Technical Document

Niagara Enterprise Security Installation and Maintenance Guide

March 21, 2025

niagara4

Legal Notice

Tridium, Incorporated

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

Confidentiality

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

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

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

Trademark notice

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

Copyright and patent notice

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

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

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

Contents

About this guide

This guide is for the systems integrator who is responsible for installing and configuring system software.

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.

The topics and procedures describe how to install and configure the software. Some procedures require Workbench. Others require the web UI. Most apply equally to single (stand-alone) controller systems and company-wide systems where controllers are joined and subordinate to a Supervisor station. Procedures that apply to only stand-alone or company-wide systems are noted in the text.

Document change log

This topic summarizes the changes made to this document.

March 21, 2025

- Updated the guide to include the "NAC Controller" related topics.
- Added new "Note" in the "Creating and updating the HSQL database password" topic.

June 1, 2023

Edited "Creating and updating the HSQL database password" topic in the "Controller Commissioning" chapter.

November 3, 2022

Made changes to “Access Rights” topic for clarification.

August 3, 2022

Updated “Personnel data from the LDAP server” chapter.

June 9, 2022

Edited Access Right topic in the “Controller setup, users and schedules map” chapter for access right for tenant.

July 31, 2021

Added “Configuring Asure ID secure communication” to the “Personnel setup chapter” and updated “Photo ID configuration troubleshooting” in the “Maintenance” chapter.

January 20, 2021

Added a section titled “Mobile intrusion keypad setup” to the “Intrusion zone management” chapter.

Added the topic “Adjusting controller memory” to the “Troubleshooting” section of the “Maintenance” chapter.

June 29, 2020

Added information about network ports when using fox streaming to deliver video content.

June 5, 2020

Added information specifying that the mySql Connector/J must be renamed when installed.

April 23, 2020

- Added information about securing browser communication with a camera using certificates.
- Added a section in troubleshooting for failure to connect to a remote camera.
- Significantly edited the “Video Installation” chapter, adding the Maxpro driver, removing Web Start, and adding HTML5 streaming.

- Updated the Axis and Milestone sections in the “Video Installation” chapter.
- Added Certificate Wizard information.
- Updated the New Camera window and Axis Video Camera tab in the Axis section of the “Video Installation” chapter.
- Significantly upgraded the Photo ID section in the “Personnel setup” chapter, including setting up users when oBIX is used as a server.
- Added best practice information to “System Security” chapter regarding the security benefits of changing certificates frequently.
- Added a topic titled “Configuring the WebService for Easy Lobby.”
- Added a step to “Preparing a MySQL database” for renaming the Connector/J and added a troubleshooting Q and A related to the Connector/J name.

August 8, 2019

- Reorganized document and added updates related to Niagara 4.8 release.
- 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.

October 9, 2018

Minor editorial updates.

September 17, 2018

Initial release for version 2.4

Related documentation

Several documents provide additional information about this software.

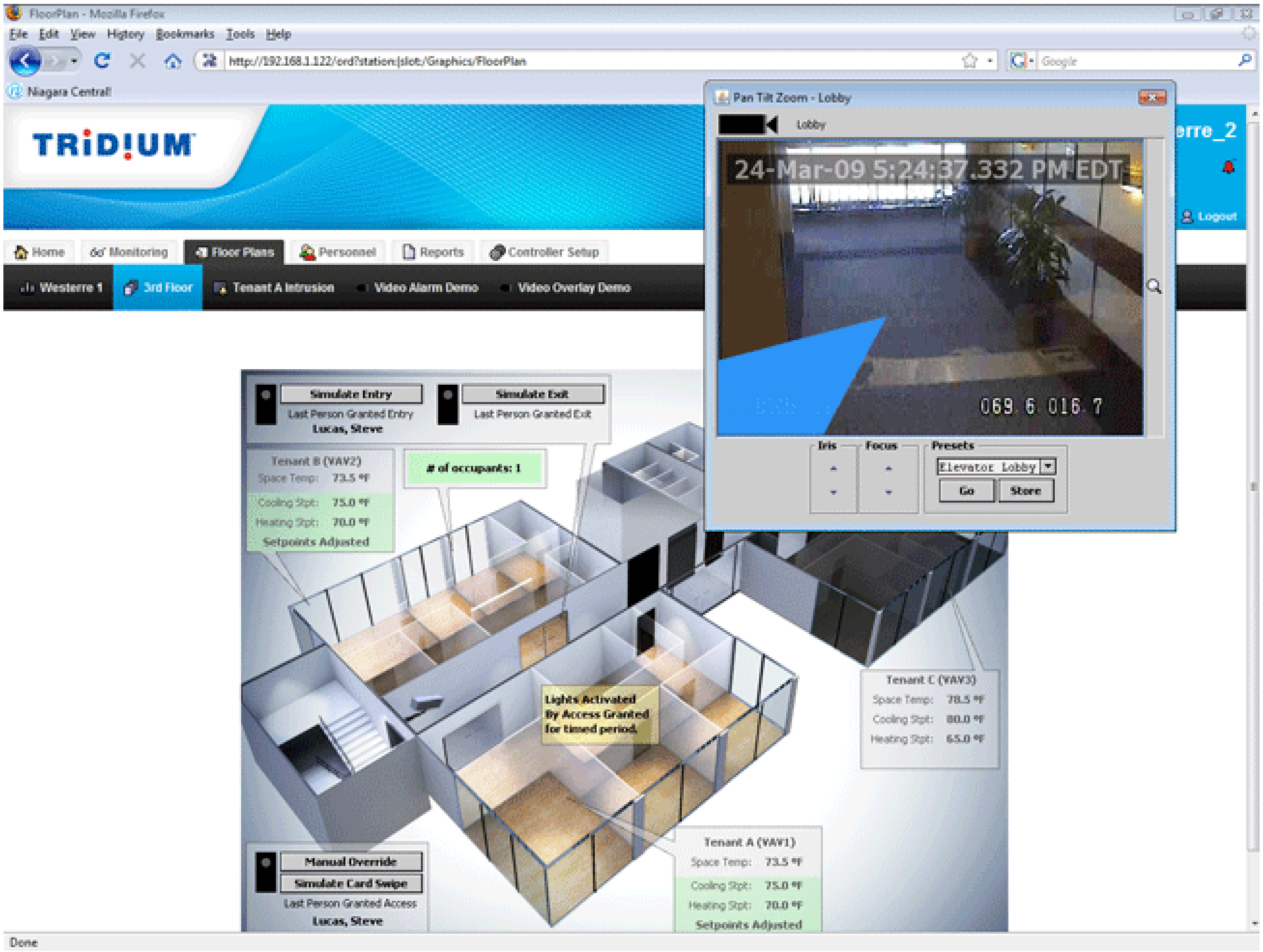
- *Niagara Enterprise Security Facility Manager's Guide*
- *Niagara Enterprise Security Reference*
- *Niagara Enterprise Security Operator's Guide*
- *Niagara Station Security Guide*
- *Niagara FIPS 140-2 Configuration Guide*
- *JACE-8000 Install and Startup Guide*
- *Niagara Graphics Guide*
- *Niagara Video Framework Guide*

Chapter 1. About this system

The Enterprise Security system provides the hardware and software to integrate a building's access control devices. Depending on the system, the devices may include controllers connected to badge readers, displays and keypads, motion detectors, video cameras, other sensors, fire alarms, and more.

Features

Figure 1. Integrating video and graphics support



As the industry's leading facility management software platform, this system, built on the Niagara Framework®, provides exceptional interoperability within traditional secure environments. It extends easily and integrates with many diverse facility systems, including environmental controls, lighting, energy management, fire and video, to create a unified, intelligent building.

The system is scalable from single-door solutions to multi-building and multi-campus deployments. It provides control and alarm supervisory and management functions through a browser-based interface that allows authorized users (based on password and privilege level) to carry out system configuration and management functions.

Stand-alone controllers may be added to the system, as needed over time, while monitoring and administration follows a hierarchical model built around Supervisor, peer, and subordinate relationships.

Feature	Description
Networking	• Features open solution-connectivity via oBIX, BACnet, SNMP, Modbus, and other non-proprietary protocols • Provides a distributed architecture with high availability at remote locations.
Interfaces	• Provides a web-based interface that is easily managed via a standard browser providing a common GUI experience regardless of manufacturer or protocol. This interface includes all the relevant building access features. • Includes a general-purpose building automation tool,Workbench, which offers additional features, such as sophisticated graphics, and general-purpose building automation tools.
Data collection and reporting	• Collects historical data and events with powerful ad-hoc reporting for on-screen viewing or exporting to PDF or CSV format. • Provides real-time data on graphical floor plans, historical data, events in tables and customized reports.
Scheduling	Provides calendar functions and scheduling tools.
Access and intrusion zones	Enables company-wide configurations with access and intrusion zones that span multiple controllers.
Threat-level management	
Diagnostics	Includes remote diagnostics and provisioning tools for servicing the system.
Documentation	Includes context-sensitive online documentation.

Stand-alone installation

A single controller managing multiple doors and other hardware provides a cost-effective solution for small companies, schools and other institutions. It differs from a company-wide installation in that it does not require a Supervisor computer.

To install a stand-alone controller (platform), commission it, and to create a station, the installer uses Workbench running on a PC, which is temporarily connected to the same network as the controller.

Access to the station for the purpose of monitoring alarms and performing routine maintenance requires any device (computer, laptop, tablet, or smartphone) connected to the network that is capable of running a browser. The first time you access each platform and station, a Guided Setup Wizard prompts you through the post-software-installation and configuration process.

These features are not available for stand-alone controllers:

- Integrated Photo ID for badges
- LDAP integration for authenticating employees
- The use of a Milestone XProtect Corporate driver to provide video surveillance

Other feature limitations that require Workbench for both the Supervisor and controller include:

- Integrated programming that requires a wire sheet
- The setting up of non-Boolean schedules
- The customizing of door sequence operations that require a wire sheet

