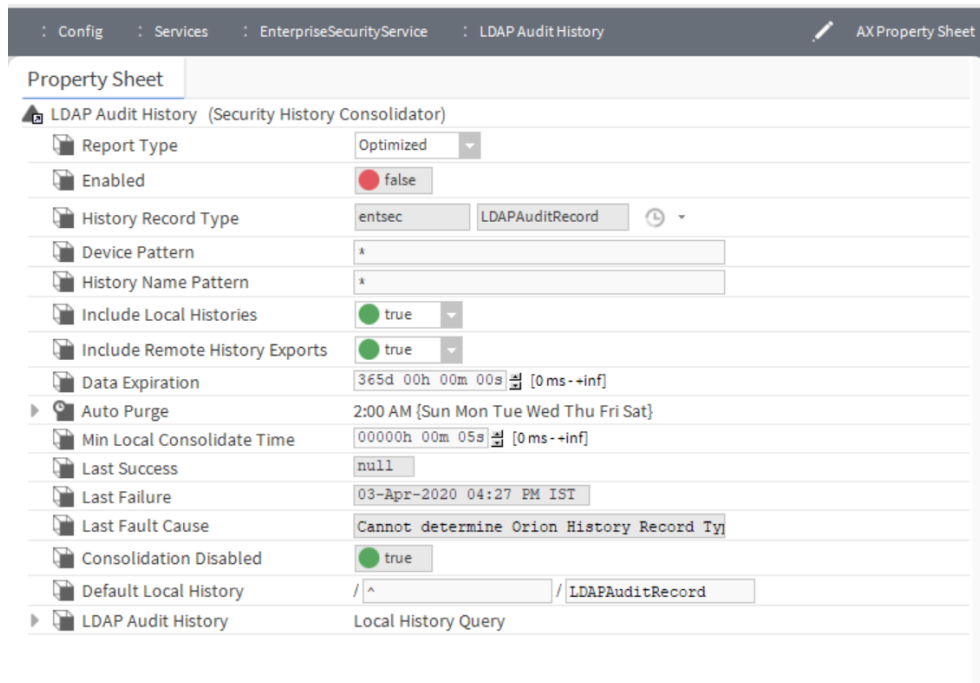
You can access these property by double-clicking the **Services**→**LogHistoryService** in Nav tree. In addition to the standard properties (Enabled). This property is unique to this service:

Property	Value	Description
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.
History Record Type	read-only	Reports the type of record.
Device pattern	text (defaults to *)	String matching to device names, meaning name of station(s) that are exporting histories Default value is a wildcard ("*"), meaning all station names are matched
History Name Pattern	text (defaults to *)	String matching to history names of histories being exported. Again, default value is a wildcard ("*"), meaning all named histories are matched. NOTE: Both Device Pattern and History Name Pattern must apply for the rule to be used—otherwise the next rule down (in order) in History Policies is evaluated.
Include Local Histories	true (defaults) or false	
Include Remote History Exports	true (defaults) or false	
Data Expiration	days, hrs, mins, seconds	
Auto Purge	all days of week	Specifies the days of the week.
Min Local Consolidate Time		
Last Success	null	
Last Failure	null	
Last Fault Cause	text	
Consolidation Disabled	true (defaults) or false	
Default Local History	text	
Log History	default	

entsec-SecurityHistoryConsolidator (Orion History View)

The `SecurityHistoryConsolidator` component

Figure 468 Security History Consolidator properties



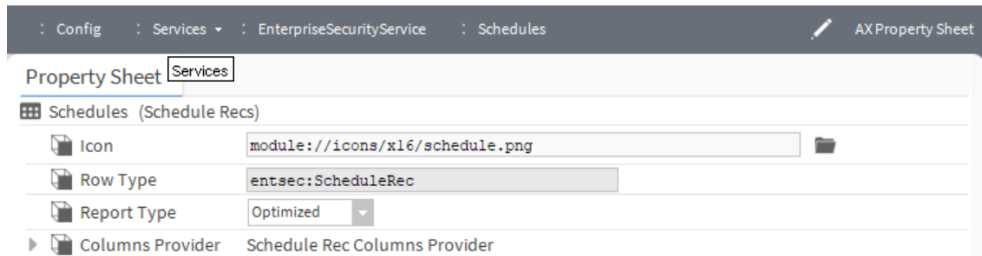
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree. In addition to the standard properties (Enabled). This property is unique to this service:

Property	Value	Description
Report Type	drop-down list	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.
History Record Type	read-only	Reports the type of record.
Device Pattern	text (defaults to *)	
History Name Pattern	text (defaults to *)	
Include Local Histories	true or false	
Include Remote History Exports	true or false	
Data Expiration	days, hrs, mins	
Auto Purge		
Min Local Consolidate Time		
Last Success	null	
Last Failure		
Last Fault Cause	text	

Property	Value	Description
Consolidation Disabled	true or false	
Default Local History		
LDAP Audit History	Local History Query	

entsec-ScheduleRecs (App Table View)

Figure 469 Security Schedule properties



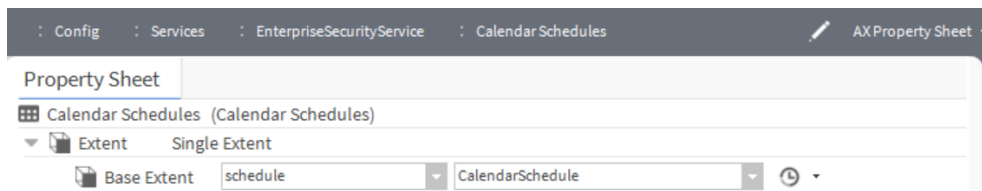
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Icon		
Row Type	Text	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.
Columns Provider		

entsec-CalendarSchedules (WB Query Table View)

The CalendarSchedule component provides a calendar for scheduling holidays or other schedule overrides.

Figure 470 Security Calendar Schedules properties



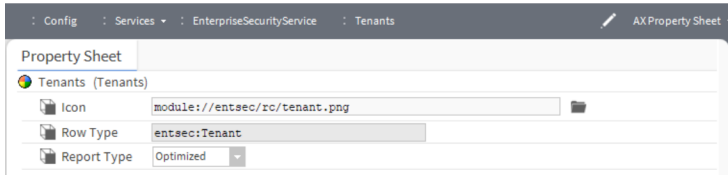
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Base	drop-down	

entsec-Tenants (App Table View)

Assigning a tenant to each personnel record allows the facility manager to demarcate a facility or an enterprise in a way that provides privacy, clarity, and flexibility for the user, tenant and owner. You may assign only one tenant to a person, whereas you may assign more than one tenant to a system user. Assigning a tenant to a user can limit the user’s access to certain areas of a system.

Figure 471 Security Tenants properties



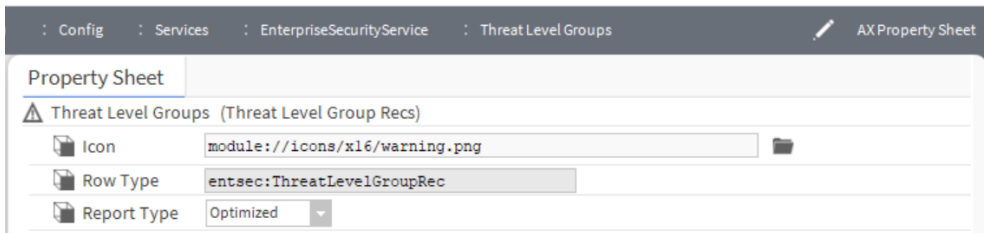
You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Icon	path	User can select the path
Row Type	text	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-ThreatLevelGroupRecs (Ac Table View)

The

Figure 472 Security Threat Level Groups properties

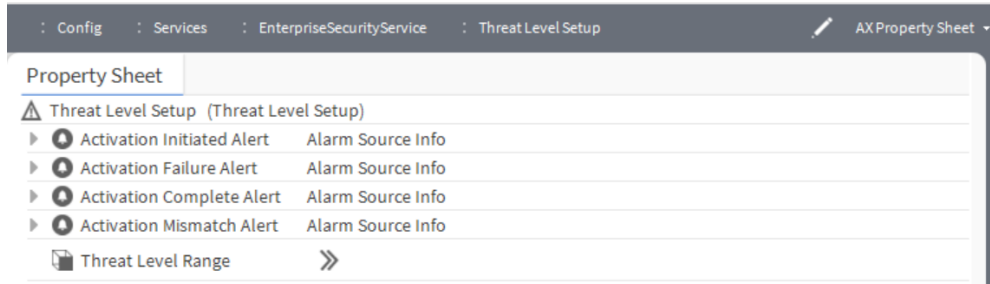


You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Icon	text	
Row Type	text	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-ThreatLevelSetup (AX Property Sheet)

Figure 473 Security Threat Level Setup properties

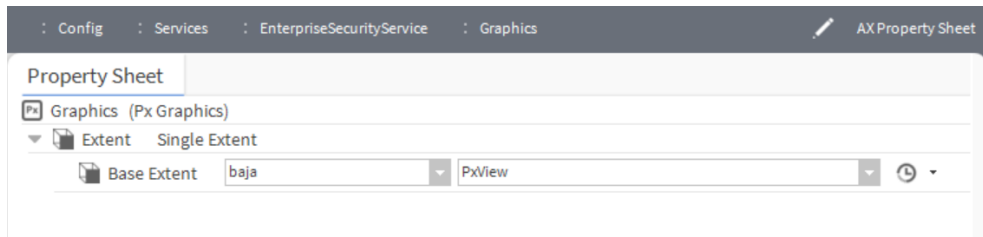


You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description

entsec-PxGraphics (WB Query Table View)

Figure 474 Security Graphics properties

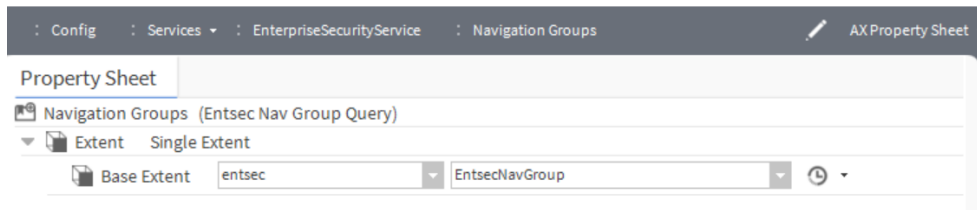


You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
Base	text	

entsec-EntsecNavGroupQuery (Wb Query Table View)

Figure 475 Security Navigation Groups properties



You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Base Extent	text	

entsec-ChangePassword (AX Property Sheet)

Figure 476

You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description

entsec-ChangePasskey (AX Property Sheet)

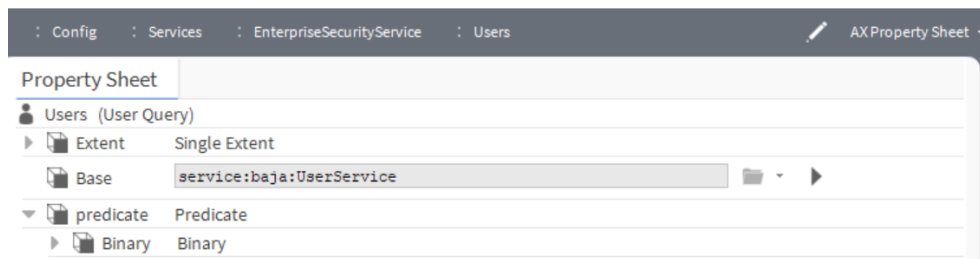
Figure 477

You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description

entsec-UserQuery (Wb Query Table View)

Figure 478 Security User Query properties

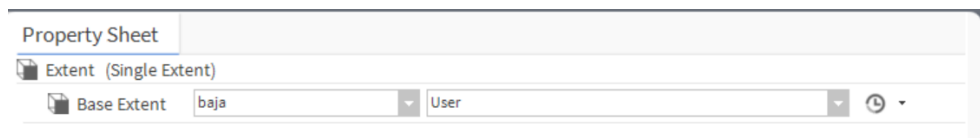


You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
predicate	predicte	

query-SingleExtent (AX Property Sheet)

Figure 479 Security query Single Extent properties

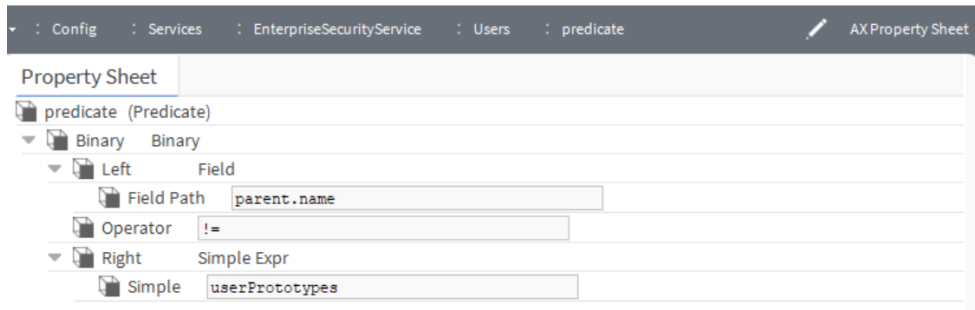


You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Extent	Single Extent	
Base	text	

query-Predicate (AX Property Sheet)

Figure 480 Security Predicate properties

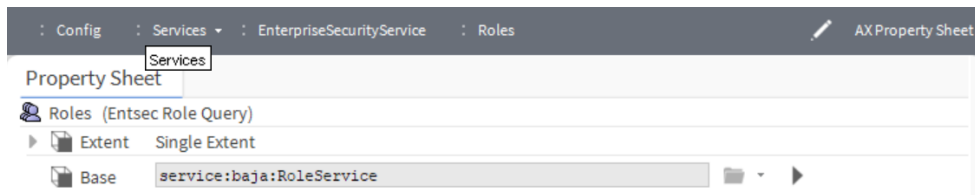


You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
Field Path	parent name	
Operator		
simple	text	

entsec-EntsecRoleQuery (Wb Query Table View)

Figure 481 Security Entsec Role Query

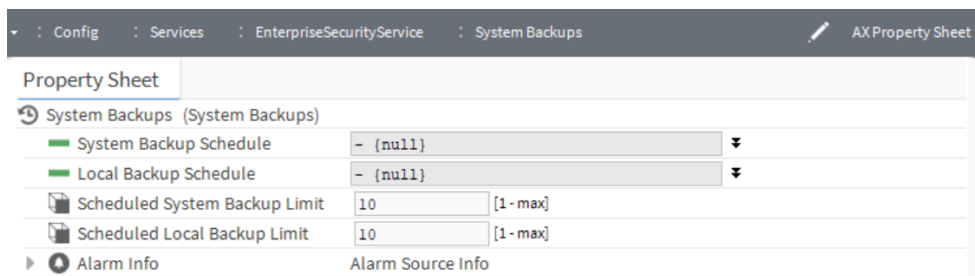


You can access these property by double-clicking the **Services**→**MonitorSysDefSecurity** in Nav tree.