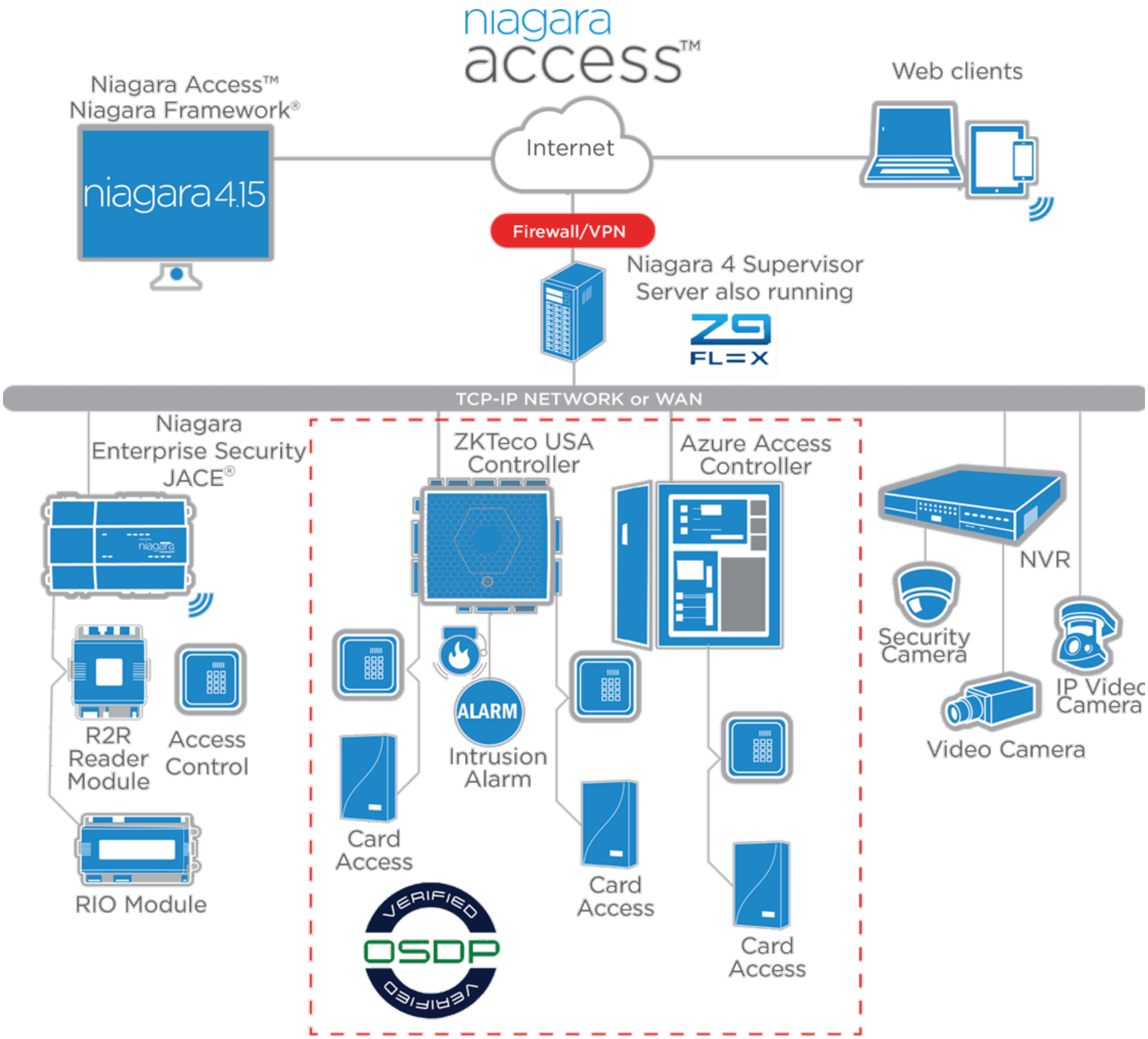
Many factors impact the network, including the number of devices, the frequency of processing transactions, and the size and frequency of generated reports. When a large installation operates on a stand-alone platform without a Supervisor PC, performance may be impacted. Although metrics are available, it is very difficult to establish a rule of thumb to work in every situation. The more you add to the installation, the higher the risk of impacting key functions, such as access validation, alarming, and card management.

Company-wide installations

A network of, potentially, hundreds of controllers meets the needs of large companies and government agencies. This type of installation includes at least one Supervisor PC.

PCs, tablets and mobile phones—any client device that can run a browser can manage a system network.

Figure 2. Company-wide network architecture



Reader modules and eight input/output modules connected to a single controller can provide a total of 32 card readers and an additional 64 input and 64 output monitoring points. These key components are connected to the controller across an RS-485 network. The controller exposes the system to web browsers, other controllers, and one or more Supervisors when configured as part of a network.

Software installation involves installing Workbench on the Supervisor PC followed by using Workbench to commission each remote controller and create each remote station.

Once the software is installed, the system, running in a browser, provides access to the Supervisor platform and station, and to each controller platform and station. The first time you access each platform and station, a Guided Setup Wizard prompts you through the post-software-installation and configuration process.

Platform (host), station, client, server

A system network includes a station running on the Supervisor PC, and at least one station running on a controller with reader modules and input/output modules attached.
Connections among system entities are frequently referred to using the standard network terms of *client* and *server*. A clear understanding of these terms is important for solving networking issues and ensuring communication security.

- Workbench is always a client.
- A *platform* provides the hardware foundation for the software interface. A platform runs basic software. It may be a PC localhost or a remote controller, such as a JACE.

  A platform (controller or Supervisor PC) is always a server. A host is another name for a platform.
- A *station* consists of the system software and an HSQL database. A station runs the software providing access for client browsers to view and control system components.

  A station may be a client or a server. A station, running on any type of controller or Supervisor platform performs all control logic and stores information including: card holder data, configuration data, system activity logs, and system relational hierarchy data

Software

The system's software includes operating systems, browsers, relational databases and video drivers. Some software modules run on the controller and others on the Supervisor PC.

System/driver	Supported	Comments
Operating system for the Supervisor station	Windows 10 x64 Windows 2016 x64 Windows 2019 x64	From the release of Niagara 4.9, the following operating systems are no longer supported: Windows 7 x86 Windows 7 x64 Windows 8.1 x86 Windows 10 x86 Windows Server 2012 x64 Controller stations run under the QNX operating system, which is provided.
Browser for the Supervisor station	Internet Explorer 6.1 and later Mozilla Firefox 5.0 and later Niagara Web Launcher Google Chrome 79	For configuration only, use Workbench and Niagara Web Launcher. The Web Launcher application supports any browser view that requires the WebApplet. Google Chrome 75 supports only the monitoring and loading of HTML views.

System/driver	Supported	Comments
JRE Plug-in for browsers (applicable to the WebApplet environment)	Oracle Java Version 8, update 241	High-level sanity test done with the latest JRE8 update 212 dated 18 April 2019. Web Launcher supports both 32–bit and 64–bit JRE.
Relational database in a Supervisor station	MySQL MS SQL Server 2016 MS SQL Server 2017	From the release of Niagara 4.9, the following database versions are no longer supported: MS SQL Server 2012 Oracle 11g MySQL 8.0 is supported but was not tested. Controller stations use an HSQL database, which is provided.
Video drivers	nAxis: Axis Video Driver nMilestone: Milestone Video driver (Professional and Professional plus editions) Milestone Xprotect Video driver)Professional plus and Corporate editions)	Milestone Professional plus (Xprotect Professional) NVR Version 2018 R3 Build: 5924 and 2009 R2 Milestone Xprotect Corporate NVR Version: 2019 R3 13.3a Build 44

Controller, options and modules

The heart of the system is a JACE-8000 controller that manages access to a facility by locking or unlocking doors depending on the data received from a badge via a badge reader. The controller processes information that it receives from all physical devices and the data stored in the system database.

The system supports both hardware and software modules. Hardware modules are add-on units that expand the capabilities of a given controller:

Model/option	Supported	Comments
JACE platforms	JACE-8000 all-in-one controller provides access control, HVAC, and video from a single device.	Security JACE 602/616 with Niagara Enterprise Security 2.3 can join to a Niagara Enterprise Security 4.9 Supervisor and replicate.
Option cards	Dual RS-485 Option Card for the JACE-8000	
NAC Controllers	IP Based network integration	The supported controllers are Azure and ZKTeko controllers.

Refer to the hardware documentation to determine how many and which hardware modules your controller(s) need.

Software modules are programs (.jar files) that reside in the system’s `modules` folder. Software modules may require licensing.

Equipment

In addition to controllers, a system consists of a group of devices that work together. These devices can include badges, readers, intrusion detection devices, fire alarm devices, motion detectors, video cameras, and more. The third-party equipment, the number of doors, readers, and other devices impacts the number of modules, enclosures, power supplies and Supervisor PCs the installation needs.

Model/option	Supported	Comments
Cameras	AXIS M5014 Version 5.50.3.1 AXIS M1065–L Version 7.20.1 AXIS 215 PTZ Version 4.49	FFmpeg video on 64-bit clients
Readers	Third-party readers come in a variety of shapes and sizes, with different features. Some have keypads; others have a weather-proof housing; and so on.	These devices detect the information on a badge and transmit it to a controller. Reader categories identify devices by their associated technology, and by the way they read a badge, such as, touch, insertion, and swipe. • Proximity readers require only that the badge pass close to the read surface. • Insertion readers require the person to insert the badge into the reader, often only half way, and then pull the badge out. • Swipe readers require that the badge pass completely through the reader.
Badges/cards	Third-party cards or badges are supported.	The system: • Centrally managed card holder and credential database. • Multiple access cards per person • Supports live credential enrollment from any card reader. • Provides simultaneous support for multiple access card formats. A variety of possible technologies and formats provide badges (also called cards). Some of the most common technologies include: • Bar Code

Model/option	Supported	Comments
		• Barium Ferrite (BaFa) • Magnetic Stripe • Proximity • Smart Card • Wiegand (the system supports Wiegand-style card readers)
Elevator control		
Door hardware	Third-party door hardware.	The system uses a door's latch or dead bolt to lock and unlock the door. There are many types of locking mechanisms. The most common include: • door strikes • magnetic locks • electric door devices • panic or push bars
Remote reader modules	10724, SEC-R2R	DIN-mountable modules that expand the door reader capacity by two, with associated supervised inputs and outputs.
Remote input output modules	10723, SEC-RIO	DIN-mountable modules that expand capacity with eight supervised inputs and eight relay outputs. Inputs and outputs are the physical connections (points) on controller modules. Two types of inputs are available on the modules attached to a controller. • inputs – DI1 through DIn • supervised inputs – SI1 though SIn: In addition to being an input, a supervised input monitors the state of the wiring between the controller and the switch. Output relays serve multiple functions, such as controlling the floors a person may select when riding in an elevator.
Building automation	UL-294 and CE listed systems available for access-control-only installations	

Inputs

Digital inputs (DI) are devices that monitor the state of electronic contacts. These include three general devices:

- Door sensors are contact devices that monitor the state of a door.
- Exit requests provide access to leave through a door without having to present a badge.
- ADA (Americans with Disabilities ACT) controls can be used with power-assisted doors that open and close automatically. On the outside of a facility, you can configure such doors to open only when the door is unlocked (after a validation or during a scheduled unlock period).
- Other inputs include devices that detect a glass break, and motion sensors.

Outputs

Digital outputs (DO) are devices that control door hardware or annunciate an alarm. For example, if a door contact (input) senses that a door has been held open too long, an output bell or horn can audibly alert personnel that the door is open. Outputs may turn on and off lights, heaters and air conditioners.

SmartKey devices

These devices provide a keypad and display screen for arming and disarming assigned intrusion zones.

Capacities

The system supports a limited number of devices, users and database records.

Maximum number of ...	Server	JACE-8000
Personnel	1,000,000	20,000
Card Readers	10,000	32
Access Rights	25,000	250
Schedules	15,000	100
Alarm Capacity	50,000	7,500
Access Zones	25,000	50
Intrusion Zones	N/A	25
Intrusion Keypads	N/A	6
On-line Historical Records	25,000,000	50,000
Simultaneous system users	25	10
Number of controllers	500	n/a

NOTE: To use the web UI to check for your software versions, licensed counts and other information, from the main menu naviagate to **Controller/System Setup** > **Miscellaneous** > **Controller/Server Maintenance**.

Chapter 2. Setup prerequisites

Before installation, a certain amount of planning is required. This includes surveying the third-party equipment already in place, determining needed equipment, identifying any additional third-party requirements, and deciding on names and credentials.

Both hardware and software require configuration and preparation. Before installing software, all controllers, modules, enclosures and power supplies should be installed. Devices, such as readers and keypads should be physically installed and connected to the local area network. The following hardware documentation provides information:

- *JACE-8000 Controller (12977) Mounting and Wiring Guide*
- *Remote 2 Reader Module (10724) Mounting & Wiring Guide.*
- *Remote 2 Reader Module (10724) Mounting & Wiring Guide.*
- *Small (10728) Security Enclosure Install Sheet*
- *Direct I/O-16 Module Installation and Configuration Guide*
- *Direct I/O-34 Module Installation and Configuration Guide*
- *Remote I/O Module (T-IO-16-485) Mounting and Wiring Instructions*
- *Remote I/O Module (10723) Mounting & Wiring Guide*

Before using the system, make sure that all setup prerequisites are met and that the host platform and system components are configured properly.

Licensing

Each installation (controller and Supervisor PC) requires at least one valid license file for operation. This file is specific to the installed platform, which is identified by its host ID that appears in the first line of the license file (a digitally-signed text/xml file). The system uniquely calculates this ID for each device.

Before licensing each controller, you should license your PC to run the software. This PC may be your Supervisor PC, or, if you do not require a Supervisor, this is usually a laptop temporarily connected to the controller or to the network that also serves the controller.

Your purchase of the software starts a license file for the PC that will serve as your Supervisor PC on the licensing server. This unbound license contains a key (a hexadecimal number). Upon fulfillment of an order, the licensing server sends this key to you by email.

When you install the software on the PC, the installation program calculates the host ID for the PC. At the end of installation, an online form that contains the calculated host ID automatically opens. You enter the license key and item number you received in the email along with your name and email address. Using this self-serve process, the licensing server immediately finishes (binds) your host ID to your license key and emails the completed license file back to you as an attachment.

More details about licensing

For more detailed information about licensing your controller or your supervisor, refer to the following topics in the Workbench online help system:

- JACE-8000 Install and Startup Guide

  Preparing for new JACE commissioning
- Niagara 4 Installation Guide

  Confirm the license
- Niagara Platform Guide

  Request License

About the licensing server

Supervisor PC requirements

The software runs on a user-supplied computer providing many of the same functions and benefits that a remote controller provides. This system may run a Supervisor for managing multiple controllers. In a stand-alone installation, it is usually a laptop capable of running the software. Compared to a remote controller, a computer has different requirements and configuration options.

Hardware and operating system

The number of PCs required to serve as system servers depends on the number of remote controllers you require.

Component	250 or less controllers	More than 250 controllers
Processor	Pentium IV @ 2GHz	Core 2 Duo 2GHz
Memory	16 GB	32/64 GB
Disk Capacity	100 GB	250 GB
Operating System	Windows 10 x64 Windows 2016 x64 Windows 2019 x64	Windows 10 x64 Windows 2016 x64 Windows 2019 x64

PC requirements include a working Ethernet adapter with TCP/IP support (browser capable). An Ethernet TCP/IP connection to a controller is required to install the software and configure properties.

NOTE: An administrator-level Windows user account and password for each server platform are required to install the system software.

The computer must be connected to the network that includes the remote controllers.

Java

The PC must be running Sun Java Runtime Environment (JRE) version 1.8 or higher.

Browser

Your Supervisor computer must have access the Internet using a supported browser and to your local area network. The following table includes a list of browser support levels.

Browse	Version Support
Mozilla Firefox	Version 5.0 and later
Niagara Web Launcher	Latest version
Google Chrome	Version 79 and later

These browsers allow you to view both applet views and Hx views concurrently.

Upgrading the OS in the Supervisor PC

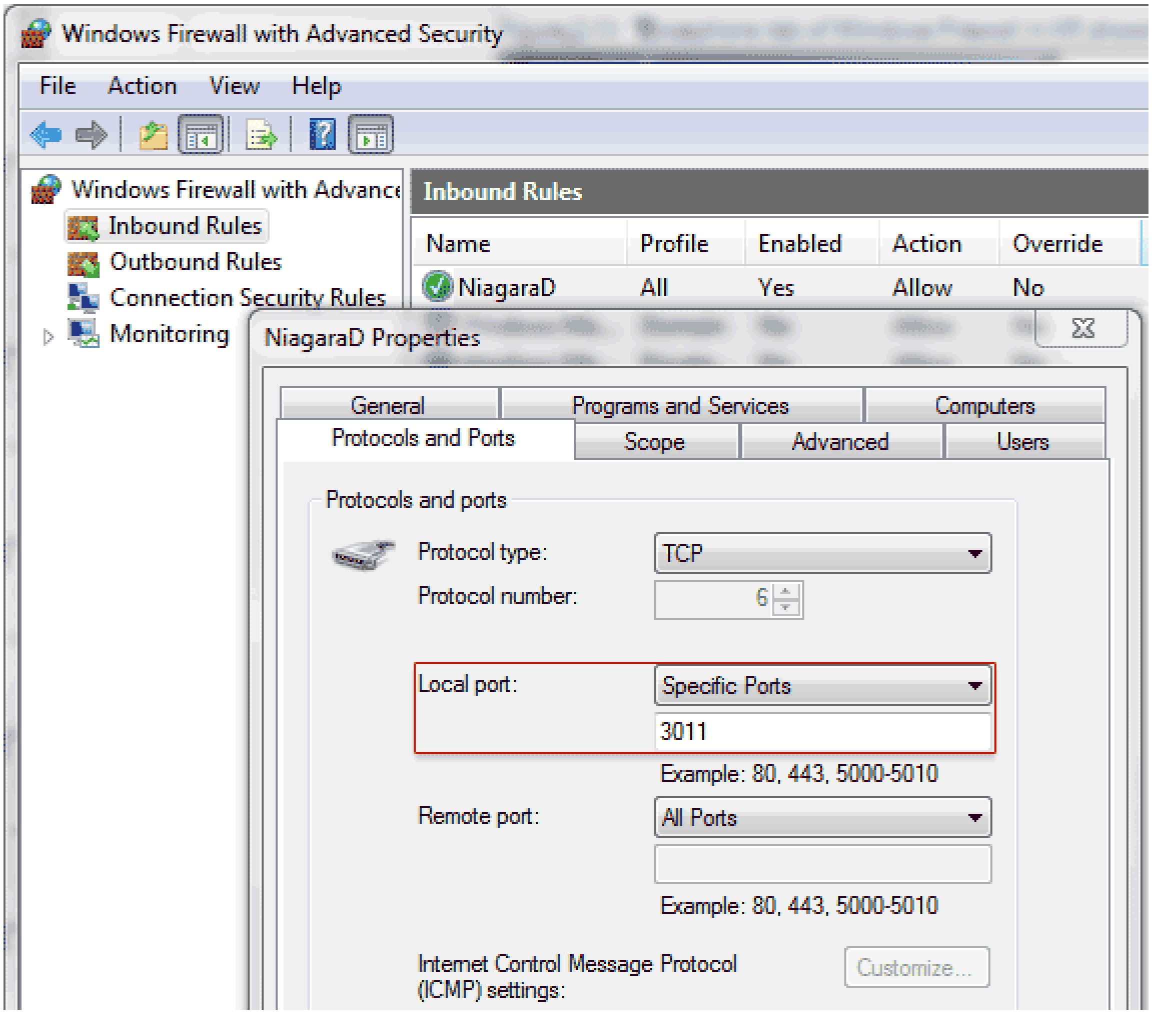
Before installing the software on your Supervisor computer, upgrade the operating system to the latest version, and/or download and install the latest security patches for the specific OS that is running on the Supervisor computer.

Step 1. If you are upgrading the operating system in a computer that already contains a functioning Supervisor station, back up the station to a safe location before updating the operating system.

CAUTION: Typically, an installation of OS updates or security patches ends with a system reboot. Please keep this in mind when you install OS updates on a Supervisor computer. Use the backup feature (System Backups view) to backup your Supervisor station to a safe location, before installing updates!

Step 2. Download and install the latest security patches for the specific OS that is running on the computer.

Step 3. If you are running a firewall, configure it to recognize the station’s port: 3011 or 5011 (if you are using TLS security).



Name	Profile	Enabled	Action	Override
NiagaraD	All	Yes	Allow	No

Protocol type: TCP

Protocol number: 6

Local port: Specific Ports

3011

Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

Supervisor database requirement

All installation procedures that employ a true company-wide solution (anything other than a stand-alone controller) require that, prior to installation, a suitable RDBMS (Relational Database Management System) be installed and running on the Supervisor computer or available to the software on a remote server. You need only one SQL (Structured Query Language) server.

Third-party Orion databases

The system requires an Orion database to store people, badges, access rights, tenants, floors and other data. An Orion database is an open-source RDBMS for managing uncertain data. While any number of databases may appear as options, and may be used to store data, the system provides licenses for, and has been tested with the latest versions of these third-party Orion databases:

- MySQL
- Oracle
- MS SqlServer

Secure database connection

To prevent malicious hacker attacks on the database or station, the station must be able to authenticate the database server (especially if it is remote) and communication between station and server must be encrypted.

Documentation

Some databases may require additional licensing. For more information, refer to this online documentation.

- MySQL database documentation.

  http://dev.mysql.com/doc/
  http://dev.mysql.com/doc/refman/5.1/en/installing.html

- SqlServer database documentation.

  https://docs.microsoft.com/en-us/sql/sql-server/sql-server-technical-documentation?view=sql-server-2017

  https://docs.microsoft.com/en-us/sql/sql-server/install/planning-a-sql-server-installation?view=sql-server-2017

Preparing a MySQL database

The MySQL database is an Oracle Corporation RDBMS that requires a GPL (General Purpose License) or proprietary license.

Prerequisites:
Your computer has access to the Internet. You are preparing a database for the first time.

Step 1. Make a `MySQL` folder on your desktop or somewhere else on your hard drive.

Step 2. Download and extract three resources from `http://dev.mysql.com` (downloading may require you to create an Oracle Account).

- MySQL Community Server
- Connector/J: for this standardized database driver, scroll down to MySQL Connectors. The connector may be named `mysql-connector-java-x.x.x.jar`, where `x.x.x` is the version number.
- MySQLWorkbench (For this application, scroll down to MySQL Workbench.)

Step 3. Run the installer.
Select the `Full` option, which installs both the server and MySQL Workbench. For **`Type of Networking`**, select `Server Computer`.
The installer sets up the server and MySQL Workbench.

Step 4. If possible, verify with the framework release documentation that the version of the Connector/J you downloaded is compatible with the framework.

Step 5. Locate and rename the Connector/J to this generic name: `mysql-connector-java.jar`.

Step 6. Copy the renamed Connector/J to your `C:\Niagara\Niagara.home\jre\lib\ext` folder, where: `C:` represents your drive, and `Niagara\Niagara_home` represents the location and version number of your unique N4 installation.

Step 7. Use MySQL Workbench to create a new schema (new database) and get it running.

Make sure that the new schema has a default Charset/Collation of **`latin1, latin1_bin`**, a user account other than "root," and a strong password.

NOTE: The MySQL default "root" user connects only to a schema associated with localhost. For maximum flexibility and security, create a custom user for your schema.

As a minimum, you will need this information to connect from the Supervisor station to the database:

- Name of the MySQL schema (used in the **`Database Name`** property)
- User Name (other than "root") required to access the schema (used for the **`User Name`** property)
- Password required to access the schema (used for the **`Password`** property)

Acquiring an SQL Server Express database

With SQL Server 2016 Express (Microsoft) you can build desktop and small server data-driven applications up to 10 GB.

Step 1. Navigate to `https://www.microsoft.com/en-us/sql-server/sql-server-editions-express` and download the database.

Step 2. Run the .exe file and follow the installation steps.
For more information, refer to the Microsoft SQL Server Forum.

Result

As a minimum, you will need this information to connect the Supervisor station to this database:

- Name of the MSSQL database (used in the **`Database Name`** property)
- User Name required to access the MSSQL database (used in **`User Name`** property)
- Password required to access the MSSQL database (used as the **`Password`** to access the database)

Security requirements

This system requires the latest technology and procedures to prevent malicious attacks. This includes physical security, running the software on your Supervisor PC behind a firewall, strong password protection, as well as communications security within each station and between stations.

Physical location

In company-wide installation with multiple routers, controllers and Supervisor PCs, each piece of equipment needs to be physically secure. Make sure that no casual visitor has access to these pieces of equipment.

Firewall

A firewall program running on the Supervisor computer is highly recommended. Initially, you should disable the firewall while configuring a new system. After configuration, remember to enable the firewall allowing access through PC ports as necessary.

User names, passwords, and passphrases

- User names and passwords protect access to platforms, stations, and the Supervisor and controller databases.
- A passphrase protects the platform's file system.

All passwords and passphrases are case sensitive.