Property	Value	Description
Base	text	

entsec-SystemBackups (AX Property Sheet)

Figure 482 Security System Backups properties

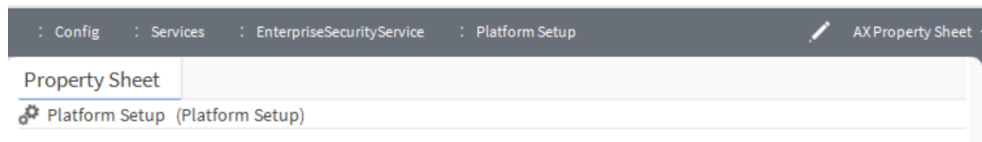


You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description
System Backup Schedule	null or true or false	
Local Backup Schedule	null or true or false	
Schedule System Backup Limit	number	As per requirement can select the value 1 – max.
Schedule Local Backup Limit	number	As per requirement can select the value 1 – max.

entsec-PlatformSetup (AX Property Sheet)

Figure 483 Security Platform Setup properties

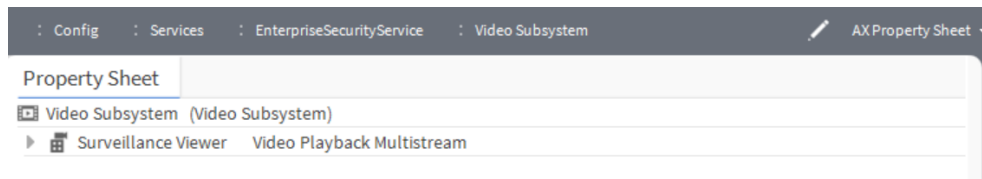


You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description

entsec-VideoSubsystem (AX Property Sheet)

Figure 484 Security Video Subsystem properties



You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description

entsec-EndUserLicenseAgreement (AX Property Sheet)

Figure 485 Security End User License Agreement properties

You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree.

Property	Value	Description

entsec-ThirdPartyLicenses (AX Property Sheet)

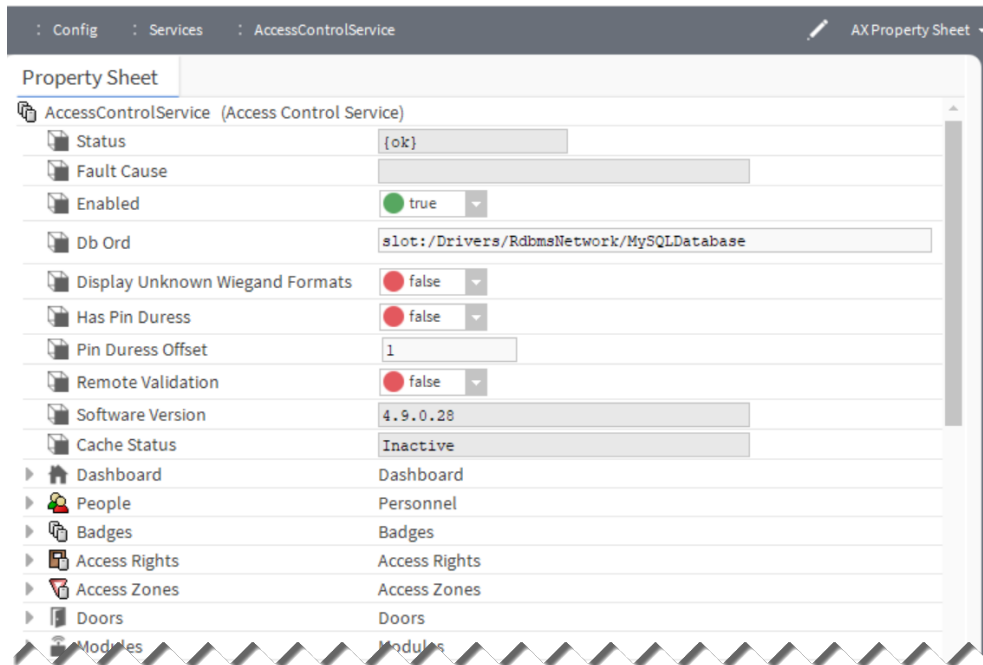
Figure 486 Security Third Party Licenses properties

You can access these property by double-clicking the **Services**→**EnterpriseSecurityService** in Nav tree. In addition to the standard properties (Enabled). This property is unique to this service:

Property	Value	Description

entsec-AccessControlService (AX Property Sheet)

Figure 487 Security Access Control Service properties



You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree. In addition to the standard properties (Enabled). this property is unique to this service:

Property	Value	Description
Db Ord	ORD	Identifies the location of the Orion database in the station.
Display Unknown Wiegand Formats	true or false	
Has pin Duress	true or false	
Pin Duress Offset	number	
Remote Validation	true or false	
Software Version	4.9.0.28	
Cache Status	Inactive	

entsec-Dashboard (AX Property Sheet)

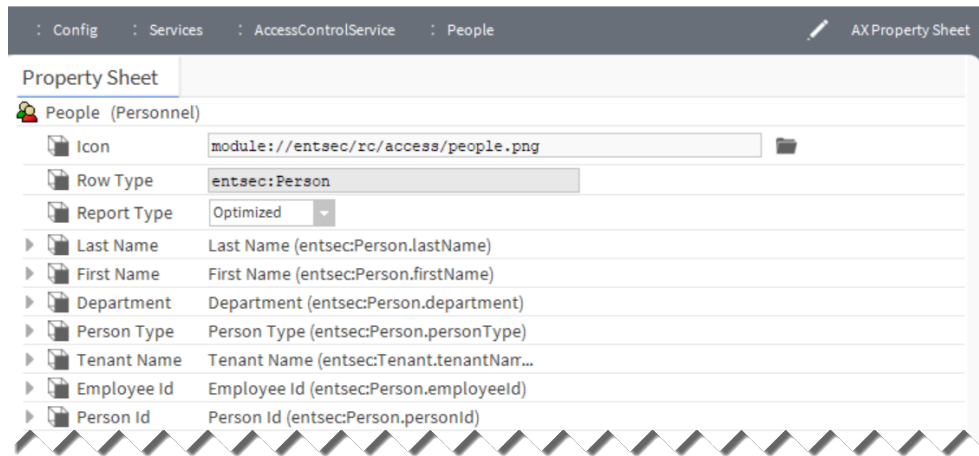
Figure 488 Security Access Control Service properties

You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description

entsec-Personnel (Ac Table View)

Figure 489 Security Personnel properties

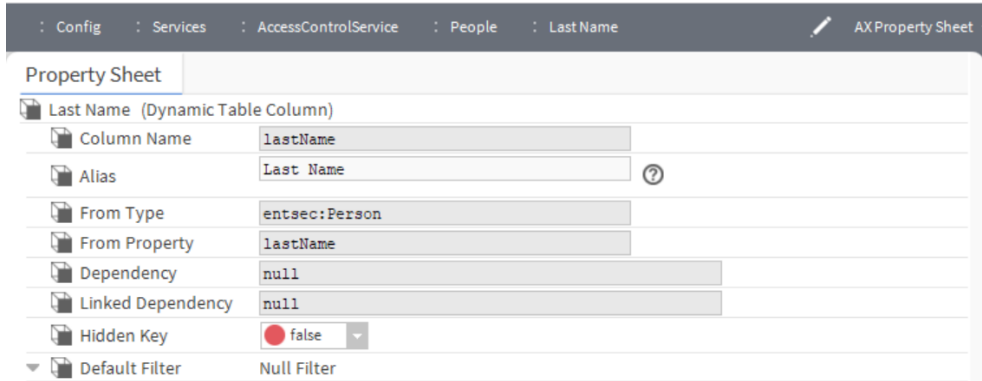


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:Person	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

orion-DynamicTableColumn (AX Property Sheet)

Figure 490 Security Access Control Service properties

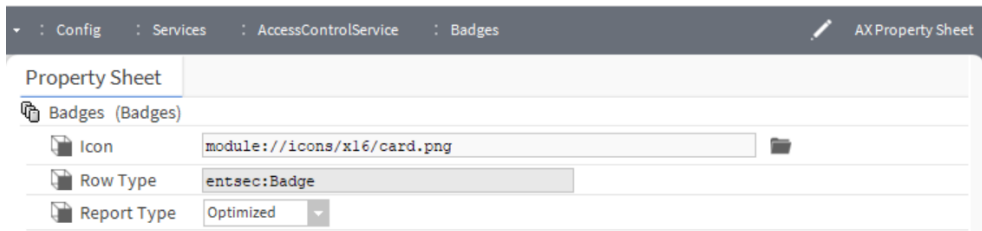


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Column Name	Last Name	
Alias	Last Name	
From Type	entsec:Person	
From Property	lastName	
Dependency	null	
Linked Dependency	null	
Hidden Key	true or false	
Default Filter	Null Filter	

entsec-Badges (Badges View)

Figure 491 Security Personnel properties

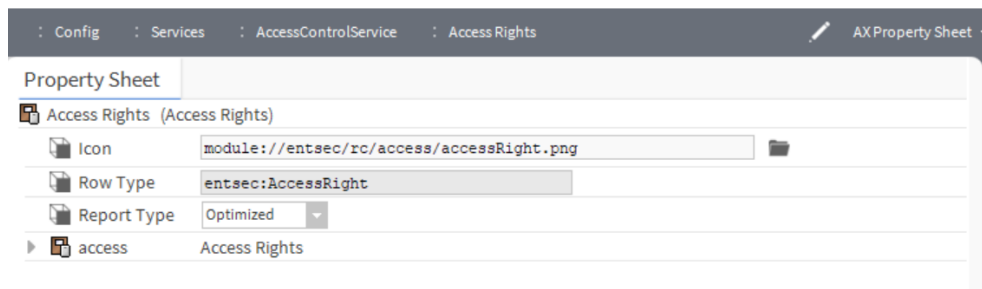


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:Badge	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-AccessRights (AC Table View)

Figure 492 Security Access Rights properties

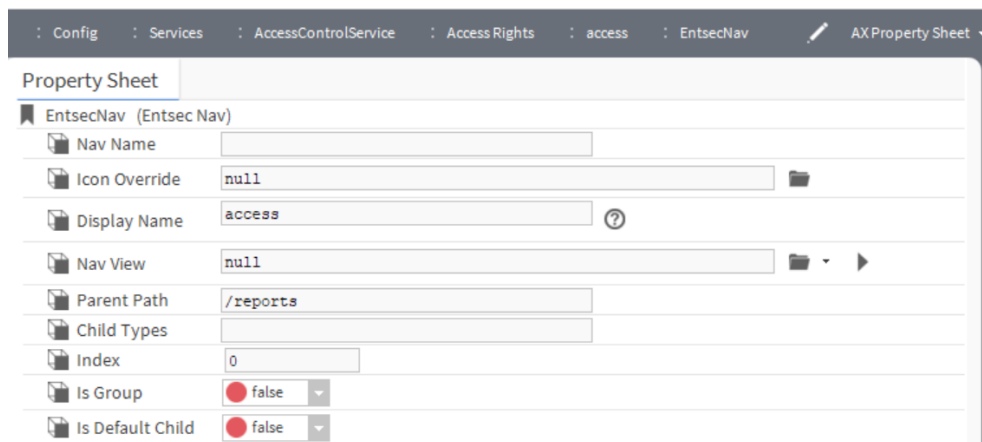


You can access these property by double-clicking the **Services→AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:AccessRight	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-EntsecNav (AX Property Sheet)

Figure 493 Security Entsec Nav properties

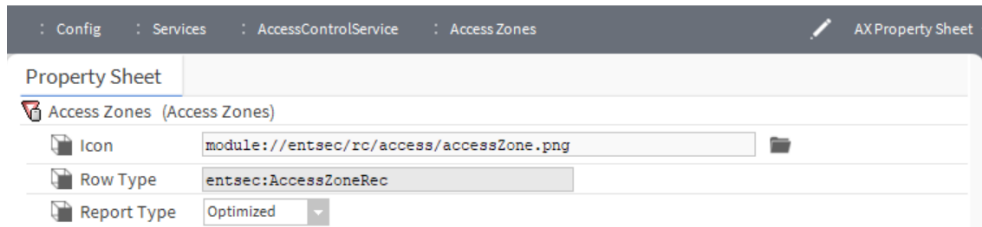


You can access these property by double-clicking the **Services**→**AccessControlService**→**AccessRight** in Nav tree.

Property	Value	Description
Nav Name	text	
Icon Override	null	
Display Name	access	
Nav View		
Parent Path		
Child Types		
Index		
Is Group	true or false	
Is Default Child	true or false	

entsec-AccessZones (AC Table View)

Figure 494 Security Access Zones properties



You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec: AccessZonesRec	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

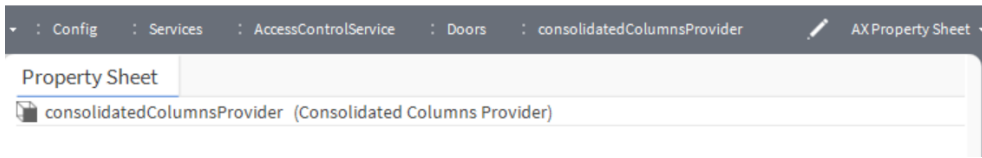
entsec-Doors (Wb Query Table View)

You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description

entsec-ConsolidatedColumnsProvider (AX Property Sheet)

Figure 495 Security Consolidated Columns Provider properties

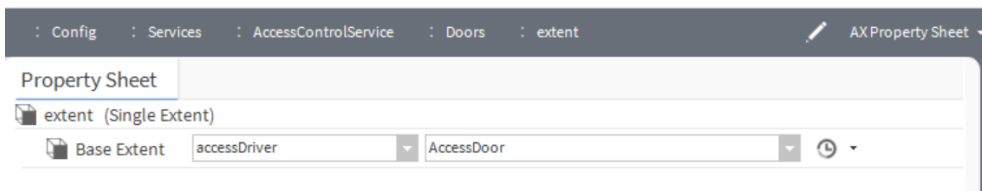


You can access these property by double-clicking the **Services**→**AccessControlService**→**entsec-Doors** in Nav tree.