Best practice: When you receive a new controller, you may choose to power it up and verify that it is functional before placing it in stock ready to assign to a particular job. At this time, its passphrase and user credentials may be very generic. You should create stronger passphrases and passwords before installing the controller at a customer site.

Secure communication

Two aspects of communication are important: encryption, and server authentication. If either is compromised, your system becomes vulnerable to an external attack. Without secure communication links, the remote controllers will not connect to the system station.

PKI (Public Key Infrastructure), which uses certificates to verify server identity and encrypt data transmission, provides this secure link. If the station's server certificate is signed by an external CA (Certificate Authority), such as Verisign and Thawte, EntsecAsureID should connect to a station without requiring additional configuration.

NOTE: Having a recognized CA sign the server certificate provides the highest level of PKI security and requires the least amount of system preparation because the root certificates for recognized CAs already reside in the client's Windows trust store.

If, instead of using an external CA, you are your own CA, you use your root certificate to sign each station's server certificate and import it into the station's User Key Store. Then you import your root CA certificate into each station's Windows trust store.

Secure communication is configured with admin privileges using Workbench. The *Niagara Station Security Guide* explains how secure communication works and provides procedures for creating and signing certificates, and for installing certificates (server and signed CA root certificates) in a station.

Caveat

In Niagara 4.9, RTSP (Real Time Streaming Protocol) over TCP (Transmission Control Protocol), which is used for streaming media servers (video on demand and voice recording), is not secure. It does not use a TLS connection.

Planning lists

As you prepare for an installation, make a list of the hardware, software, licenses, names and codes you need. Print out these pages and keep the actual list secure as you work on the system.

The interview

The interview you have with the customer should identify:

- Which door(s) employees use to routinely enter the building
- On what days of the week they routinely enter the building
- During what hours of the day they routinely enter the building
- Person types
- Departments
- Names of supervisor personnel
- Card formats
- Facility codes
- Access rights

You will use this information in advance to prepare the system and create a blank template file in Excel, which the customer can use to provide comma-delimited personnel records. This guide documents how to set up the system and import the collected personnel data.

Licenses and hardware

System Display Name :______________________________________

Table 1. Licenses

Description	License key	Quantity

Description	License key	Quantity

Table 2. Hardware

Description	Part number	Quantity

Table 3. Third-party power supplies and batteries

Description	Quantity

Table 4. Doors and readers

Description	Module/Location name	Door name	Associated reader

Table 5. Inputs and outputs

Description	Module/Location name	Di/Sdi name

System names

Table 6. Network, platform and station names

Location	IP Address	Network Host Name	Domain name	Platform Passphrase	Station Display Name

Table 7. Platform credentials

Platform/ station IP address or other name	User name	Password
Supervisor		
Controller ...		

Table 8. User names

Role	User name	Password	Email address	Cell/ mobile number
Admin				
Badge Operator				
Maintenance				
Operator				
Personnel Management				

Table 9. Schedule names

Schedule names	Days of the week	Hours of the day

Company root certificate name: ________________________________

Table 10. Certificate folder names

Type of folder	Location	Name
Root certificate folder		
Server CSR folder		
Signed CSR folder		
Server certificate backup (with private keys)		

Table 11. Certificate names

IP Address, Display Name or Domain name (Subject)	Server/host cert name	CSR name	Export name

Table 12. Supervisor station Orion database names and credentials

You need only one of these for a Supervisor station.

Database	Schema/database name	Connector/J version	User Name	Password
My SQL				
MSSQL		N/A		
SQL Server Express		N/A		

Table 13. Controller station HSQL database passwords

Each controller should have a unique and strong password to protect its HSQL database.

IP address or Name	Password

Installing Workbench

A wizard manages the installation of Workbench and the web UI. The software installation ZIP file is available for downloading from your software vendor. This procedure describes how to install Workbench for the first time on a computer.

Prerequisites:
The PC is connected to the network shared by the remote controller(s). You downloaded the Workbench installation executable ZIP file and have the necessary license(s) to use the software.

This computer could belong to a systems integrator who connects it temporarily to the network that supports a stand-alone controller. Or it could be a computer connected to the network and used daily to manage a complex, company-wide system.

NOTE: The system supports only English. Additional lexicons are available to Workbench users only.

Step 1. Close all open applications.

Step 2. Extract all files from the software image ZIP file to any folder on your hard drive.

Step 3. Open Windows Explorer, navigate to the folder you just created, and double-click the `Installer_64.exe` file.
The **`Installation`** wizard opens.

Step 4. To begin the installation, click **Next**, accept the license agreement and click **Next**.

The wizard collects information with a series of prompts including:

- Where to set up the Niagara Home Folder. This folder defaults to:`C:\niagara\niagara` followed by the version numbers. The System Home (Sys Home or niagara_home) is where the wizard installs Workbench, and from where you use Workbench to commission each remote controller. The System Home contains the core software modules, the JRE (Java Runtime Environment), binary executables, and licenses (in the `C:\niagara\niagara[version numbers]\security\licenses` subfolder). It contains no configuration files. Except when upgrading, the runtime files in the System Home are read-only. Although you may specify another location for the System Home, the default folder is generally recommended as the remote controllers use this same System Home directory.

  To enable Workbench to commission remote controllers (hosts), leave **`This instance of ... will be used as an installation tool`** selected.

  If you select a different location for the System Home, a confirmation window requests approval. The **Refresh** button recomputes the space available statistic, and can be useful if you change the target drive location from the default `C:` to another drive partition.

- Where to set up the User Home folder. This location defaults to `C:\ProgramData\Niagara4.x\<brand>`. This folder contains all configurable data including stations, templates, registry, logs and other data. Separating data that can be configured from the software System Home (C:\niagara\niagara) is a security feature of the Niagara Framework and is designed to prevent unauthorized software manipulation.

- What to define for the system passphrase. You may skip this step and set up the system passphrase later.

  The system uses this phrase (which defaults to the factory default platform password: Admin12345) to protect sensitive information stored in file systems, and on the SD card in each controller. The system passphrase encrypts portable files, such as backups and station copies. You should define a strong system passphrase.

  If your installation is licensed for FIPS (Federal Information Processing Standard), the passphrase must be at least 14 characters including at least one number, as well as lower and upper case letters.

  WARNING: Remember, and store the system passphrase in a safe place. If you lose it, you will lose access to encrypted data.

- Where to install shortcuts.

Depending on each individual installation, the wizard may present additional prompts.

Step 5. When all information is collected, click **Next**.

The wizard installs the software and prompts you for what to do next.

The platform daemon is a program that runs independently from the core runtime. It is pre-installed at the factory on every controller, and runs when the controller boots up. The platform daemon, locally installed and running on a PC, opens the Workbench client platform connection to the local (My Host) platform and enables remote client platform connections to the PC.

Step 6. To continue, click **Finish**.
Workbench confirms that the software is licensed. This may take a minute or so. After confirming the license, the wizard closes and, if you configured it to do so, opens Workbench.

Installing the PC's license

If you received a license file as an email attachment, installing it is a matter of saving it to the correct System Home folder.

The System Home folder defaults to the software installation folder: `C:\Niagara\MySoftware` (where `MySoftware` is the version of the system you are installing).

Step 1. Create a subfolder under the `licenses` folder of the System Home, for example, `C:\Niagara\MySoftware\licenses\SupervisorLicenses`

Step 2. Copy the `tridium.license` file to the subfolder you just created.

Managing licenses

The License Manager view allows you to view, upload and remove licenses.

Prerequisites:
The software is installed and configured. You are working in the web UI.

Step 1. To view access this view, click **Controller (System) Setup** > **Miscellaneous** > **License Manager**
The License Manager view opens.

Step 2. To view a license, click on the hyperlinked file name.
The license file opens in the browser.

Step 3. To remove a license, click the check box to the left of the license hyperlink and click **Delete**.

Step 4. To upload a new license, browse for the license in the **Upload New license, certificate or lar File** section, and click **Upload**.

NOTE: If you update your license file you may need to clear your browser cache to view the updated file. For how to clear the browser's cache, refer to your browser documentation.

Chapter 3. Software installation

Installing on a PC or laptop is the first step to configuring a Supervisor platform and station as well as each controller platform and station.

The big steps are:

1. Install Workbench on a PC (either your PC or laptop for a stand-alone network, or the network's Supervisor PC for a company-wide network).
2. Configure and install the certificates required to ensure secure network communication.
3. Commission and configure one or more controllers.
4. Set up users, access rights and schedules.
5. Set up network devices including doors, readers, keypads, etc.
6. Connect and join one or more controllers to the Supervisor.
7. Set up personnel and badges.

Getting to know Workbench

Workbench is the name for the framework's graphical user interface. There are several ways to start Workbench. Depending on your configuration and licensed features additional information may be required.

Prerequisites:
You are working on a PC.

Step 1. To open Workbench click start and navigate to the `Niagara` folder.
The Start menu displays the Workbench options.

Step 2. Click on one of the following:

- To open from an Administrator: Command Prompt window, type `-- start_wb` or `-s` in the command prompt.

  The splash screen opens.
- To open with a background command-line console and launch Workbench, click `(Console)`, type `wb` at the console command prompt, and press **Enter**.

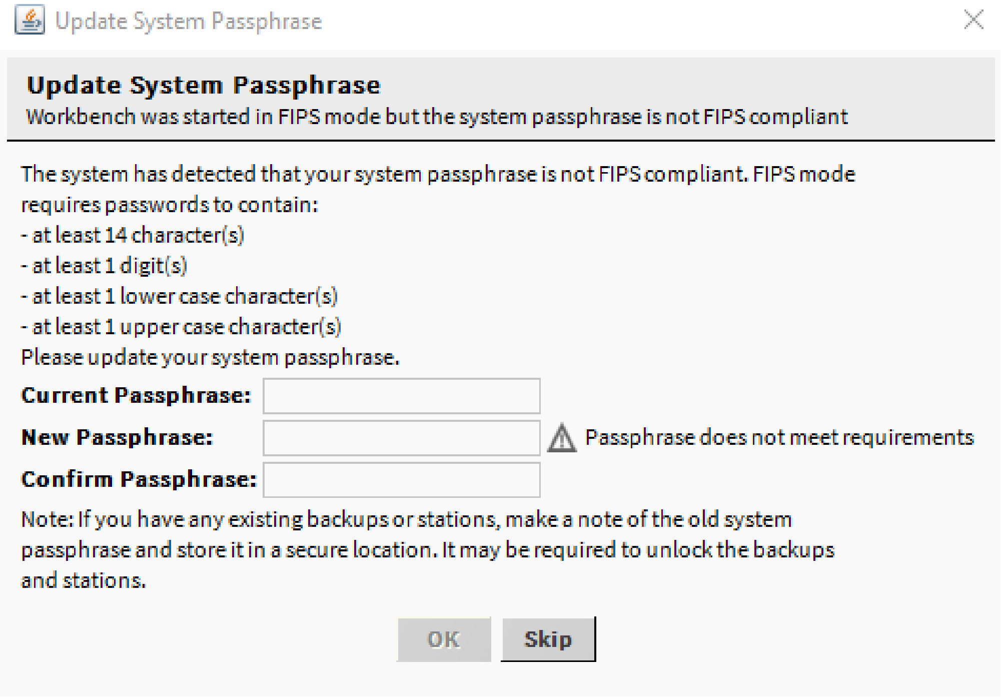
  Workbench opens with a console, which stays open even if you close the program.
- To openWorkbench and a console, click `Workbench (Console)`.

  This opens a command window that immediately launches the program. Closing this console closes the corresponding instance of Workbench.
- Click Workbench alone or double-click its icon on your desktop.

  The splash screen opens.

TIP: Opening Workbench with a background console ensures that you (and Technical Support) have ready access to important diagnostic information in the event that something goes wrong in the Supervisor platform or station. If you wait until you are already experiencing symptoms before you open the console, you may miss the opportunity to gather important data.

If you skipped the passphrase when you installed the software or if your installation requires FIPS, and the passphrase you created does not meet the FIPS requirementsWorkbench prompts you to define the passphrase now.



Update System Passphrase

Workbench was started in FIPS mode but the system passphrase is not FIPS compliant

The system has detected that your system passphrase is not FIPS compliant. FIPS mode requires passwords to contain:
- at least 14 character(s)
- at least 1 digit(s)
- at least 1 lower case character(s)
- at least 1 upper case character(s)

Please update your system passphrase.

Current Passphrase:

New Passphrase: ⚠ Passphrase does not meet requirements

Confirm Passphrase:

Note: If you have any existing backups or stations, make a note of the old system passphrase and store it in a secure location. It may be required to unlock the backups and stations.

Step 3. Enter the current passphrase (defaults to the platform password for new installations), and create a new passphrase or skip it again and click **OK**.
If the platform requires FIPS, skipping this configuration window disables FIPS.

Step 4. If you skipped updating the FIPS passphrase, click **File** > **Non-FIPS Restart**.
Workbench starts again and prompts you to confirm that you choose to work without FIPS.

Step 5. Later, to re-enable FIPS, click **File** > **FIPS Restart**.
Workbench restarts.

Adding the RDBMS driver

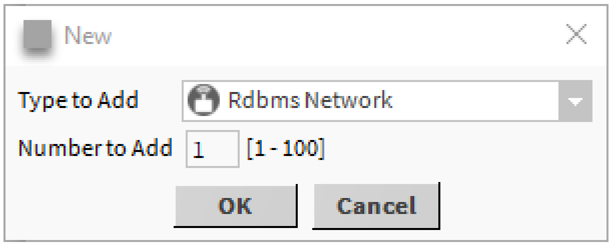
A Supervisor station requires the RDBMS (Relational Database Management System) driver, which supports the Supervisor station’s database. This driver is not appropriate for a controller station.

Prerequisites:
You are using Workbench connected to a Supervisor PC.

Step 1. In the Nav tree, navigate to the **Config** > **Drivers** and double-click on the **Drivers** node.

Step 2. Click the **New** button on the Driver Manager view.

The **New** window opens.

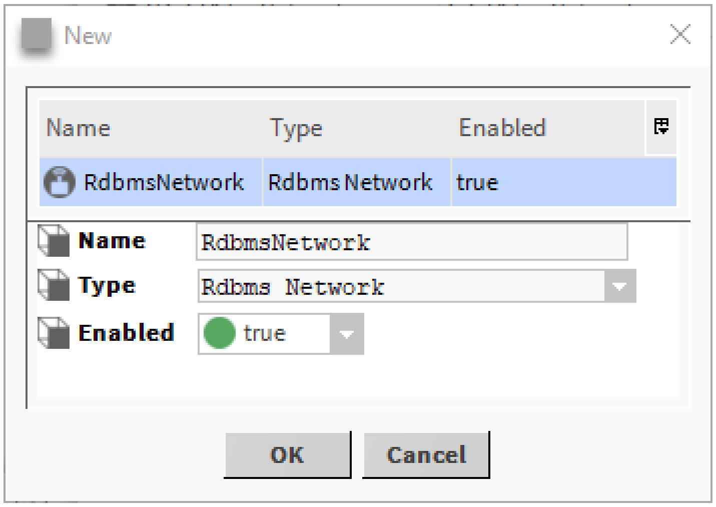


New

Type to Add: Rdbms Network

Number to Add: 1 [1 - 100]

Step 3. Select the `Rdbms Network` from the drop-down list and click **OK**.
A second **New** window opens.



New

Name	Type	Enabled
RdbmsNetwork	Rdbms Network	true

Name RdbmsNetwork

Type Rdbms Network

Enabled true

Step 4. Use this window to give the network a unique name and click **OK**.

Setting up the Supervisor's database password

When you upgrade a Supervisor station from AX to N4, the migrator preserves the password for the Supervisor's third-party database (MySQL, Oracle, MS SqlServer).

Prerequisites:
The third-party database exists in the Supervisor station.

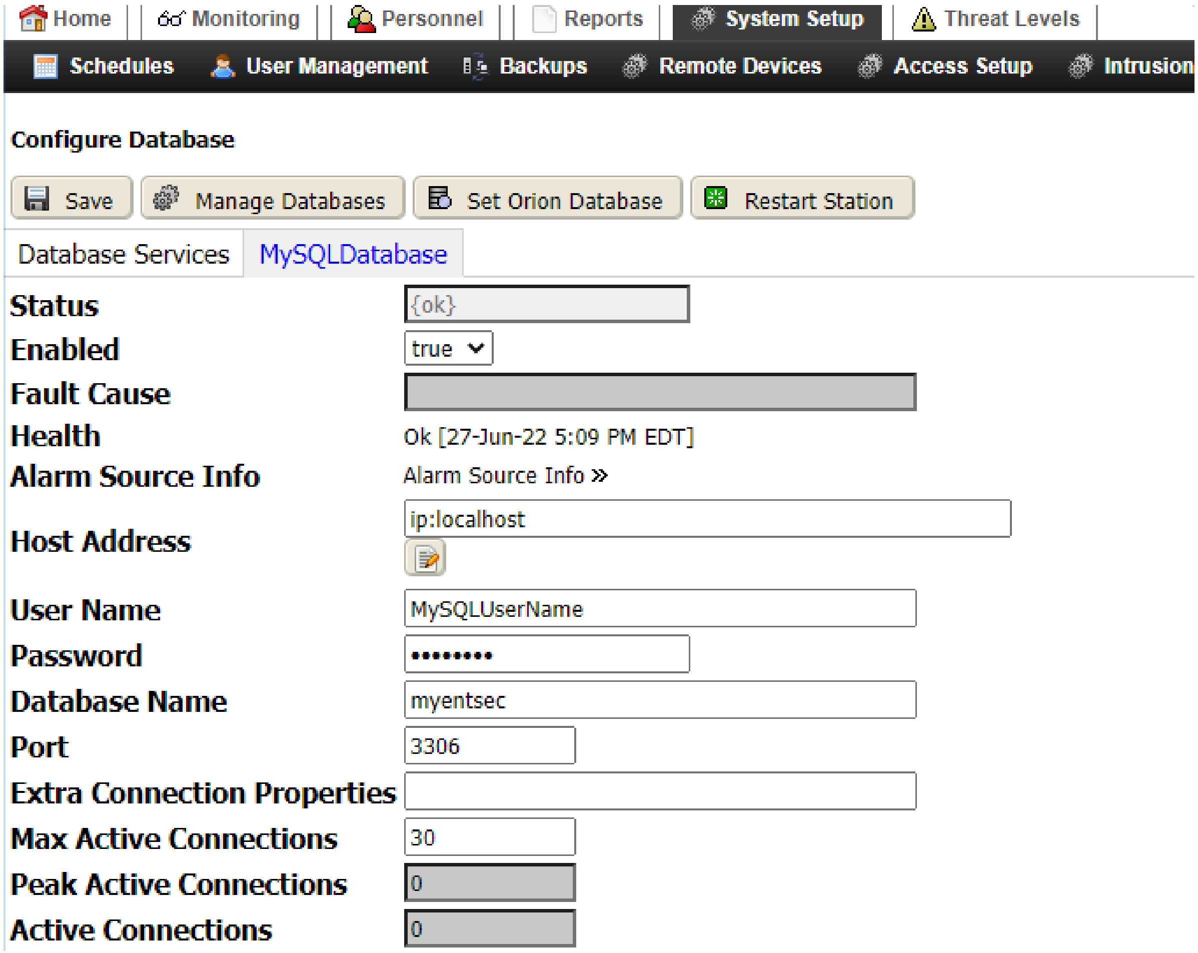
If no database exists in the Supervisor station, create the new database schema and import to the new schema the database tables that you previously exported.

Step 1. Using a browser (web UI), make a connection to the station.

Step 2. Click **System Setup** > **Miscellaneous** > **Configure Database**.
The **Configure Database** view opens to the Database Services tab.

Step 3. Select the Database tab, for example, MySQLDatabase or SqlServerDatabase.

The selected database (MySQLDatabase or SqlServerDatabase.) tab opens.



Configure Database

Status	{ok}
Enabled	true
Fault Cause	
Health	Ok [27-Jun-22 5:09 PM EDT]
Alarm Source Info	Alarm Source Info »
Host Address	ip:localhost
User Name	MySQLUserName
Password	••••••••
Database Name	myentsec
Port	3306
Extra Connection Properties	
Max Active Connections	30
Peak Active Connections	0
Active Connections	0

Step 4. Confirm that:

- **Enabled** is set to `true`.
- **Host Address** is localhost (for the Supervisor station).
- **User Name** is correct for the password.
- **Database Name** matches the name of the database.

Step 5. To change the **Password** type a new, strong password and click **Save**.
The password must contain a minimum of 10 alphanumeric-only characters along with these special characters: @ # ! $ & + > <] [ ) (. The password strength check requires at least: 1 digit, 1 upper case character and 1 lower case character.
After making any database change, the framework restarts the station. After the station restarts, the database should connect using the new credentials, providing data communication from the newly-connected database.

If **Status** is {down} and **Fault Cause** reports that Workbench cannot find the connector even though a connector is in the `C:\Niagara\Niagara-home\jre\lib\ext folder`, make sure that the connector you are using is compatible with the MySQL software version. For example, version 5 connector will not work with MySQL version 8.

The User Name to define on the MySQLDatabase tab is the database User Name, not your station's User name.

Installing Workbench

A wizard manages the installation of Workbench and the web UI. The software installation ZIP file is available for downloading from your software vendor. This procedure describes how to install Workbench for the first time on a computer.

Prerequisites:
The PC is connected to the network shared by the remote controller(s). You downloaded the Workbench installation executable ZIP file and have the necessary license(s) to use the software.

This computer could belong to a systems integrator who connects it temporarily to the network that supports a stand-alone controller. Or it could be a computer connected to the network and used daily to manage a complex, company-wide system.

NOTE: The system supports only English. Additional lexicons are available to Workbench users only.

Step 1. Close all open applications.

Step 2. Extract all files from the software image ZIP file to any folder on your hard drive.

Step 3. Open Windows Explorer, navigate to the folder you just created, and double-click the `Installer_64.exe` file.
The **`Installation`** wizard opens.

Step 4. To begin the installation, click **Next**, accept the license agreement and click **Next**.

The wizard collects information with a series of prompts including:

- Where to set up the Niagara Home Folder. This folder defaults to:`C:\niagara\niagara` followed by the version numbers. The System Home (Sys Home or niagara_home) is where the wizard installs Workbench, and from where you use Workbench to commission each remote controller. The System Home contains the core software modules, the JRE (Java Runtime Environment), binary executables, and licenses (in the `C:\niagara\niagara[version numbers]\security\licenses` subfolder). It contains no configuration files. Except when upgrading, the runtime files in the System Home are read-only. Although you may specify another location for the System Home, the default folder is generally recommended as the remote controllers use this same System Home directory.

  To enable Workbench to commission remote controllers (hosts), leave **`This instance of ... will be used as an installation tool`** selected.

  If you select a different location for the System Home, a confirmation window requests approval. The **Refresh** button recomputes the space available statistic, and can be useful if you change the target drive location from the default `C:` to another drive partition.
- Where to set up the User Home folder. This location defaults to `C:\ProgramData\Niagara4.x\<brand>`. This folder contains all configurable data including stations, templates, registry, logs and other data. Separating data that can be configured from the software System Home (C:\niagara\niagara) is a security feature of the Niagara Framework and is designed to prevent unauthorized software manipulation.
- What to define for the system passphrase. You may skip this step and set up the system passphrase later.