Property	Value	Description

query-SingleExtent (AX Property Sheet)

Figure 496 Security Single Extent properties

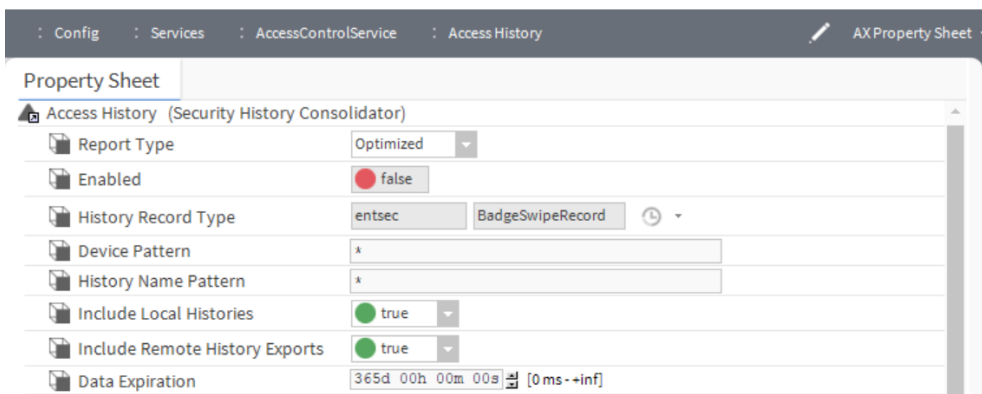


You can access these property by double-clicking the **Services**→**AccessControlService**→**entsec-Doors** in Nav tree.

Property	Value	Description
Base Extent	drop-down	

entsec-SecurityHistoryConsolidator (Orion History View)

Figure 497 Security History Consolidator properties

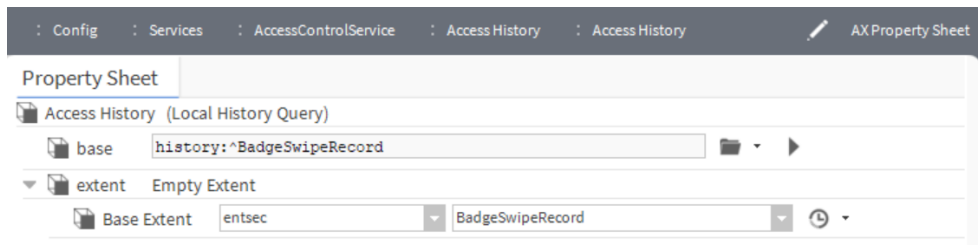


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.
History Record Type		
Device Pattern		
History Name Pattern	true or false	
Include Local Histories	true or false	
Include Remote History Exports		
Data Expiration	day, hr, min, sec	

entsec-LocalHistoryQuery (Wb Query Table View)

Figure 498 Security Local History Query properties

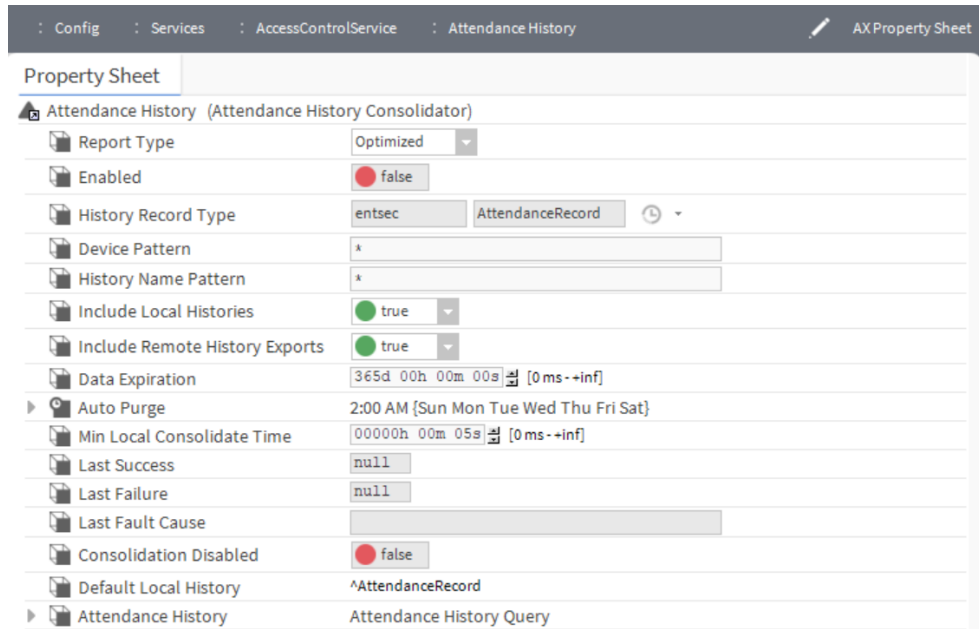


You can access these property by double-clicking the **Services**→**AccessControlService**→**AccessHistory** in Nav tree.

Property	Value	Description
base		
Base Extent	drop-down	

entsec-AttendanceHistoryConsolidator (Orion History View)

Figure 499 Security Attendance History properties



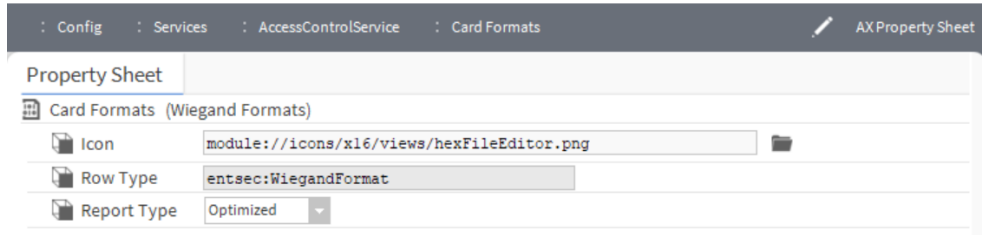
You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.
History Record Type		
Device Pattern		
History Name Pattern	true or false	
Include Local Histories	true or false	
Include Remote History Exports		
Data Expiration	day, hr, min, sec	
Min Local Consolidate Time	hr, min, sec	
Last Success	null	
Last Failure	null	
Last Fault Cause		

Property	Value	Description
Consolidation Disabled	true or false	
Default Local History	AttendanceRecord	

entsec-WiegandFormats (Ac Table View)

Figure 500 Security Wiegand Formats properties

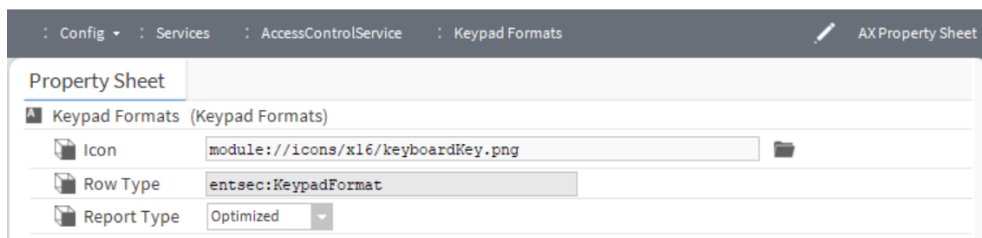


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:WiegandFormat	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-KeypadFormats (Ac Table View)

Figure 501 Security Keypad Formats properties

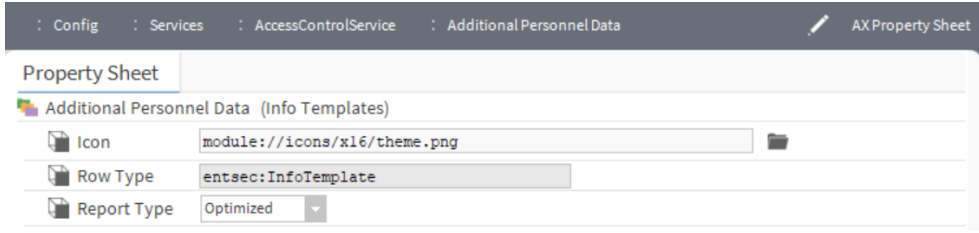


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:AccessRight	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-InfoTemplates (Ac Table View)

Figure 502 Security InfoTemplates properties

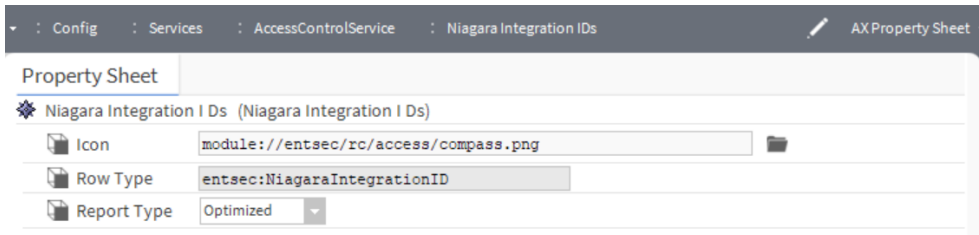


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec: InfoTemplate	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-NiagaraIntegrationIDs (Ac Table View)

Figure 503 Security Niagara Integration IDs properties

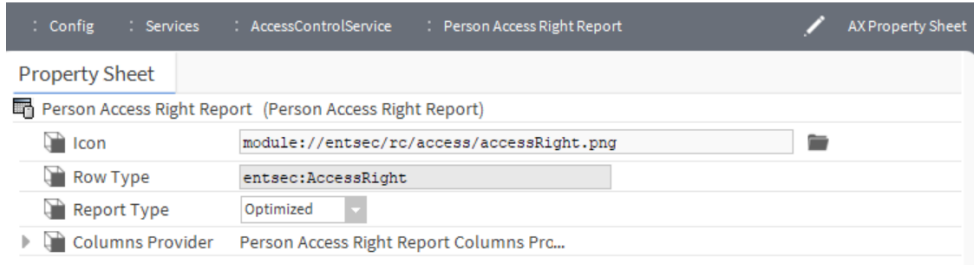


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:entsec-Ni- agaraIntegratio- nIDs	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-PersonAccessRightReport (App Table View)

Figure 504 Security Person Access Right Report properties

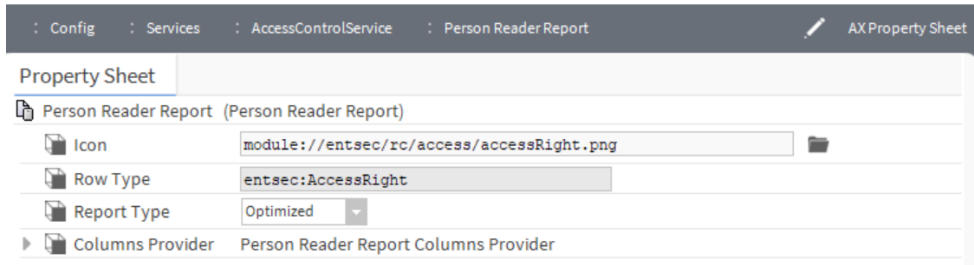


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:AccessRight	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-PersonReaderReport (App Table View)

Figure 505 Security Person Reader Report properties

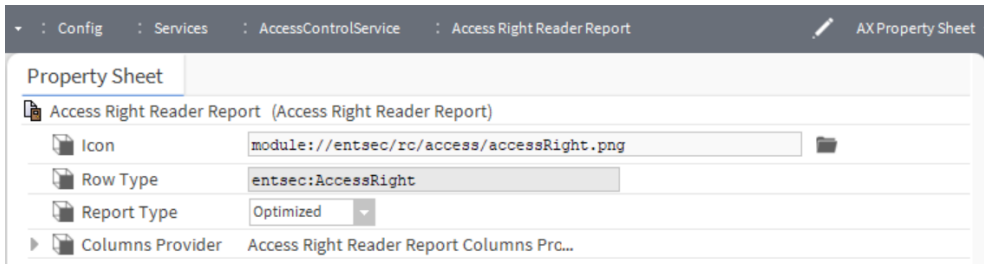


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:AccessRight	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-AccessRightReaderReport (App Table View)

Figure 506 Security Access Right Reader Report properties

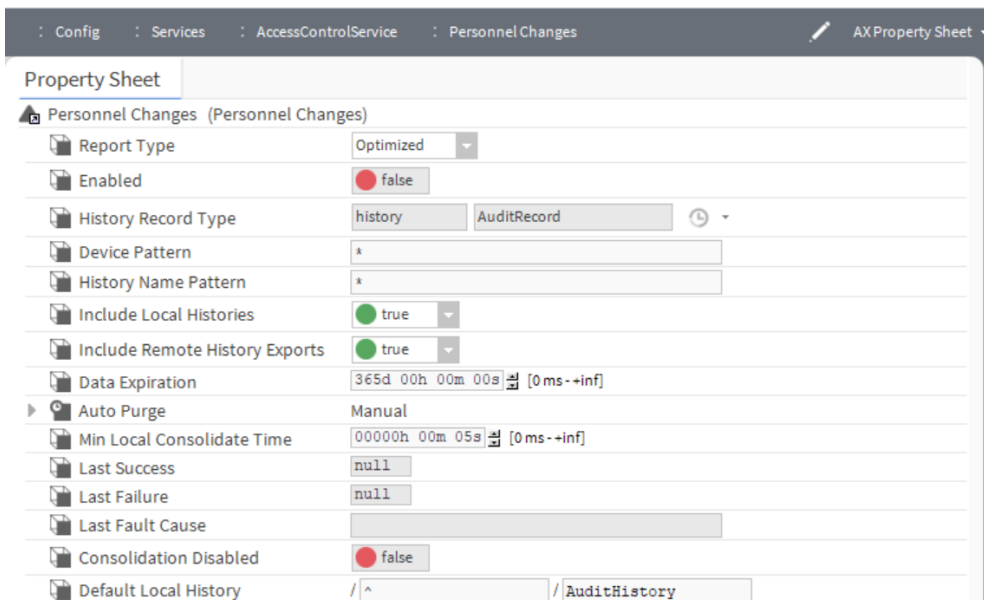


You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Icon	path	
Row Type	entsec:AccessRight	
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.

entsec-PersonnelChanges (Orion History View)

Figure 507 Security Personnel Changes properties



You can access these property by double-clicking the **Services**→**AccessControlService** in Nav tree.