  The system uses this phrase (which defaults to the factory default platform password: Admin12345) to protect sensitive information stored in file systems, and on the SD card in each controller. The system passphrase encrypts portable files, such as backups and station copies. You should define a strong system passphrase.

  If your installation is licensed for FIPS (Federal Information Processing Standard), the passphrase must be at least 14 characters including at least one number, as well as lower and upper case letters.

WARNING: Remember, and store the system passphrase in a safe place. If you lose it, you will lose access to encrypted data.

- Where to install shortcuts.

Depending on each individual installation, the wizard may present additional prompts.

Step 5. When all information is collected, click **Next**.

The wizard installs the software and prompts you for what to do next.

The platform daemon is a program that runs independently from the core runtime. It is pre-installed at the factory on every controller, and runs when the controller boots up. The platform daemon, locally installed and running on a PC, opens the Workbench client platform connection to the local (My Host) platform and enables remote client platform connections to the PC.

Step 6. To continue, click **Finish**.
Workbench confirms that the software is licensed. This may take a minute or so. After confirming the license, the wizard closes and, if you configured it to do so, opens Workbench.

Creating a Supervisor station

To create a Supervisor station you use a station-create wizard within Workbench.

Prerequisites:
You are working in Workbench running on a PC.

Step 1. Click **Tools** > **New Station**.
The New Station Wizard opens.

Step 2. Enter a **Station Name**, select `NewEntSecSupervisorStationTemplate.ntpl` and click **Next**.
The **Next** button remains disabled until you give the station a name. This name is usually a technical name to identify the station. Later you can use the Network TCP/IP Settings view to give the station a friendly **Station Display Name**.
The window for configuring the station password opens.

Step 3. Click **Set Password**, create a strong password, click **OK**

Step 4. Select `copy it to secure platform for "localhost" with Station Copier`, and click **Finish**.
The wizard creates and copies the Supervisor station and displays **Transferring station "[Station Name]"** with two start-up options. These options configure when the station starts. When installing new software or upgrading existing software the recommendation is to leave these options enabled. Otherwise you must start the station in the Application Director before you can connect to it.

Step 5. To continue with the transfer, click **Next**, followed by clicking **Finish**.
The wizard asks if you want to open the Application Director.

Step 6. Click **Yes** and confirm that the station you created is running.

Installing the PC's license

If you received a license file as an email attachment, installing it is a matter of saving it to the correct System Home folder.

The System Home folder defaults to the software installation folder: `C:\Niagara\MySoftware` (where `MySoftware` is the version of the system you are installing).

Step 1. Create a subfolder under the `licenses` folder of the System Home, for example, `C:\Niagara\MySoftware\licenses\SupervisorLicenses`

Step 2. Copy the `tridium.license` file to the subfolder you just created.

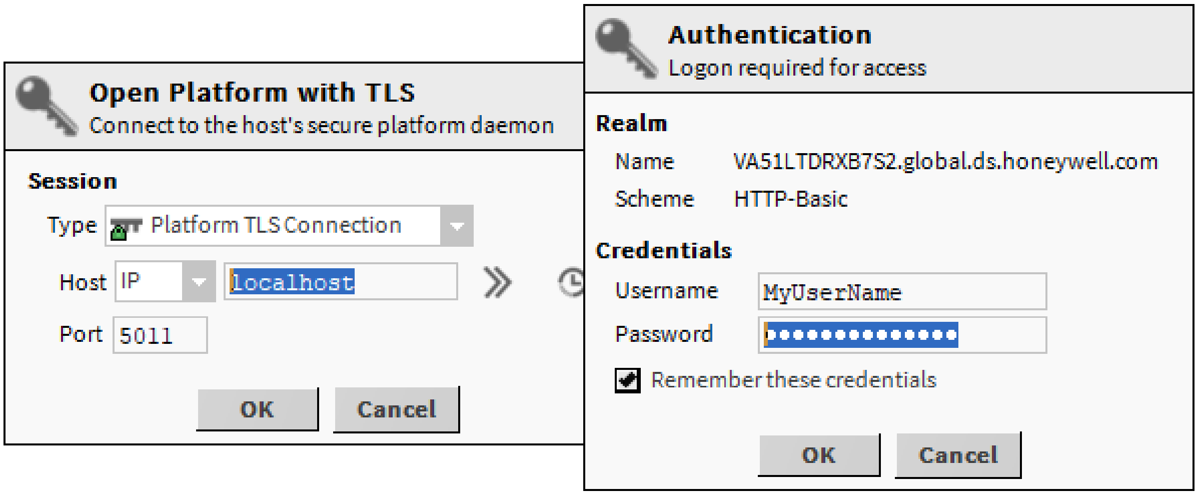
Opening a platform connection to the PC

Opening a platform connection loads the software and utilities related to managing the software's interface to the computer. This connection is required before connecting to a station.

Prerequisites:
Workbench is installed on your PC and running.

Step 1. To open a platform connection to the Supervisor platform (localhost), do one of the following:

- Right-click **My Host** and click **Open Platform**. The **Connect** window opens.
- Expand **My Host** and right-click the platform and click **Connect**. The **Authentication** window opens.
- Click **File** > **Open** > **Open Platform**. The **Connect** window opens.



Open Platform with TLS

Connect to the host's secure platform daemon

Session

Type: Platform TLS Connection

Host: IP localhost

Port: 5011

Authentication

Logon required for access

Realm

Name: VA51LTDRXB7S2.global.ds.honeywell.com

Scheme: HTTP-Basic

Credentials

Username: MyUserName

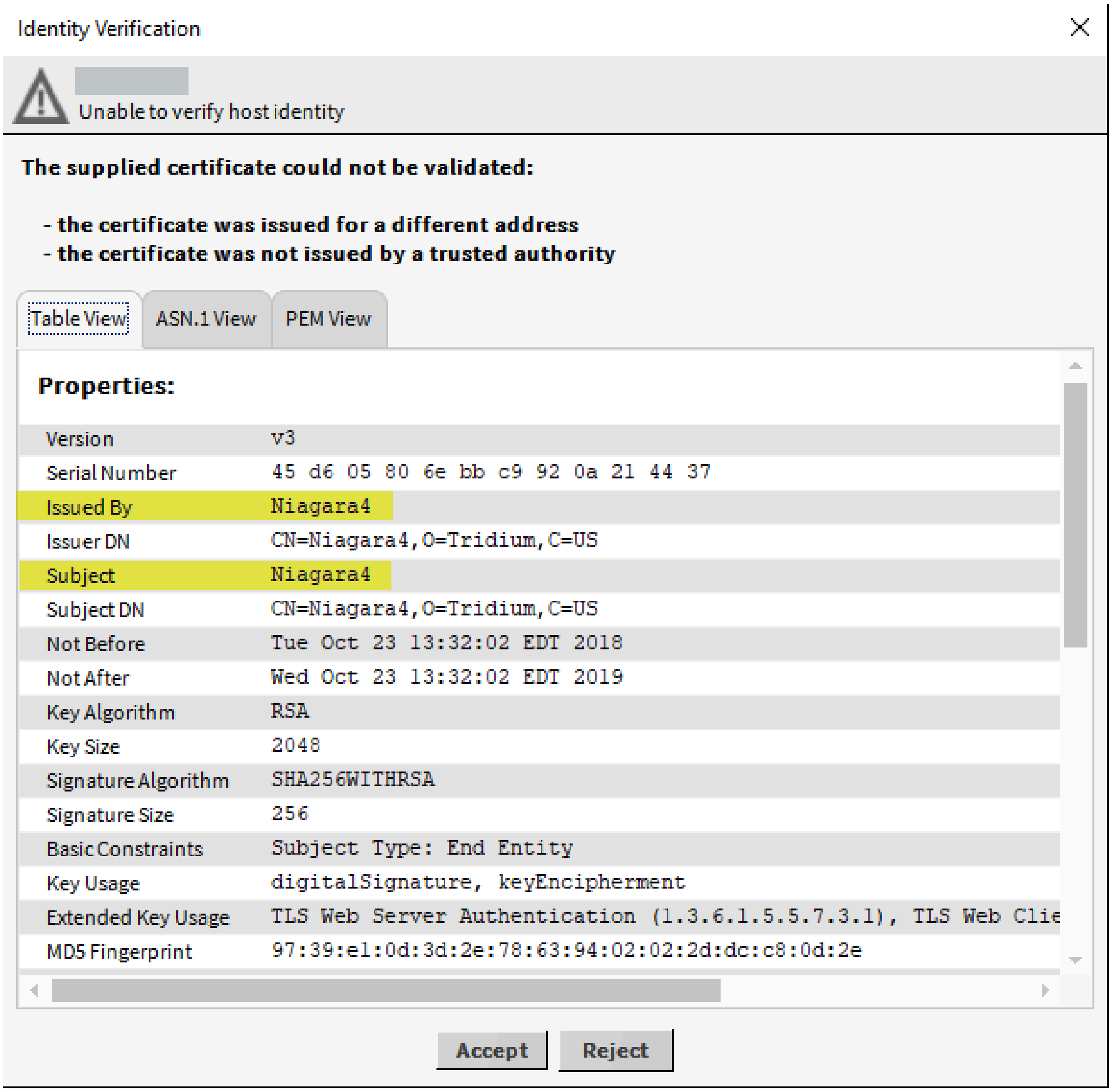
Password: ●●●●●●●●●●●●●●

☑ Remember these credentials

On the left is the **Connect** window. On the right is the **Authentication** window. Both windows assume a secure connection.

Step 2. Enter your computer credentials, enable `Remember these credentials`, and click **OK**.

The **Identify Verification** window opens with the message: `Unable to verify host identity`.



Identity Verification

[redacted]

Unable to verify host identity

The supplied certificate could not be validated:

- **the certificate was issued for a different address**
- **the certificate was not issued by a trusted authority**

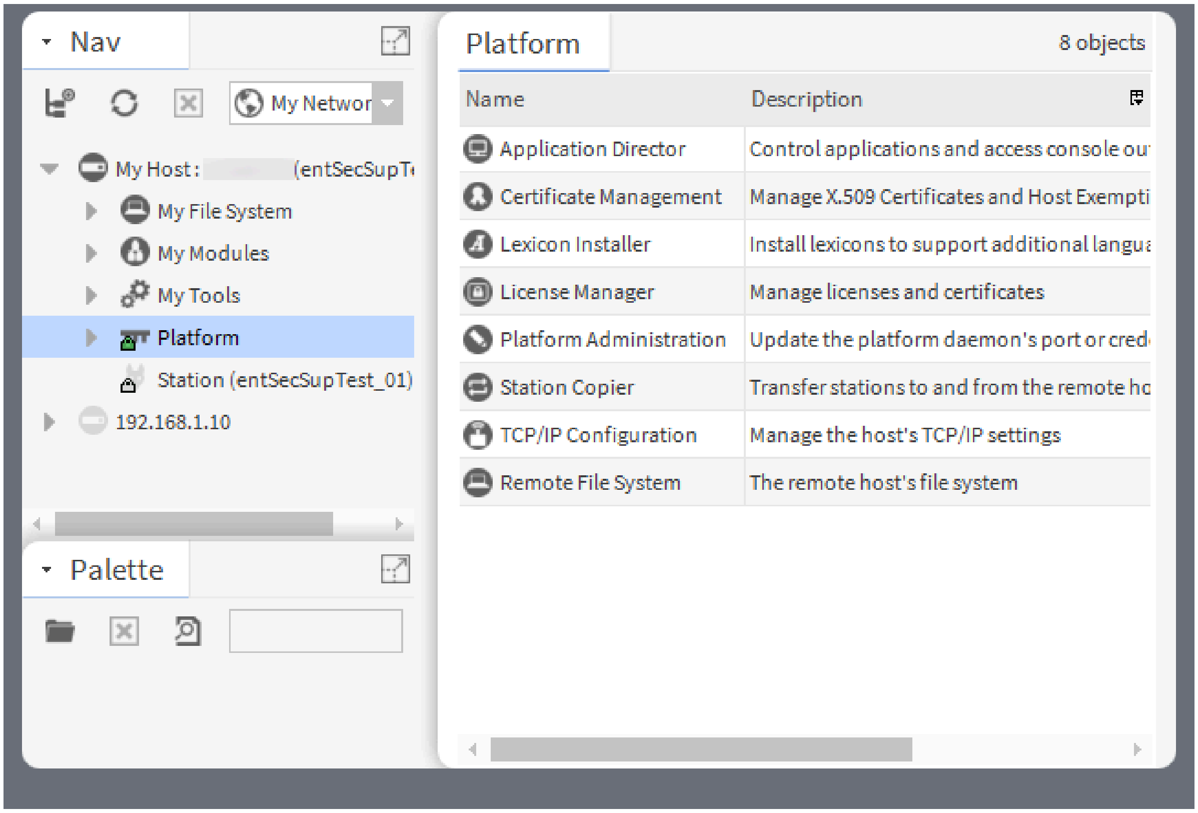
Properties:

Version	v3
Serial Number	45 d6 05 80 6e bb c9 92 0a 21 44 37
Issued By	Niagara4
Issuer DN	CN=Niagara4,O=Tridium,C=US
Subject	Niagara4
Subject DN	CN=Niagara4,O=Tridium,C=US
Not Before	Tue Oct 23 13:32:02 EDT 2018
Not After	Wed Oct 23 13:32:02 EDT 2019
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	SHA256WITHRSA
Signature Size	256
Basic Constraints	Subject Type: End Entity
Key Usage	digitalSignature, keyEncipherment
Extended Key Usage	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1), TLS Web Clie
MD5 Fingerprint	97:39:e1:0d:3d:2e:78:63:94:02:02:2d:dc:c8:0d:2e

An **`Issued By`** property that is the same as the **`Subject`** property indicates that this certificate has been signed by its own private key. As a self-signed certificate, it can encrypt data communication, but it cannot authenticate the server (the platform) to its client (Workbench). This is because none of the root certificates in the Workbench Trust Store recognize this certificate. Since you know that the platform is a valid server you can accept the self-signed certificate temporarily so as to continue. The acceptance of this self-signed certificate is temporary. Later, you will configure signed certificates that provide server authentication as well as data encryption without human intervention.

Step 3. To continue, click **Accept**.

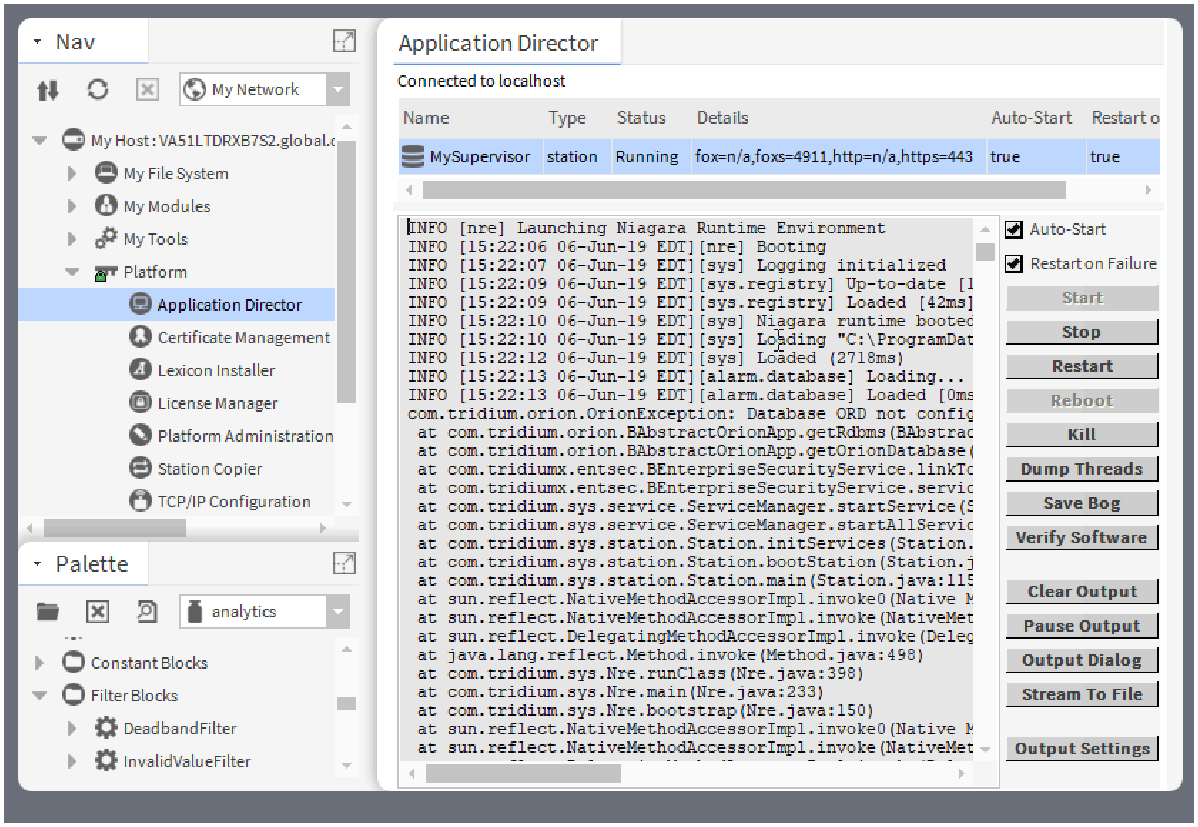
The system completes making the connection between the host and Workbench, and displays the **Nav Container View**.



Name	Description
Application Director	Control applications and access console ou
Certificate Management	Manage X.509 Certificates and Host Exempti
Lexicon Installer	Install lexicons to support additional langu
License Manager	Manage licenses and certificates
Platform Administration	Update the platform daemon's port or cred
Station Copier	Transfer stations to and from the remote ho
TCP/IP Configuration	Manage the host's TCP/IP settings
Remote File System	The remote host's file system

Step 4. Double-click the Application Director

The Application Director view opens.



Connected to localhost

Name	Type	Status	Details	Auto-Start	Restart o
MySupervisor	station	Running	fox=n/a,foxs=4911,http=n/a,https=443	true	true

```
INFO [nre] Launching Niagara Runtime Environment
INFO [15:22:06 06-Jun-19 EDT][nre] Booting
INFO [15:22:07 06-Jun-19 EDT][sys] Logging initialized
INFO [15:22:09 06-Jun-19 EDT][sys.registry] Up-to-date [1
INFO [15:22:09 06-Jun-19 EDT][sys.registry] Loaded [42ms]
INFO [15:22:10 06-Jun-19 EDT][sys] Niagara runtime bootec
INFO [15:22:10 06-Jun-19 EDT][sys] Loading "C:\ProgramDat
INFO [15:22:12 06-Jun-19 EDT][sys] Loaded (2718ms)
INFO [15:22:13 06-Jun-19 EDT][alarm.database] Loading...
INFO [15:22:13 06-Jun-19 EDT][alarm.database] Loaded [0ms
com.tridium.orion.OrionException: Database ORD not config
 at com.tridium.orion.BAbstractOrionApp.getRdbms(BAbstrac
 at com.tridium.orion.BAbstractOrionApp.getOrionDatabase(
 at com.tridiumx.entsec.BEnterpriseSecurityService.linkTc
 at com.tridiumx.entsec.BEnterpriseSecurityService.servic
 at com.tridium.sys.service.ServiceManager.startService(S
 at com.tridium.sys.service.ServiceManager.startAllServic
 at com.tridium.sys.station.Station.initServices(Station.
 at com.tridium.sys.station.Station.bootStation(Station.j
 at com.tridium.sys.station.Station.main(Station.java:115
 at sun.reflect.NativeMethodAccessorImpl.invoke0(Native M
 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMet
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(Deleg
 at java.lang.reflect.Method.invoke(Method.java:498)
 at com.tridium.sys.Nre.runClass(Nre.java:398)
 at com.tridium.sys.Nre.main(Nre.java:233)
 at com.tridium.sys.Nre.bootstrap(Nre.java:150)
 at sun.reflect.NativeMethodAccessorImpl.invoke0(Native M
 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMet
```

Step 5. If you cannot see the station, click the top of the console and drag down.

Step 6. To start the station, click **Start**.

Setting up domain names

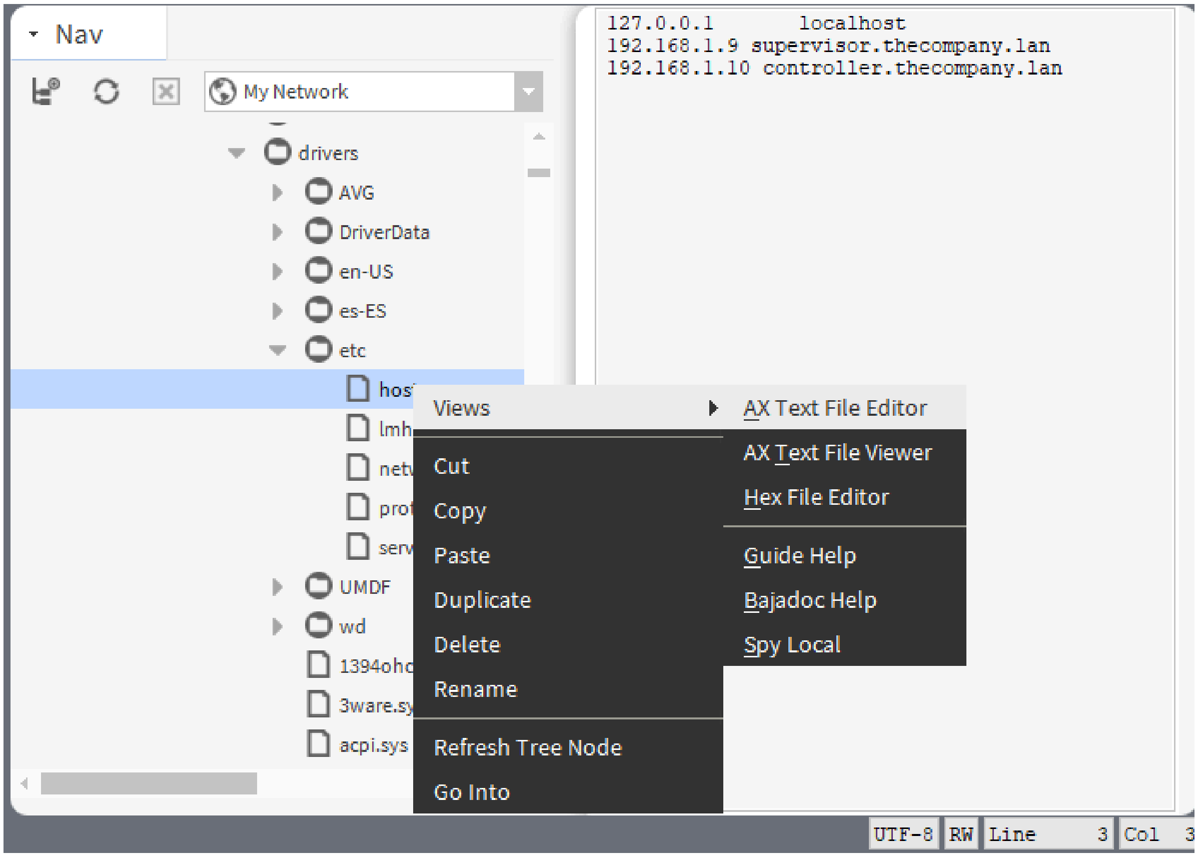
In the absence of a DNS (Domain Name System) server, the system can correlate station IP addresses with domain names. Domain name connections may be easier to remember than IP addresses.