Property	Value	Description
Report Type	drop-down	Selects how much data to report. Optimized limits the amount of data on the report. Full Report outputs all data.
History Record Type		
Device Pattern		
History Name Pattern	true or false	
Include Local Histories	true or false	
Include Remote History Exports		
Data Expiration	day, hr, min, sec	
Min Local Consolidate Time	hr, min, sec	
Last Success	null	
Last Failure	null	
Last Fault Cause		
Consolidation Disabled	true or false	
Default Local History	AttendanceRecord	

entsec-ReplicationService (AX Property Sheet)

Figure 508 Replication Service properties



You can access these property by double-clicking the **Services**→**ReplicationService** in Nav tree.

Property	Value	Description
State	read-only	

Chapter 20 Workbench components in the accessDriver module

Topics covered in this chapter

- ◆ accessDriver-AccessAlarmSourceExt
- ◆ accessDriver-AccessDoor
- ◆ accessDriver-AccessElevator
- ◆ accessDriver-AccessFloor
- ◆ accessDriver-AccessInputOutputModule
- ◆ accessDriver-AccessNetwork
- ◆ accessDriver-AccessProxyExt
- ◆ accessDriver-AccessReader
- ◆ accessDriver-AccessRex
- ◆ accessDriver-AccessSdi
- ◆ accessDriver-AccessStrike
- ◆ accessDriver-Remote2ReaderModule
- ◆ accessDriver-Remote2ReaderPoints
- ◆ accessDriver-ActivityAlertExt

Components include services, folders and other model building blocks. You may drag them onto a property or wire sheet from a palette. These components configure system stations using Workbench.

The descriptions included in the following topics appear as headings in documentation. They also appear as context-sensitive help topics when accessed by:

- Right-clicking on the component and selecting **Views→Guide Help**
- Clicking **Help→Guide On Target**.

accessDriver-AccessAlarmSourceExt

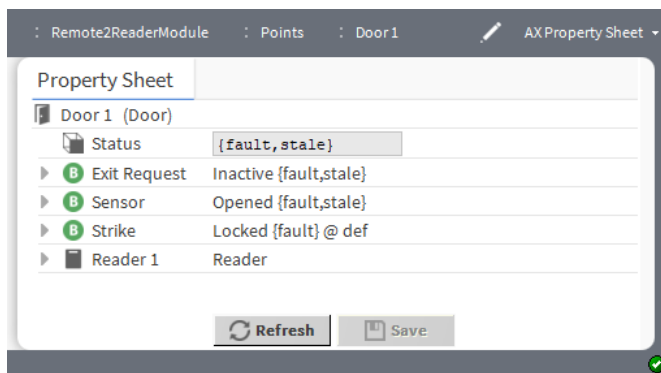
This component provides alarm configuration properties for the **accessDriver**.

The properties you can configure are the same as those for other drivers and components. Refer to the Alarms Guide.

accessDriver-AccessDoor

This component represents the security configuration for a single door.

Figure 509 Door properties



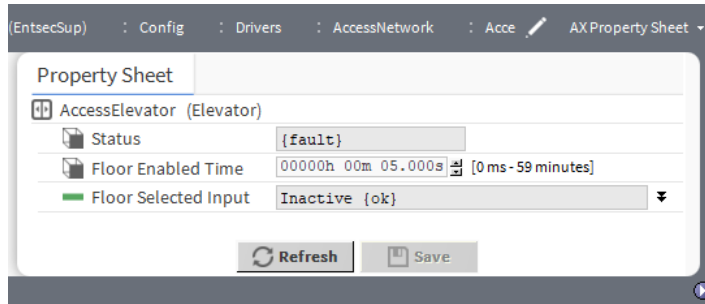
To access this component, expand the **AccessNetwork**→**Remote2ReaderModule**→**Points** container, right-click a **Door** node in the Nav tree and click **Views**→**AX Property Sheet**.

Each door has three Boolean digital inputs: Exit Request, Sensor and Strike, and a Reader. Each digital input and reader is a component in its own right with associated properties.

accessDriver-AccessElevator

This component configures elevator properties.

Figure 510 Elevator properties



You add this component to the **AccessNetwork** node in the station from the **accessDriver** palette. Once in the station, double-click this node to view its properties.

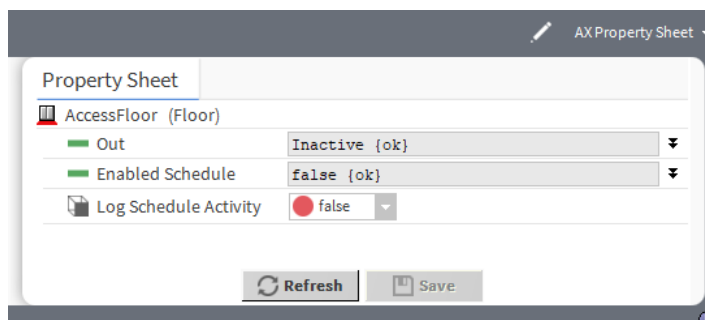
In addition to the standard properties (Status) these properties configure this component:

Property	Value	Description
Floor Enabled Time	hours minutes seconds (defaults to 5 seconds in a range from 0 ms to 59 minutes)	Sets the amount of time that the elevator floor button is active after access is granted to the floor.
Floor Selected Input	null, Inactive (default) or Active	A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.

accessDriver-AccessFloor

This component configures floor properties.

Figure 511 Access Floor properties



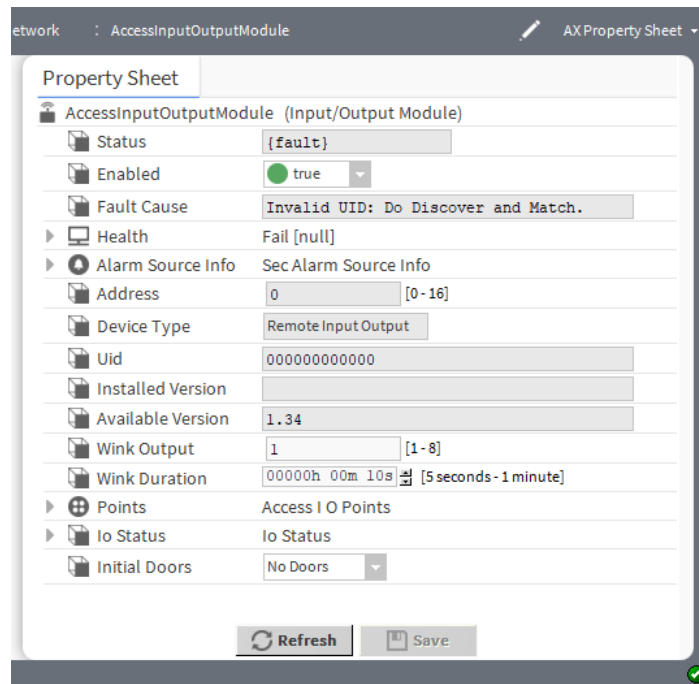
You add this component to the **AccessNetwork** node in the station from the **accessDriver** palette. Once in the station, double-click this node to view its properties.

Property	Value	Description
Out	null, Inactive (default) or Active	A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Enabled Schedule	null, true or false (default)	A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Log Schedule Activity	true or false (default)	Determines the creation a log record when a schedule controls activity at the elevator. true creates a record in the Access History report when a schedule controls activity the elevator. false does not record the scheduled activity.

accessDriver-AccessInputOutputModule

This component configures an I/O module.

Figure 512 Input/Output Module properties



You add this component to the **AccessNetwork** node in the station from the **accessDriver** palette. Once in the station, double-click this node to view its properties.

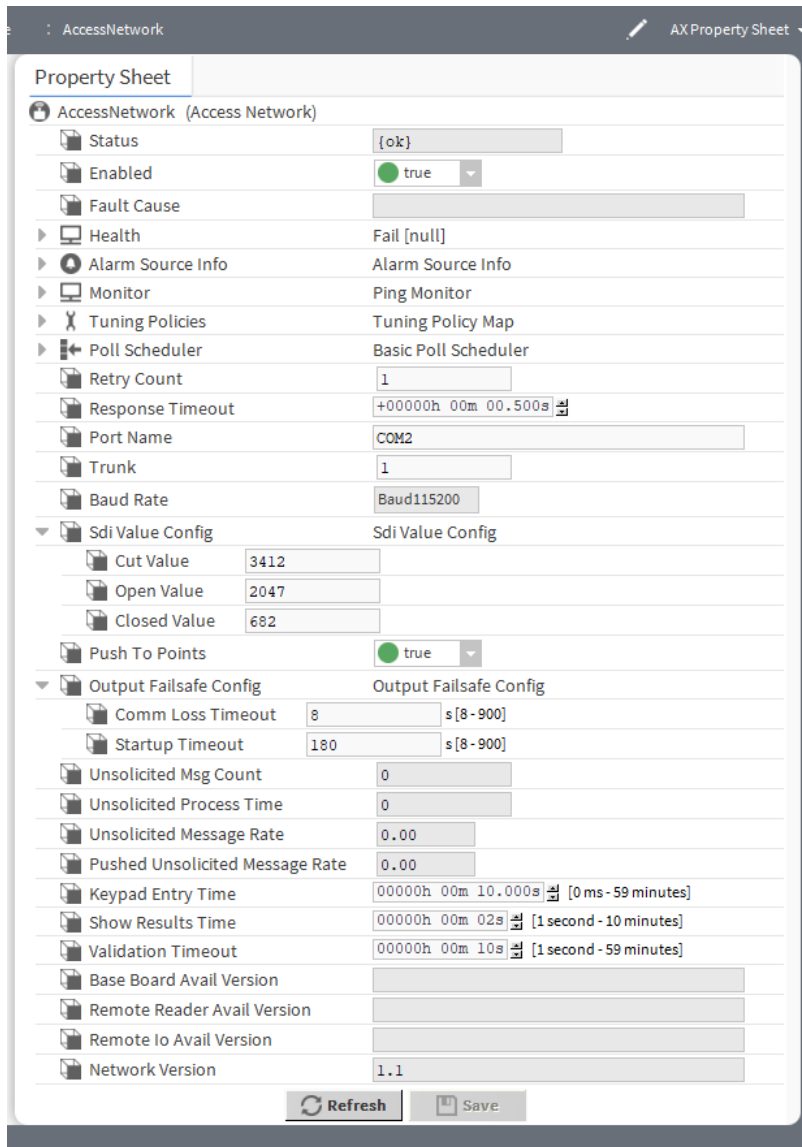
In addition to the standard properties (Status, Enabled, Fault Cause, Health and Alarm Source Info), these properties support this component:

Property	Value	Description
Address	read-only	Reports the unique integer value automatically assigned to each physical I/O module during discovery.
Device Type	read-only	Identifies the type of remote device.
Uid	read-only	Reports a six-byte number that is globally unique to this specific I/O hardware device. Discovery automatically obtains this Unique ID (Uid) from each device.
Installed Version	read-only	Reports the firmware version installed in the I/O module or device.
Available Version	read-only	Reports the firmware version available for the installed module. If this number is more recent (higher) than the installed version, you can initiate an I/O firmware upgrade from the Device Manager.
Wink Output	number (defaults to 1)	(Writable) Specifies which digital output (relay output) is cycled On and Off when a Wink Device action is invoked on the module. Although the range is from 1 to 8, the I/O hardware may have fewer outputs.
Wink Duration	hours minutes seconds (defaults to 10 seconds)	(Writable) Specifies how long the wink output cycles on and off at a constant rate of 1 second on followed by 1 second off. NOTE: Wink is typically used only in the early stages of station configuration. After configuring, you may hide the Wink Device action to prevent inadvertent and unintended cycling of loads.
Points	points container	Documented elsewhere.
Io Status	additional properties	Contains a concatenated summary of current IO values in hexadecimal coded format, and numerous component children with individual hexadecimal values. These are the last values received by the actrlid process running on the controller. This information is usually used for advanced debugging only.
Initial Doors	drop-down list (defaults to Two Doors)	Defines the number of doors. No Doors One Door Two Doors

accessDriver-AccessNetwork

This component manages and configures the access network.

Figure 513 AccessNetwork properties



To open this Property Sheet, right-click the AccessNetwork node in the Nav tree and click **Views→AX Property Sheet**.

In addition to the standard properties (Status, Enabled, Fault Cause, Health, Alarm Source Info, Monitor, Tuning Policies and Poll Scheduler), these properties configure this component:

Property	Value	Description
Retry Count	number	Configures how many times to repeat a network read request, if no response is received before the response timeout interval elapses.
Response Timeout	hours minutes seconds (defaults to .500 seconds)	Configures the length of time before the system times out when interrogating a device on the network. Start by setting this value to a large number, such as 40 seconds. Then, reduce it depending on the number of devices and on the discovery performance.

Property	Value	Description
		NOTE: Baud rate also impacts performance especially if each device has a different baud rate.
Port Name	COM2, COM3	Defines the communication port to use: <i>none</i> , COM2 or COM3.
Trunk	number	Each RS-485 connection is called a trunk. If your network has multiple RS-485 trunks, a separate network and remote I/O module is required to support each. This property specifies which trunk the port is connected to.
Baud Rate	read-only	Defines communication speed in bits per second.
Sdi Value Config	additional properties	Sdi (Sensor Digital Interface) configures input from the sensor. Refer to Sdi Value Config, page 515 .
Push To Points	true (default) or false	Enables (<i>true</i>) and disables (<i>false</i>) the sending of data to points.
Output Failsafe Config	read-only seconds (defaults to 8)	Configures timeout values. Refer to Output Failsafe Config, page 515 .
Unsolicited Msg Count	read-only	Reports the number of unexpected messages.
Unsolicited Process Time	read-only	Reports the amount of unexpected process time.
Unsolicited Message Rate	read-only	Reports the rate at which unexpected messages are being received.
Pushed Unsolicited Message Rate	read-only	Reports the rate at which unexpected messages are being sent.
Keypad Entry Time	hours minutes seconds (defaults to 10 seconds)	Configures an amount of time.
Show Results Time	hours minutes seconds (defaults to 2 seconds)	Configures an amount of time.
Validation Timeout	hours minutes seconds (defaults to 10 seconds)	Configures an amount of time.
Base Board Avail Version	read-only	Reports a version number.
Remote Reader Avail Version	read-only	Reports a version number.
Remote Io Avail Version	read-only	Reports a version number.
Network version	read-only	Reports a version number.

Sdi Value Config

Figure 514 Sdi Value Config properties

Sdi Value Config		Sdi Value Config
Cut Value	<input type="text" value="3412"/>	
Open Value	<input type="text" value="2047"/>	
Closed Value	<input type="text" value="682"/>	

Property	Value	Description
Cut Value	number (defaults to 3412)	Defines a value for the cut voltage parameter on the network.
Open Value	number (defaults to 2047)	Defines a value for the open voltage parameter on the network.
Closed Value	number (defaults to 682)	Defines a value for the close voltage parameter on the network.

Output Failsafe Config

Figure 515 Output Failsafe Config properties

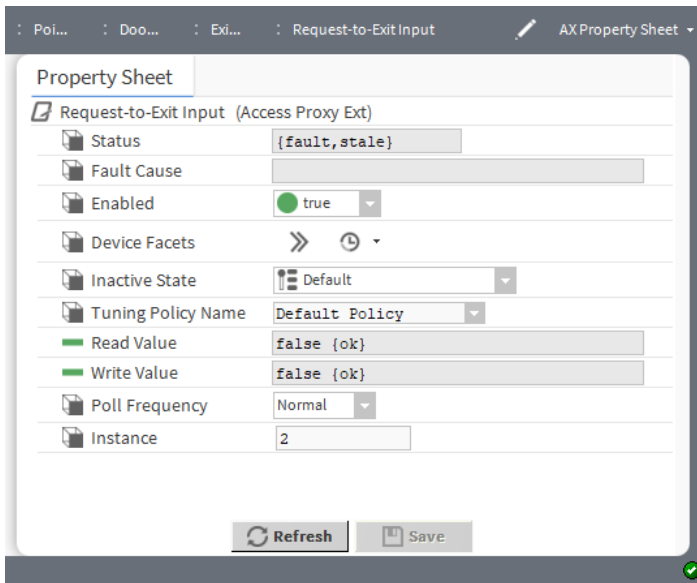
Output Failsafe Config		Output Failsafe Config
Comm Loss Timeout	<input type="text" value="8"/>	s [8 - 900]
Startup Timeout	<input type="text" value="600"/>	s [8 - 900]

Property	Value	Description
Comm Loss Timeout	seconds (defaults to 8 seconds)	Defines a number of seconds after which the station stops sending data, thereby indicating a loss of communication signal.
Startup Timeout	seconds (defaults to 180 seconds)	Defines a number of seconds after which the startup times out.

accessDriver-AccessProxyExt


This component configures the request-to-exit input associated with a specific door. This proxy extension serves the Request-to-Exit, Sensor and Strike components.

Figure 516 Example of accessDriver proxy extension properties



To access one of these components, expand the **AccessNetwork**→**Remote2ReaderModule**→**Points** in the Nav tree, then expand any of the Boolean points that have a **Proxy Ext** and double-click the node. Each door component's **Exit Request** has a similar component: **Request-to-Exit Input**. Each Sensor's **Sensor Input** component is also a proxy extension.

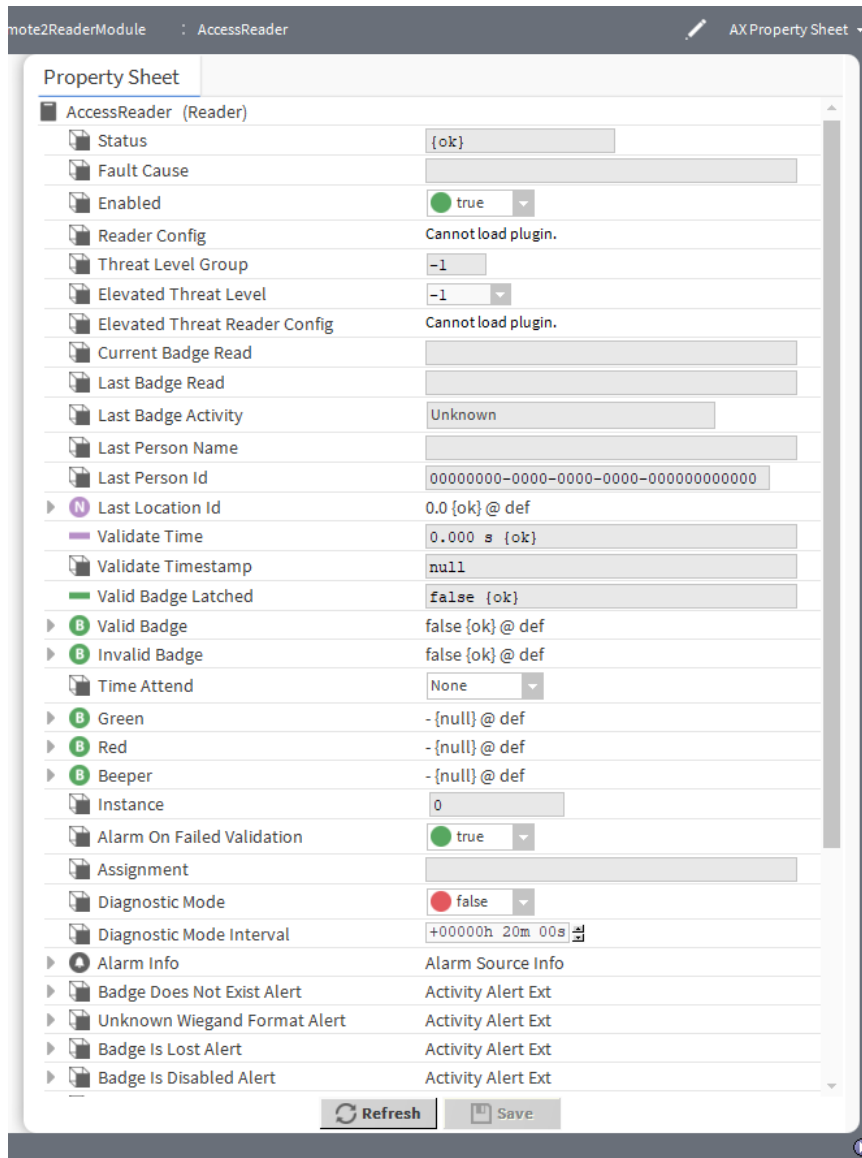
In addition to the standard properties (Status, Fault Cause, Enabled, Device Facets, Tuning Policy Name and Poll Frequency), these unique properties support this component:

Property	Value	Description
Inactive State or Closed State (Sensory Input)	drop-down list (defaults to <code>Default</code> for most components; for <code>Sensory Input</code> defaults to <code>Reverse Polarity</code>)	<p>Configures the type of facet conversion for a specific point.</p> <p><code>500 Ohm Shunt (nr10)</code> applies only to a voltage input point used to read a 4–to-20mA sensor where the UI input requires a 500 ohm resistor wired across (shunting) the input terminals. The input signal is 2 to 10V. Compared to a linear or generic tabular conversion, the 500–Ohm-Shunt conversion provides better resolution near the upper (20mA/10V) input range. This compensates for input clamping protection and the circuitry automatically applies when input voltage rises above 3.9V.</p> <p><code>Default</code> automatically converts between similar units.</p> <p><code>Linear</code> applies to voltage input, resistive input and voltage output writable points, which, typically, need point output values in some units other than device facets (voltage or resistance).</p> <p><code>Linear With Unit</code></p> <p><code>Reverse Polarity</code> applies only to a Boolean input point or relay output writable. It reverses the logic of the hardware binary input or output.</p> <p><code>Tabular Thermistor (nr10)</code> provides an edit button () that opens a window for editing the current ohms-to-degrees Celsius curve used by the proxy point, importing another thermistor curve (.xml file) or exporting (saving) the current thermistor curve as an .xml file.</p> <p><code>Thermistor Type 3 (nr10)</code> applies only to a thermistor input point, where it provides a built-in input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p>
Read Value	read-only	Reports the value read from the access point.
Write Value	read-only	Reports the value written to the access point.
Instance	number (defaults to 2)	Corresponds to the point's I/O terminal address. It is recommended to leave this property at the default.

accessDriver-AccessReader

This component configures an access reader.

Figure 517 Access Reader properties



You add this component to the **AccessNetwork** node in the station from the **accessDriver** palette. Once in the station, double-click this **AccessReader** node to view its properties.

In addition to the standard properties (Status, Fault Cause, and Enabled), these properties support this component:

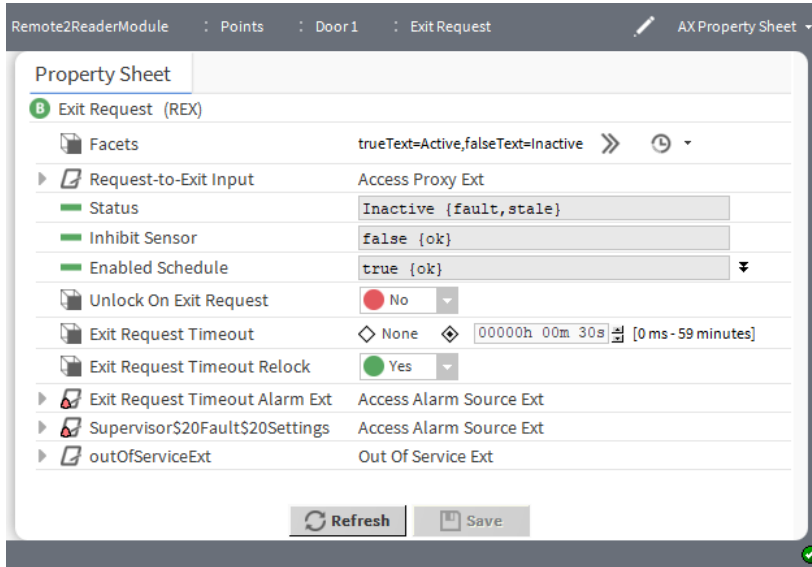
Property	Value	Description
Reader Config	additional properties	Sets up the required hardware to validate an entry request, as well as a request to arm or disarm an intrusion zone.
Threat Level Group	read-only	Reports the currently-assigned threat level group.
Elevated Threat Level	drop-down list	Defines a threat level for changing the reader configuration. The default ignores any active threat level changes.

Property	Value	Description
Elevated Threat Reader Config	drop-down list	Specifies a reader configuration to enable when the active threat level matches or exceeds the Elevated Threat Level1 .
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.
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.
Last Location Id	proxy extension	This is a standard Numeric Writable proxy extension.
Validate Time	read-only seconds	Reports the time taken to validate the badge.
Validate Timestamp	read-only	Reports when the system validated the badge.
Valid Badge Latched	read-only true or false	Indicates if the badge successfully latched the door.
Valid Badge	additional properties	This is a standard Boolean Writable component.
Invalid Badge	additional properties	This is a standard Boolean Writable component.
Time Attend	drop-down list	None Clock In Clock Out
Green	additional properties	This is a standard Boolean Writable component.
Red	additional properties	This is a standard Boolean Writable component.
Beeper	additional properties	This is a standard Boolean Writable component.
Instance	read-only	Reports the current number.
Alarm On Failed Validation	true (default) or false	Configures the driver to generate an alarm if account validation fails.
Assignment	read-only	
Diagnostic Mode	true or false (default)	Enables and disables the ability to see the keypad PIN. true displays the PIN so that the super user, who is configuring the reader, can confirm that the correct PIN was entered during testing. false hides the PIN. This is the obvious setting for normal operations.

Property	Value	Description
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.

accessDriver-AccessRex

Figure 518 Exit Request properties



To access this component, expand the **AccessNetwork**→**Remote2ReaderModule**→**Points**→**Door**, and double-click the **Exit Request** node in the Nav tree.

In addition to the standard properties (Facets), these unique properties support this component:

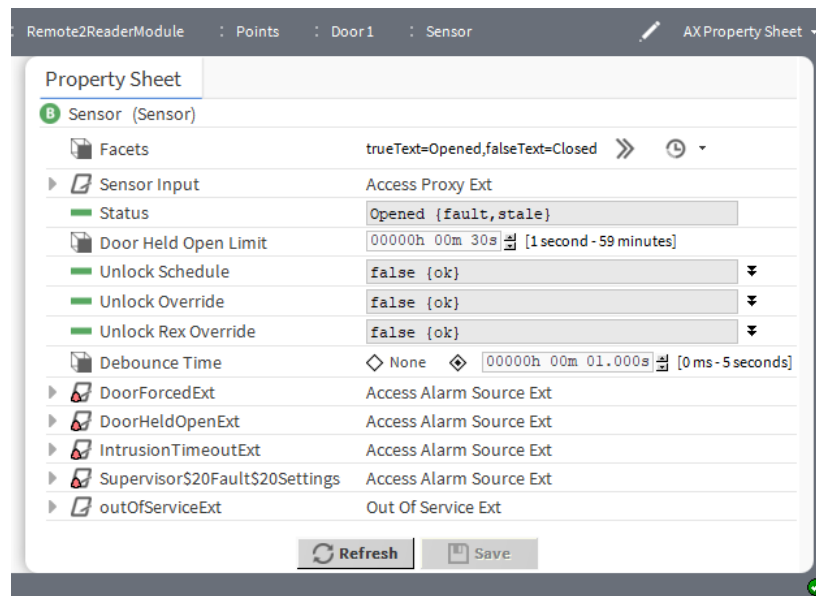
Property	Value	Description
Request-to-Exit Input	additional properties	This proxy extension component is documented in a separate topic.
Status	read-only	Indicates the current state of the sensor (<i>Active</i> or <i>Inactive</i>), and its status {ok}, or other possibilities.
Inhibit Sensor	read-only true or false	Indicates what happens to a door-forced-open alarm during an exit request. true indicates that the door-forced-open alarm stays inhibited during an exit request. This is only possible if Status is <i>Active</i> and Enabled Schedule is true. If either changes, Inhibit Sensor changes from true to false after a time that is equal to the Access Unlock Time . false indicates the door-forced-open alarm manifests during an exit request.
Enabled Schedule	null, true (default) or false	Indicates if a schedule exists.

Property	Value	Description
		A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Unlock on Exit Request	yes or no (default)	Allows an exit request to unlock a door.
Exit Request Timeout	None or hours minutes seconds (defaults to 30 seconds)	Configures an amount of time for the person who requested an exit to pass through the door before the door locks again. This component is documented in a separate topic.
Exit Request Timeout Relock	true (default) or false	Configures whether or not the door locks after the exit request timeout.
Exit Request Timeout Alarm Ext	additional properties	This alarm-source-extension component is documented in a separate topic.
Supervisor Fault Settings	additional properties	This alarm-source-extension component is documented in a separate topic.
outOfServiceExt	BACnet extension	This out-of-service component is documented in a separate topic.

accessDriver-AccessSdi

This component configures a Sensor Digital Input (Sdi).

Figure 519 Sensor properties



To access this component, expand the **AccessNetwork**→**Remote2ReaderModule**→**Points**→**Door**, and double-click the **Sensor** node in the Nav tree.

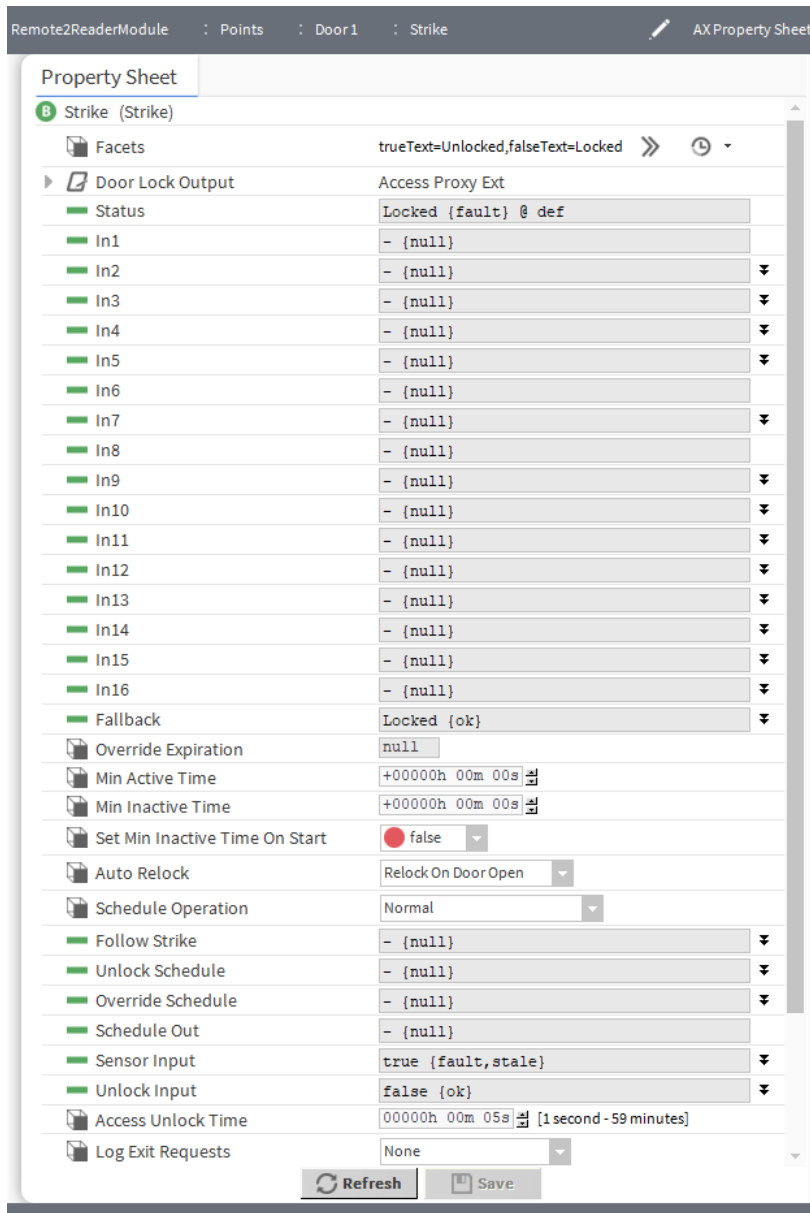
In addition to the standard properties (Facets), these unique properties support this component:

Property	Value	Description
Sensor Input	additional properties	This proxy-extension component is documented in a separate topic.
Status	read-only	Indicates the current state of the sensor (<i>Active</i> or <i>Inactive</i>), and its status {ok}, or other possibilities.
Door Held Open Limit	hours minutes seconds (defaults to 30 seconds)	Configures how long the door may be held open before an alarm condition manifests.
Unlock Schedule	null, true or false (default)	Indicates if an unlock schedule exists. A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Unlock Override	null, true or false (default)	Indicates if an override exists. A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Unlock Rex Override	null, true or false (default)	Indicates if an override exists. A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Debounce Time		
DoorForcedExt	additional properties	This alarm-source-extension component is documented in a separate topic.
DoorHeldOpenExt	additional properties	This alarm-source-extension component is documented in a separate topic.
IntrusionTimeoutExt	additional properties	This alarm-source-extension component is documented in a separate topic.
Supervisor Fault Settings	additional properties	This alarm-source-extension component is documented in a separate topic.
outOfServiceExt	BACnet extension	This out-of-service component is documented in a separate topic.

accessDriver-AccessStrike

This component configures the door strike.

Figure 520 Door strike properties



To access this component, expand the **AccessNetwork**→**Remote2ReaderModule**→**Points**→**Door**, and double-click the **Strike** node in the Nav tree.

In addition to the standard properties (Facets and Status), these unique properties support this component:

Properties	Value	Description
Door Lock Output	heading	Serves as a heading for the read-only values that follow.
In1–In16	true or false, defaults to false	Report the door lock inputs. Each writable point uses a 16-level priority scheme, with corresponding inputs In1—In16, plus a Fallback property. Level 1 is the highest priority, and level 16 is the lowest.

Properties	Value	Description
		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 In value.
Fallback	true or false, defaults to false	Pre-defines and output value in case of a null input.
Override Expiration	read-only	Reports when a waiting period is over and the driver issues an automatic action to the point.
Min Active Time	hours minutes seconds	Specifies that once opened, how long the door just remain open.
Min Inactive time	hours minutes seconds	Specifies that once closed, the door must remain closed for this amount of time.
Set Min Inactive Time On Start	true or false (default)	Ensures the minimum inactive time when the station starts.
Auto Relock	drop-down list	<p>Defines what should happen with a door that has just been unlocked.</p> <p>Unlock Time permits the door to remain unlocked for the amount of time defined by Access Unlock Time.</p> <p>Relock On Door Open locks the door as soon at it unlocks.</p> <p>Relock On Door Close locks the door either after the Access Unlock Time expires (if the door has been unlocked, but not opened) or when the door closes.</p>
Schedule Operation	drop-down list	<p>Specifies when to set the strike status. All options work with the selected unlock schedule. If no schedule is selected, (property set to none), none of the options are available for specifying how to set the strike status.</p> <p>Normal follows the schedule defined by the Unlock Schedule property.</p> <p>Unlock on first validation causes the strike to unlock (if access is granted) and remain unlocked after the first time access is granted within the scheduled open time. If access is granted outside of the scheduled open time, an unlock-on-first-validation is not performed.</p> <p>Unlock and Relock alternately unlocks and re-locks with each card swipe.</p> <p>Follow Another Strike opens a Ref Chooser used to select a module and door strike to follow. Door status reflects the status of the strike to follow. Choosing this option, when the schedule is true, inhibits the door force alarm without waiting for the door to follow to have its strike enabled.</p>
Follow Strike	null (default), true or false	A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Unlock Schedule	null (default), true or false	Selects a schedule to indicate when a door should be unlocked. None disables all strike properties. If no schedules appear in the Ref Chooser, none may have been created yet.

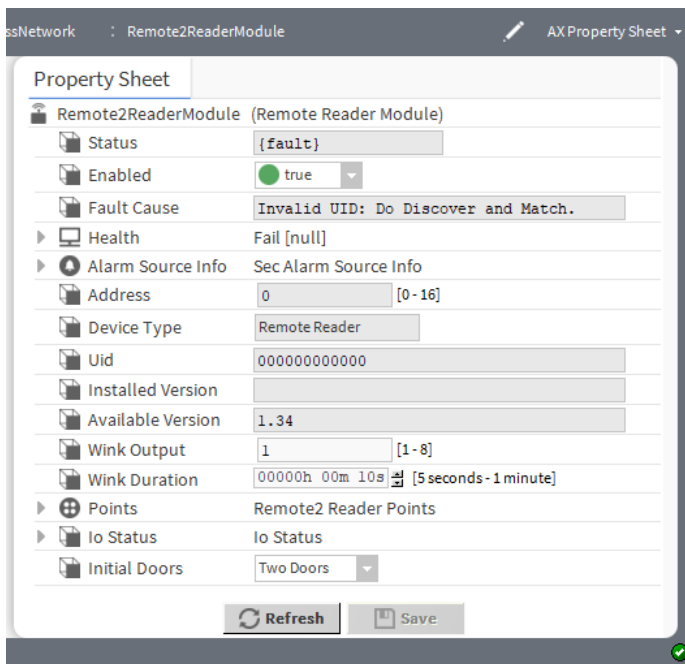
Properties	Value	Description
		A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Override Schedule	null (default), true or false	A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Schedule Out	null (default), true or false	A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Sensor Input	null, true (default) or false	A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Unlock Input	null, true or false (default)	A check-marked null value defaults to the incoming value from the device. If you remove the check mark you can configure this value.
Access Unlock Time	hours minutes seconds (defaults to 5 seconds)	Defines the length of time that a door may remain unlocked after access is granted. Values are only used when Auto Re-Lock is set to Unlock Time .
Log Exit Requests	drop-down list (defaults to None)	None Unloaked Opened Unlocked Or Opened
Log Schedule Activity	true (default) or false	Manages the log for a scheduled activity. true creates a record any time a schedule controls activity at this door. The record may be displayed in the Access History report. false disables the recording of scheduled activity.
Threat Level Group	read-only	Reports the threat level group.
Schedule Lock-down Threat Level	drop-down list (defaults to -1)	Specifies a threat level that keeps the door locked no matter what the state of the associated schedule is. The default sets the door to follow the associated schedule without regard to the active threat level. A value other than the default (Low , Normal or High) keeps the door locked as long as the active threat level is at or above that specified here. This value must be greater threat than the value specified in the Unlock Threat Level . If not, the system displays a warning message next to the property when you try to save.

Properties	Value	Description
Unlock Threat Level	drop-down list (defaults to -1)	Specifies a threat level that keeps the door unlocked, no matter what the state of the associated schedule is. The default follows the associated schedule without regard to the active threat level. A value other than the default (that is, <i>Low</i> , <i>Normal</i> or <i>High</i>) keeps the door unlocked as long as the active threat level is at or below the level specified here. The value of the Schedule Lockdown Threat Level must be a greater threat level than the value specified by this property, otherwise, a warning message displays when you try to save changes.
outOfServiceExt	BACnet extension	This out-of-service component is documented in a separate topic.

accessDriver-Remote2ReaderModule

This component configures a Remote 2 Reader module.

Figure 521 Remote2ReaderModule properties



You add this component to the **AccessNetwork** node in the station from the **accessDriver** palette. Once in the station, double-click this node to view its properties.

In addition to the standard properties (Status, Enabled, Fault Cause, Health and Alarm Source Info) these properties configure this component:

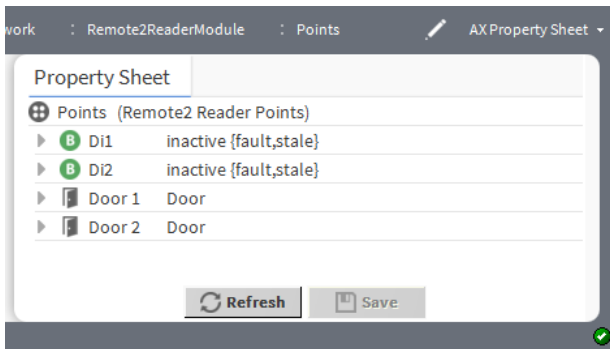
Property	Value	Description
Address	read-only	Reports the unique integer value automatically assigned to each physical I/O module during discovery.
Device Type	read-only	Identifies the type of remote device.

Property	Value	Description
Uid	read-only	Reports a six-byte number that is globally unique to this specific I/O hardware device. Discovery automatically obtains this Unique ID (Uid) from each device.
Installed Version	read-only	Reports the firmware version installed in the I/O module or device.
Available Version	read-only	Reports the firmware version available for the installed module. If this number is more recent (higher) than the installed version, you can initiate an I/O firmware upgrade from the Device Manager.
Wink Output	1–8 (defaults to 1)	(Writable) Specifies which digital output (relay output) is cycled On and Off when a Wink Device action is invoked on the module. Although the range is from 1 to 8, the I/O hardware may have fewer outputs.
Wink Duration	hours minutes seconds (defaults to 10 seconds) 5–60 seconds	(Writable) Specifies how long the wink output cycles on and off at a constant rate of 1 second on followed by 1 second off. NOTE: Wink is typically used only in the early stages of station configuration. After configuring, you may hide the Wink Device action to prevent inadvertent and unintended cycling of loads.
Points	points container	Documented elsewhere.
Io Status	additional properties	Contains a concatenated summary of current IO values in hexadecimal coded format, and numerous component children with individual hexadecimal values. These are the last values received by the actrlD process running on the controller. This information is usually used for advanced debugging only.
Initial Doors	drop-down list (defaults to Two Doors)	Defines the number of doors. No Doors One Door Two Doors

accessDriver-Remote2ReaderPoints

This component (default name Points) is the container for Remote 2 Reader devices. Each device controls two Boolean Digital Inputs (Di1 and Di2) as well as two doors (Door 1 and Door 2)

Figure 522 Remote 2 Reader Points properties



You add this component to the **AccessNetwork** node in the station from the **accessDriver** palette. Once in the station, double-click this node to view the points it contains. To view the Property Sheet, right-click the **Remote2Reader** node in the Nav tree and click **Views→AX Property Sheet**.

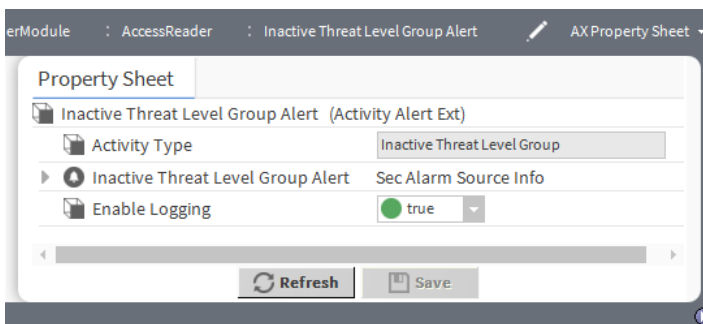
Each digital input and door is a component in its own right with associated properties and additional devices.

The default and primary view for this component is the **R2 R Point Manager**.

accessDriver-ActivityAlertExt

This component servers multiple uses to track access activity.

Figure 523 Example of an activity alert extension



Property	Value	Description
Activity Type	read-only	Identifies the type of activity.
Inactive Threat Level Group Alert (example)	additional properties	This is a standard alarm-AlarmSourceInfo component.
Enable logging	true (default) or false	Turns activity logging on and off.

Chapter 21 Workbench plugins

Topics covered in this chapter

- ◆ Access Device Manager
- ◆ R2 R Point Manager

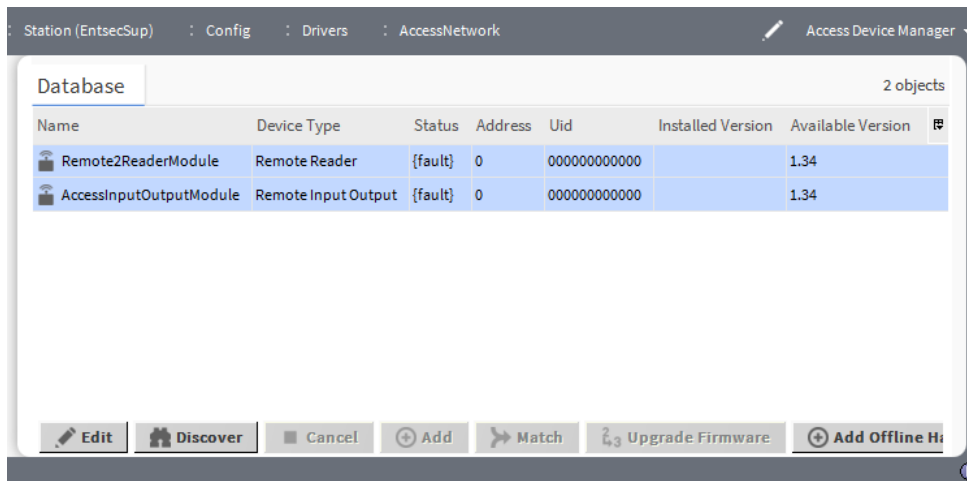
There are many ways to view plugins (views). One way is directly in the tree. In addition, you can right-click on an item and select one of its views. Plugins provide views of components.

In Workbench, access the following summary descriptions on any plugin by selecting **Help**→ **On View** (F1) from the menu, or pressing F1 while the view is open.

Access Device Manager

This view shows the access devices connected to the AccessNetwork.

Figure 524 Access Device Manager



To open this view, navigate to **Config**→**Drivers** and double-click the **AccessNetwork** node in the Nav tree.

Table 92 Columns

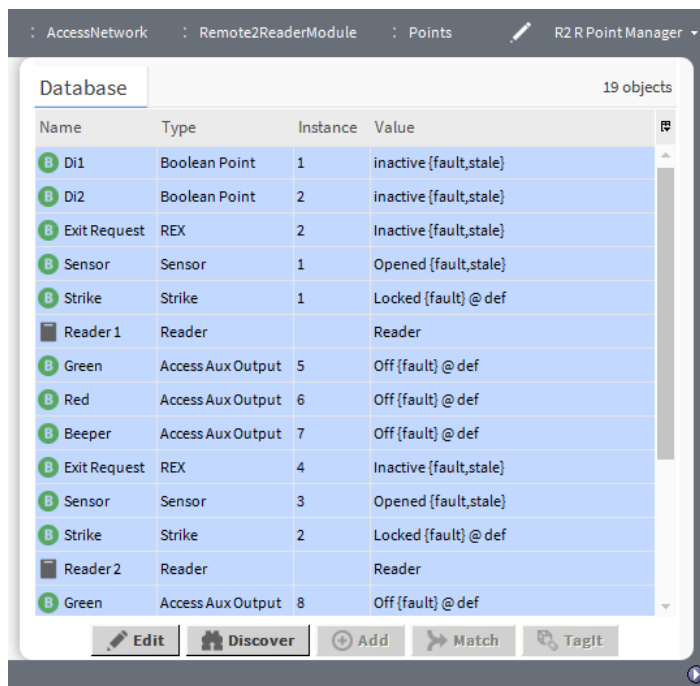
Column	Description
Name	Provides descriptive text that reflects the identity of the entity or logical grouping.
Device Type	Identifies the type of remote device.
Status	Indicates the condition of the network, device or component at the last check. {ok} indicates that the component is licensed and polling successfully. {down} indicates that the last check was unsuccessful, perhaps because of an incorrect property, or possibly loss of network connection. {disabled} indicates that the Enable property is set to false . {fault} indicates another problem. Refer to Fault Cause for more information.
Enabled	Activates (true) and deactivates (false) use of the network, device, point and component.
Health	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.

Column	Description
Address	Reports the unique integer value automatically assigned to each physical I/O module during discovery.
Uid	Reports a six-byte number that is globally unique to this specific I/O hardware device. Discovery automatically obtains this Unique ID (Uid) from each device.
Installed Version	Reports the firmware version installed in the I/O module or device.
Available Version	Reports the firmware version available for the installed module. If this number is more recent (higher) than the installed version, you can initiate an I/O firmware upgrade from the Device Manager.
Initial Doors	Defines the number of doors. No Doors One Door Two Doors

R2 R Point Manager

This view lists the R2 R points in the database and provides point discovery.

Figure 525 R2 R Point Manager



To access this view, expand the **Config→Drivers→AccessNetwork→Remote2ReaderModule** node in the Nav tree and double-click the **Points** node.

Table 93 Columns

Column	Description
Name	Provides descriptive text that reflects the identity of the entity or logical grouping.
Type	Indicates the type of component.
Instance	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.

Column	Description
	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.
Is Sdi	... Supervised Digital Input (Sdi)
Conversion	Specifies the units used between the read value (as defined in Device Facets) and the parent point's output (in selected point facets).
Value	Reports the current point datum (data item).
Facets	Indicates the text used to describe true and false device states.

Buttons

-

Chapter 22 Windows

Topics covered in this chapter

- ◆ Edit remote reader module window

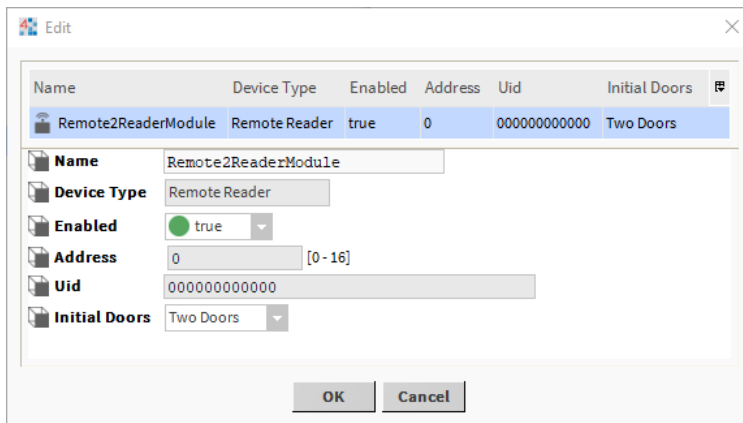
Windows create and edit database records or collect information when accessing a component. You access them by dragging a component from a palette to a nav tree node or by clicking a button.

Windows do not support **On View (F1)** and **Guide on Target** help. To learn about the information each contains, search the help system for key words.

Edit remote reader module window

This window configures a remote reader module record in the database.

Figure 526 Edit remote module window



To open this window, expand **Config**→**Drivers**, double-click **AccessNetwork**, select a module and click the **Edit** button.

Property	Value	Description
Name	text	Provides descriptive text that reflects the identity of the entity or logical grouping.
Device Type	read-only	Identifies the type of remote device.
Enabled	true (default) or false	Activates (<i>true</i>) and deactivates (<i>false</i>) use of the network, device, point and component.
Address	read-only	Reports the unique integer value automatically assigned to each physical I/O module during discovery.

Property	Value	Description
Uid	read-only	Reports a six-byte number that is globally unique to this specific I/O hardware device. Discovery automatically obtains this Unique ID (Uid) from each device.
Initial Doors	drop-down list (defaults to Two Doors)	Defines the number of doors. No Doors One Door Two Doors

Index

A

access control service	300
access control setup view.....	300
access device manager	164
add device window, discovered device.....	167–168
manage devices windows	165
Access Device Manager	529
access history filter window.....	91
access history report and summary window	88
Access Network	161
access network view and tab.....	198
access right reader report and filter.....	114
access rights	
filter.....	53
quick edit window	69
summary tab	68
view.....	67
access rights filter window	70
access rights tab.....	51, 400
access rights tab	
tenants view	83
schedules.....	130
tenants view.....	83
access setup	287
access zone view	
activity alerts ext tab	291
supervisors tab.....	293
access zones	
add new access zone view	288
Access Zones.....	499
access zones views	287
accessDriver-AccessAlarmSourceExt	509
accessDriver-AccessDoor	509
accessDriver-AccessElevator	510
accessDriver-AccessFloor.....	510
accessDriver-AccessInputOutputModule	511
accessDriver-AccessNetwork	512
accessDriver-AccessProxyExt.....	515
accessDriver-AccessReader.....	517
accessDriver-AccessRex	520
accessDriver-AccessSdi.....	521
accessDriver-AccessStrike	522
accessDriver-ActivityAlertExt	528
accessDriver-Remote2ReaderModule	526
accessDriver-Remote2ReaderPoints	527
activate threat level window.....	396
activation alerts	403
activation badges tab	400
active schedule tab	279, 458
activity alert exts tab	183
intrusion displays.....	322
activity alerts ext tab	
access zone.....	291
activity monitor filter window.....	39
activity monitor tab.....	38

ADA tab.....	178
add (or edit) a new tenant view.....	79
add (or edit) info template view.....	85
add (or edit) report window.....	92
add a new schedule window	
schedules.....	118
add a new tenant	
badges tab.....	81
add attribute window	421
add device window, discovered Azure ID	
Client Device	168
add device window, discovered device	167
add driver windows	162
add new (edit or duplicate) schedule view.....	120
add new (or edit) calendar schedule view.....	135
add new access rights.....	71
add new access zone view	
entry readers tab.....	293
exit readers tab.....	294
grouping tab.....	295
occupants tab	292
summary tab	290
add new alarm class	
relay links tab.....	329
add new alarm class view	326
add new alarm count to relay	
relays tab	334
add new alarm count to relay view.....	332
alarm classes tab	333
add new badge	
summary tab	62
add new badge view.....	60
add new email recipient	
alarm classes tab	342
add new email recipient view	340
add new image view	393
add new intrusion display	
activity alert exts	322
intrusion zones tab	322
add new intrusion display view	319
add new intrusion pin view.....	306
add new intrusion zone	
recipients tab.....	315
relay links tab.....	316
add new keypad format view	354
add new Nav group view	394
add new Niagara integration ID.....	200
add new PDF styles view.....	355
add new person view.....	48
add new role view.....	148
add new schedule view	
summary tab	120
add new station recipient	
alarm classes tab	348
add new station recipient view	347

add new threat level group	
access rights tab	400
remote stations tab	401
add new threat level group view.....	397
activation badges tab	400
summary tab	399
add new user view	143
roles tab	147
add new Wiegand format view	297
add station windows.....	208
add threat level window.....	404
additional personnel data.....	84
additional personnel data filter window	85
additional personnel data to import.....	301
additional personnel entry	
export personnel records window	303
additional personnel entry view.....	301
additional points tab.....	171
alarm	
details.....	29
alarm classes tab	38, 333, 342, 346, 348
console recipient	343
alarm classes views	325
alarm console	
columns	27
control buttons	26
info icons	28
links.....	28
alarm consoles view	342
alarm extensions views	350
video setup window	281
alarm history filter window	96
alarm history report	94
alarm history summary window	95
alarm instructions	
edit instructions window	331
master instructions window	331
alarm instructions view.....	330
alarm relay tab.....	177, 186
alarm relays view	332
add new alarm count to relay view	332
alarm setup	325
recipients tab	328
alarm setup tab	278
alarm source info tab	350
allowed hosts	215
anti-passback controls	287
Asure ID client device view.....	470
Asure ID device view.....	472
attendance history filter window	99
attendance history report and summary	
window	97
attributes (LDAP) tab	418
audit history report.....	101
Axis	
cameras	248
video network.....	219
Axis camera	
events view	258
Axis cameras view.....	249
Axis network view.....	221
Axis video camera.....	253
Axis Video Camera	
preferences.....	257
Axis Video Network.....	161
B	
backup	
restore window	156
backup archive tab	
restore window	156
backup views.....	153
backups	153
backup archive summary window	155
backup schedule tab.....	156
recent backup history tab	157
recent backup history tab filter window	158
backups view	
local backup window	155
system backup window.....	155
BACnet BDT	
new (or edit) entry views.....	206
BACnet BDT manager.....	205
BACnet network view	202
IP port tab	203
BACnet Network view	
Door Control tab.....	205
Mstp port tab.....	204
BACnet points and filter window	109
badge tab	62
badges	
summary window	55
badges filter window	58
badges tab.....	54, 81
badges view	56
quick edit window	57
base reader	
alarm setup tab	189
base reader modules	169
base reader view	
doors tab	170
batch enroll badges	
summary tab	64
batch enroll badges view	63
bindings	379
bound label.....	380
increment set point bindings.....	384
set point bindings.....	383
spectrum bindings.....	382
spectrum set point	384
value bindings.....	381
bound label bindings	380
burglar panel view	193
burglar panels tab.....	171

C

calendar schedules Filter window	134
calendar schedules view	133
camera	
event extension	194
Milestone New window	262
camera events	274
camera grid	248
cameras	
Axis	248
Maxpro	270
cameras tab	
maxpro	269
card formats	
add new Wiegand format	297
card formats view	296
card reader	
for entering a zone	293
certificate	
create	218
certificate management	
private key password window	219
certificate management view	
trust stores	215
change assignment properties	52
change password view	151
cleanup LDAP deleted entries	424
component	
SecurityActivityMonitor	475, 486
SecurityAlarmConsoleOptions	476
components	
accessDriver	509
entsec	475
configuration tab	202
configure database view	365
console layout window	34
console recipient	
alarm classes tab	343
consolidated intrusion displays report	110
controller (system) setup	
backup views	153
controller setup	20
miscellaneous	353
user management	139

D

data to import (personnel)	301
database configuration tab (HsqlDbDatabase) ...	367
database configuration tabs	
MySQL database	367
SqlServer database	367
Database Services	365
device	
configuration	164
device ext tab	215
device modules	168

digital points tab	429
discover and preferences windows	284
display camera grid	248
display image view	393
displays tab	234
distributed schedule manager–database view ...	212
document change log	15
Door Control tab (BACnet Network view)	205
door view	172
ADA tab	178
alarm relay tab	177
exit request tab	176
manual override window	172
override input	177
relay out tab	179
sensor tab	175
strike tab	173
doors report and filter window	104
doors tab	170
download window (Nrio)	464
DVR cameras tab	259
DVR views	228

E

edit Activity Monitor view	38
edit alarm extension properties	350
edit digital point views	442
edit instructions window	331, 405
edit intrusion displays tab	312
edit intrusion pins	
escalation level tabs	315
grouping tab	314
points tab	313
readers tab	312
edit intrusion pins tab	317
edit intrusion zone	
manual override window	310
edit metadata window	405
edit person view	48
edit points view	274
active schedule tab	279
alarm relay tab	186
alarm setup tab	278
manual override window	199
edit remote module	533
elevator view	
floors tab	190
readers tab	193
elevators report and filter window	107
elevators tab	170
email recipients view	339
email service	
incoming account tab	338
outgoing account tab	335
email service view	335
end user licenses agreement view	372
EndUserLicenseAgreement	494

- enroll new badge view 59
 - summary tab 59
 - EnterpriseSecurityService 477
 - entry readers tab 293
 - entsec-AccessControlService 495–497
 - entsec-AccessRightReaderReport 506
 - entsec-AccessRights 498
 - entsec-AlarmClasses 479
 - entsec-AlarmClassRelayLinks 482
 - entsec-AlarmConsoles 479
 - entsec-AlarmExtInstructions 481
 - entsec-AlarmHistory 480
 - entsec-AlarmSourceExts 481
 - entsec-AttendanceHistoryConsolidator 502
 - entsec-BacnetPoints 482
 - entsec-Badges 497
 - entsec-CalendarSchedules 489
 - entsec-ChangePasskey 492
 - entsec-ChangePassword 492
 - entsec-ConsolidatedColumnsProvider 500
 - entsec-Doors 499
 - entsec-EmailRecipients 480
 - entsec-EntsecNav 498
 - entsec-EntsecNavGroupQuery 491
 - entsec-EntsecRoleQuery 493
 - entsec-InfoTemplates 504
 - entsec-KeypadFormats 503
 - entsec-LocalHistoryQuery 501
 - entsec-MonitorSysDefSecurity 478
 - entsec-NiagaraIntegrationIDs 504
 - entsec-NiagaraStationQuery 483
 - entsec-PersonAccessRightReport 505
 - entsec-Personnel 496
 - entsec-PersonnelChanges 506
 - entsec-PersonReaderReport 505
 - entsec-PlatformSetup 494
 - entsec-PxGraphics 491
 - entsec-ScheduleRecs 489
 - entsec-SecurityActivityMonitor 475, 486
 - entsec-SecurityAlarmConsoleOptions 476
 - entsec-SecurityAuditHistory 484
 - entsec-SecurityHistoryConsolidator 487, 500
 - entsec-StationRecipients 480, 507
 - entsec-SystemBackups 493
 - entsec-Tenants 490
 - entsec-ThirdPartyLicenses 495
 - entsec-ThreatLevelGroupRecs 490
 - entsec-ThreatLevelSetup 491
 - entsec-UserQuery 492
 - entsec-VideoSubsystem 494
 - entsec-WiegandFormats 503
 - escalation level tabs 315
 - event view
 - link to tab 282
 - events (camera) 274
 - events tab 273
 - calendar schedules 135
 - events tab **Milestone camera** 264
 - exit readers tab 294
 - export personnel records window 303
- ## F
- fade rate window 197
 - floors tab 190
- ## G
- Generate Self-Signed Certificate window 218
 - get corrupt Pin numbers window 365
 - go to module window 429
 - graphic editor canvas 387
 - graphic editor objects 388
 - graphic editor toolbar 389
 - graphics configuration 22
 - graphics side bar pane 389
 - graphics view
 - add graphics window 378
 - edit nav window 379
 - graphic editor view 386
 - modify settings window 378
 - view graphic 386
 - graphics view (graphics management) 377
 - grouping tab 295, 314
 - groups tab 421
- ## H
- hardware
 - module configuration 164
 - hardware reports 104
 - history (Nrio) extension view 460
 - HsqlDbDatabase 365, 367
- ## I
- images view 392
 - import preferences window 412
 - incoming account tab 338
 - increment set point bindings 384
 - info template view 85
 - input/output module
 - alarm relay 88
 - input/output module tab 210
 - input/output modules 169
 - inputs 277
 - inputs report and filter window 106
 - intrusion display tab 321
 - intrusion displays
 - add new intrusion display view 319
 - intrusion displays report and filter window 110
 - intrusion displays tab 312
 - intrusion displays views 318
 - intrusion history filter window 100
 - intrusion history report 99

intrusion pin			
summary tab	306		
Intrusion Pin tab	306		
intrusion pins			
intrusion zone tab.....	307		
intrusion pins tab	317		
add new schedule	131		
intrusion Pins tab			
tenants view.....	80		
intrusion pins views.....	305		
intrusion setup	305		
intrusion zone			
add or edit.....	308		
summary tab	311		
intrusion zones tab	307, 322		
intrusion zones views	308		
IP Port tab (BACnet Network view).....	203		
J			
job service view	371		
join station view.....	210		
K			
key store	215		
keypad formats views	353		
L			
LDAP audit history report	111		
LDAP audit history view	423		
LDAP network driver	407		
new LDAP server window	410		
LDAP network view	407		
LDAP Servers tab	409		
Ldap server view			
add attribute window	421		
groups tab	421		
Ldap Server view			
attributes tab	418		
LDAP server view.....	413		
LDAP servers tab.....	409		
import preferences window	412		
license manager view.....	356		
link from tab (Nrio).....	460		
link to tab.....	459		
log history filter window.....	104		
log history report.....	103		
M			
maintenance view (server).....	361		
manage devices windows.....	165		
manage drivers window	162		
manage Nrio points window.....	428		
manage reports window	92		
manual add (attendance record) window	98		
manual hide (confirmation) window	98		
manual override window	172, 199, 310		
master instructions window.....	331		
maxpro			
camera.....	270		
cameras tab	269		
Maxpro	219, 248		
cameras	248		
video network	219		
Maxpro network tab	226		
Maxpro Nvrs tab	241		
media types.....	22		
meta data.....	280		
Milestone	219, 248		
camera.....	260		
camera, events tab	264		
cameras	248		
DVR properties	233		
Dvr tab	229		
DVRs tab.....	228		
video network	219		
X Protect DVRs tab.....	234		
Milestone DVR			
cameras tab	259		
Milestone Network	161		
properties	224		
Milestone X Protect			
properties.....	225		
miscellaneous graphics	377		
miscellaneous reports	112		
modules			
remote.....	163		
modules report and filter window.....	108		
monitoring views	25		
MS SQL database	365, 367		
Mstp port tab (BACnet Network view).....	204		
multi source view options window	32		
MySQL database	365		
N			
navigation groups			
add new Nav group view	394		
navigation groups view	393		
network view	161		
new access right			
floors tab	75		
reader's tab filter window	75		
readers tab summary window	74		
new access right floors tab			
filter window	76		
new access rights			
people tab	72		
readers tab	73		
new LDAP server window.....	410		
new person			

summary tab	50
New window	
Axis camera	250
Maxpro Nvr	245
Niagara integration ID	200
Niagara Integration ID	
Quick Edit window	202
Niagara integration ID view	
access rights tab	201
summary tab	201
Niagara Integration IDs tab	79
Niagara integration IDs view	199
Nrio device manager	
download window	464
upload window	463
Nrio device manager view	425
Nrio driver	425
Nrio module view	426
go to module window	429
Nrio point manager	428
Nrio network filter window	464
Nrio point edit view	430
Nrio point manager	428
active schedule tab	458
digital points tab	429
high speed counter tab	446
history extension view	460
history setup tab	457
link from tab	460
link to tab	459
manage extensions windows	457
manage Nrio points window	428
relay output tab	449
resistive input tab	438
temperature input tab	435
voltage input tab	430
Nrio Point Manager, Voltage Output tab	453
NTP properties	
controller	372
Supervisor PC	374
NVR tab	241
NVR views	228

O

obix links	465
Obix Network	161
Settings window	468
Obix network driver	465
occupants tab	292
outgoing account tab	335
output configuration tab	183
outputs	278
outputs report and filter window	107
override input	177

P

PDF styles views	355
people tab	
tenants view	80
people view	45
filter window	47
quick edit window	47
people view access rights	
summary window	52
person access right report	112
person reader report	113
personnel	
building re-entry control	287
personnel changes filter window	116
personnel changes report and summary	
window	115
personnel data to import	301
personnel views	45
photo ID	
badges tab	472
edit template data	473
tenants tab	472
Photo ID configure window	469
Photo ID device add window	468
photo ID management	467
Photo ID network view	467
photo ID template manager	471
photo ID viewer view	474
photo ID viewers view	473
playback viewer	41
plugins	529
points	
editing	274
points tab	313
power alarm setup view	349
power monitor view	195
preferences	
Maxpro camera	246
preferences window	257
private key password window	219
properties	24
purge config window (expanded)	90
purge config window (simple)	90

Q

query-Predicate	493
query-SingleExtent	492, 500
quick edit window	
schedules	118

R

R2 R Point Manager	530
range create badges	
summary tab	66
range create badges view	65

reader	
for entering a zone	293
reader modules	169
reader tab	181
reader view	180
activity alert exts tab	183
output configuration tab.....	183
reader configuration options.....	179
reader tab.....	181
readers report and filter window	105
readers tab.....	172, 193, 312
recent backup history tab.....	157
recipients tab	315, 328
recover station view.....	214
related documentation	16
relay links tab	316, 329
relay out tab.....	179
relay output tab.....	449
relays tab	334
remote drivers	
add driver windows	162
filter window.....	163
manage drivers window.....	162
remote drivers view	161
enable/disable networks window	163
remote module network ID	
fade rate window	197
output test window	197
wink device window	197
remote module network ID view.....	195
remote modules	163
access device manager	164
remote reader modules.....	169
remote stations tab	401
report	
LDAP audit history	111
reports	
hardware	104
hardware inputs	106
hardware outputs.....	107
reports views.....	87
resistive input tab	438
restore backup window.....	156
restore from backup distribution file.....	158
retrieve active status.....	397
review video view	96
role view	
users tab.....	150
roles tab.....	147
roles view.....	147
filter window	148
S	
schedule emailed report window.....	93
schedule setup (calendar schedules) tab	136
schedule setup (weekly schedules) tab.....	123
scheduler tab	
add new schedule window.....	121
schedules	117
schedules filter window	
schedules.....	119
sensor tab	175
set COM port window	463
set point bindings.....	383
settings window	468
settings windows.....	209
show alarm details window.....	29
SmartKey	
add device tab	284
discover and preferences windows.....	284
SmartKey device manager - Database view	283
SmartKey Network	161
special events tab	
add new schedule	124
spectrum bindings.....	382
spectrum set point bindings.....	384
standard properties.....	24
station device properties view.....	214
station manager	
add station windows.....	208
distributed schedule manager–database	
view	212
join station view	210
recover station view	214
settings windows.....	209
station device properties view	214
station manager–database view	206
station recipients views.....	347
strike tab.....	173
summary tab	59, 64, 66, 120
summary window.....	155
additional personnel data	84
summary window	84
supervisors tab.....	293
surveillance viewer.....	40
system date time editor view	372
system setup	20
system trust store.....	215
T	
temperature input tab.....	435
tenants view	77
filter window	78
Intrusion Pins tab.....	80
summary window and tab	78
third party licenses view.....	372
threat level	
groups.....	395
threat level	
windows	395
views	395
threat level group filter	396
threat level groups tab	
tenants view.....	82

threat level setup view	402
activation alerts	403
add threat level window	404
edit instructions window	405
edit metadata window	405
threat levels	395
trust stores	215

U

update reader count window	364
user interface	21
user management	139
user trust store	215
users tab	150
users view	139
configure window	140
filter window	143
quick edit window	142

V

value bindings	381
video	
reviewing	96
video alarm classes (recipient) view	345
video alarm recipient	
alarm classes tab	346
video camera views	248
video monitoring	40
video network	
Axis	219
video setup window	169, 281
virtual display tab	321
voltage	
input facets	431
input, linear calibration ext properties	434
proxy ext properties	431
voltage input tab	430
voltage input view	442
voltage output tab (Nrio)	453
voltage, edit input voltage	430

W

web service view	369
Wiegand card format	297
Wiegand card formats	296
Wiegand format summary tab	299
window	
Maxpro New and Edit	246
windows	533

X

X Protect

Cameras tab	265
Recording Servers view	239
X Protect Camera tab	266
X Protect Management Server	235
X Protect Recording Server tab	240