Prerequisites:
You are connected to a computer and running Workbench.

Step 1. Open Workbench using **Run as administrator** (right-click the icon on the desktop and click **Run as administrator**, or right-click the application in the start menu and click **More** > **Run as administrator**.

Step 2. In the Nav tree, expand **My File System** > **C:** > **Windows** > **System32** > **drivers** > **etc**, right-click `hosts` and click **AX Text File Editor**.

The hosts file opens in the AX Text File Editor view editor.



```
127.0.0.1       localhost
192.168.1.9 supervisor.thecompany.lan
192.168.1.10 controller.thecompany.lan
```

Step 3. Scroll to the end of the document, place your cursor at the end of the last line and press Enter to create a new line.

Step 4. Type a line for each Supervisor and controller:
`<999.999.99.99 >` where:

- `<999.999.99.99>` is the IP address on the network of the PC or controller.
- `<domainName>` is the domain name the system can use to connect to the controller.

There must be at least one space between the IP address and the domain name on each line.

Step 5. Click the Save button (💾).

Step 6. To verify that the hosts file contains the domain names, open a platform connection to your localhost and double-click **TCP/IP Configuration**.

Step 7. To open the **`Hosts File`**, click the double down arrows (⏬).

Step 8. If needed, scroll to the bottom of the file and confirm that the IP addresses are associated with the correct display names.

Chapter 4. System security

The system exists to protect buildings and the people who work in them from multiple external threats. This chapter concerns securing this system itself so that only authorized users may view and configure its properties, and all communication within the system is protected from malicious activity.

The security of your access system relies on these factors:

- Physical protection: Supervisor stations need to be located in physically secure areas. Controllers need to be located where they cannot be easily accessed by unauthorized personnel.
- Data communication and server authentication should be secured by signed PKI (Public Key Infrastructure) certificates.
- Passwords need to be robust and changed regularly.
- User permissions need to be configured based on need. Few should serve as administrators with unfettered access to platforms and stations.

Most of the procedures in the chapter use Workbench running on a PC. Some procedures are also available in the web UI.

Secure communication certificate setup

Secure communication applies to data transmitted among entities, which may be geographically far apart. The Niagara Framework supports TLS (Transport Layer Security), a cryptographic protocol for server authentication and secure encryption of data over the Internet. This is the same level of security provided by credit card companies and banks.

Setting up a secure network involves one or more of these tasks:

- Creating folders to organize PKI (Public Key Infrastructure) certificates and certificate signing requests.
- Creating a root CA (Certificate Authority) certificate (if the company serves as its own certificate authority).
- Creating server certificates, one for each PC, controller/station, and other connected device, such as a camera.
- Sending a certificate signing request for each server certificate to a recognized external CA for signing, or signing the requests in house using the company's root CA certificate with its private key.
- Matching the signed server certificate requests with the original certificates.
- Configuring each platform/station for secure communication. This step identifies the certificate.
- If the company serves as its own CA, importing its root CA certificate with its public key into the User Trust Store of each controller and PC, into the Windows trust store, and into the browser trust store.
- Confirming the Windows certificate.
- Importing the root CA certificate into the Java Control Panel.

If you can connect to all the subordinate stations and devices in the network, you can perform all of these steps using Workbench running on a single PC. If the network is geographically distributed, you may need to transport certificates. You can email the root CA certificate with only its public key. Do not email any certificate with its private key.

You can also use the Certificate Wizard to create a root CA and server certificates, however, if you are new to certificate management, work through the individual steps using the Certificate Management tool. This will give you a better understanding of the steps. Then use the wizard.

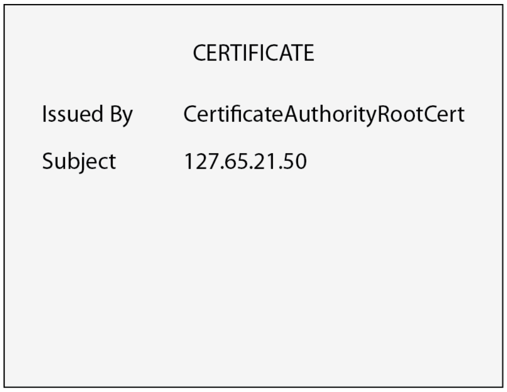
PKI certificates

TLS uses PKI (Public Key Infrastructure) certificates to authenticate each server and encrypt data transmitted within the system.

Signed certificates

A certificate is an electronic document, signed by a recognized CA (Certificate Authority), which proves to a network client that the presenting server owns a valid public key.

Figure 3. A signed certificate



CERTIFICATE

Issued By	CertificateAuthorityRootCert
Subject	127.65.21.50

Among the many properties in a certificate, a certificate's **`Subject`** identifies the entity to which the certificate belongs, that is, its owner. This is usually an IP address or a **`Station Display Name`**. Its **`Issued By`** property identifies the root certificate of the CA that signed the certificate after verifying the validity of the owner and the certificate's key. Without a CA-signed certificate, a client cannot authenticate the server and no communication should take place.

Some connections occur over a local area network. Others include a browser and the Internet. For communication to be secure, certificate authentication and encryption is required at each connection step: device or service through Niagara to another device on the LAN or through a network firewall to a browser and on to the Internet.

In a LAN, each platform/station can function as a server and as a client. Workbench is always a client. As a server, each platform/station presents its own signed certificate to the client. As a client, Workbench and each platform/station authenticate a received server certificate by comparing it with the root CA certificate in the client's trust store that signed the server certificate.

If a secure network connection cannot be made between server and client, you may temporarily accept the server's self-signed certificate.

In a broader connection that includes the Internet, a remote device, such as a camera is a server that sends live and recorded video to a client station. The browser in an Internet connection requires that the camera have a signed server certificate that is recognized by a root CA certificate in its (the browser's) trust store.

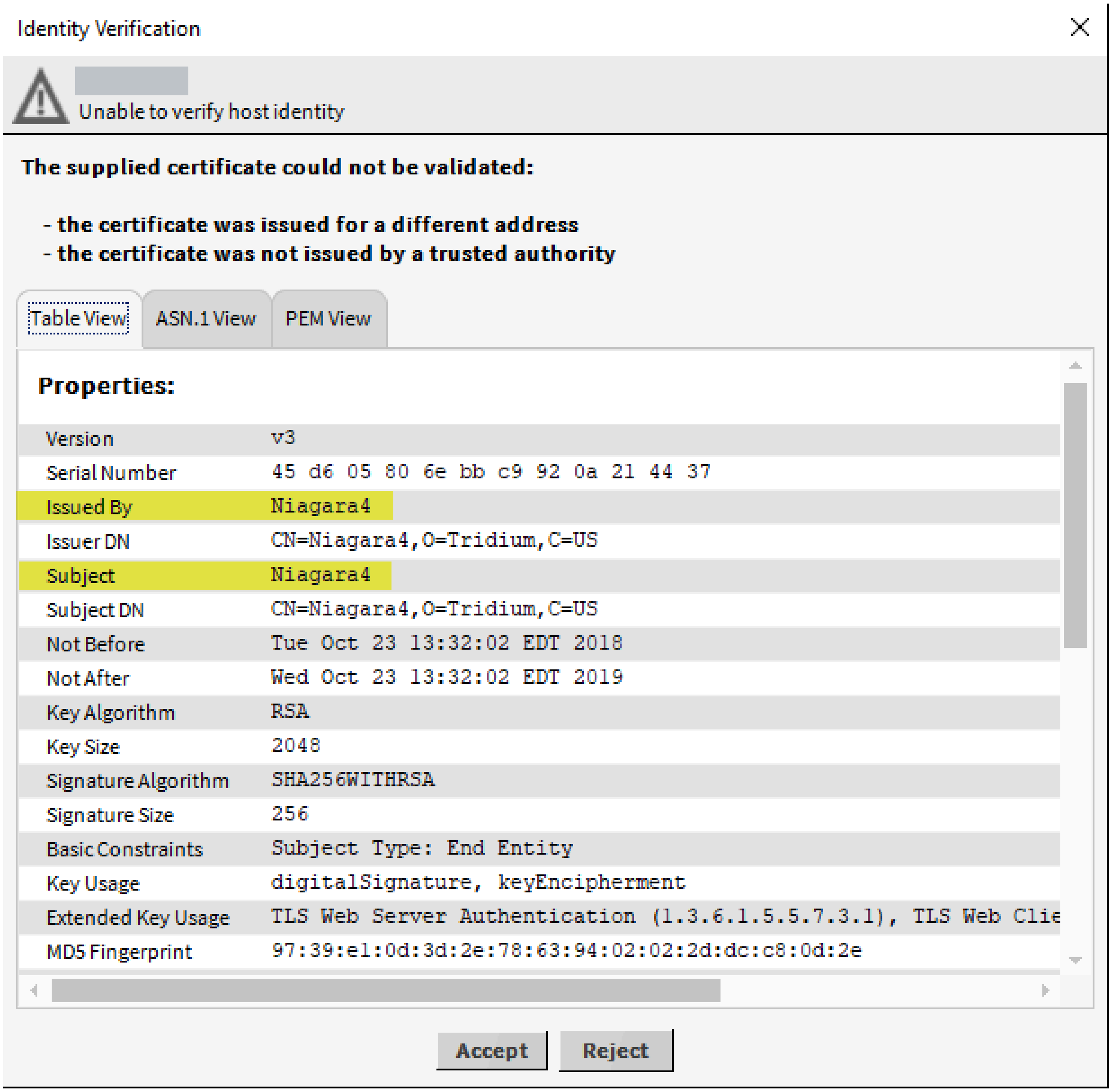
If the camera cannot make a secure browser connection, you may have to temporarily connect using http://. If you switch from an https:// to an http:// connection, empty the browser's cache before attempting the http:// connection.

The best practice is to use only server certificates signed by a root CA certificate in the clients' (station and browser) trust stores. This chapter explains how to install a server certificate in a station. You install a signed server certificate in a camera using its configuration web page.

Self-signed certificates

When you connect to a Supervisor and controller platform/station for the first time using Workbench, the platform/station, functioning as a server, presents its default self-signed `tridium` certificate to Workbench.

Figure 4. A self-signed certificate



Identity Verification

[redacted]

Unable to verify host identity

The supplied certificate could not be validated:

- the certificate was issued for a different address
- the certificate was not issued by a trusted authority

Properties:

Version	v3
Serial Number	45 d6 05 80 6e bb c9 92 0a 21 44 37
Issued By	Niagara4
Issuer DN	CN=Niagara4,O=Tridium,C=US
Subject	Niagara4
Subject DN	CN=Niagara4,O=Tridium,C=US
Not Before	Tue Oct 23 13:32:02 EDT 2018
Not After	Wed Oct 23 13:32:02 EDT 2019
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	SHA256WITHRSA
Signature Size	256
Basic Constraints	Subject Type: End Entity
Key Usage	digitalSignature, keyEncipherment
Extended Key Usage	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1), TLS Web Clie
MD5 Fingerprint	97:39:e1:0d:3d:2e:78:63:94:02:02:2d:dc:c8:0d:2e

You can tell that this server certificate is self-signed rather than CA-signed because its **`Issued By`** property and **`Subject`** property are the same. In other words, it signed itself. The system can use this certificate to encrypt data transmitted between client and server but it cannot use this certificate to authenticate the server. You manually authenticate the server by accepting this self-signed certificate.

For communication between entities to be secure without human intervention, each platform/station must present to a client its own signed server certificate, and each client needs a copy of the root CA certificate used to sign the server certificate so that the client can compare the signatures and verify the server's identity.

Each browser you use (which functions as a client) also requires the root CA certificate used to sign the server certificate(s) sent to it.

After the identity of the server is verified, encrypted communication using the certificate keys begins.

Connections that require security

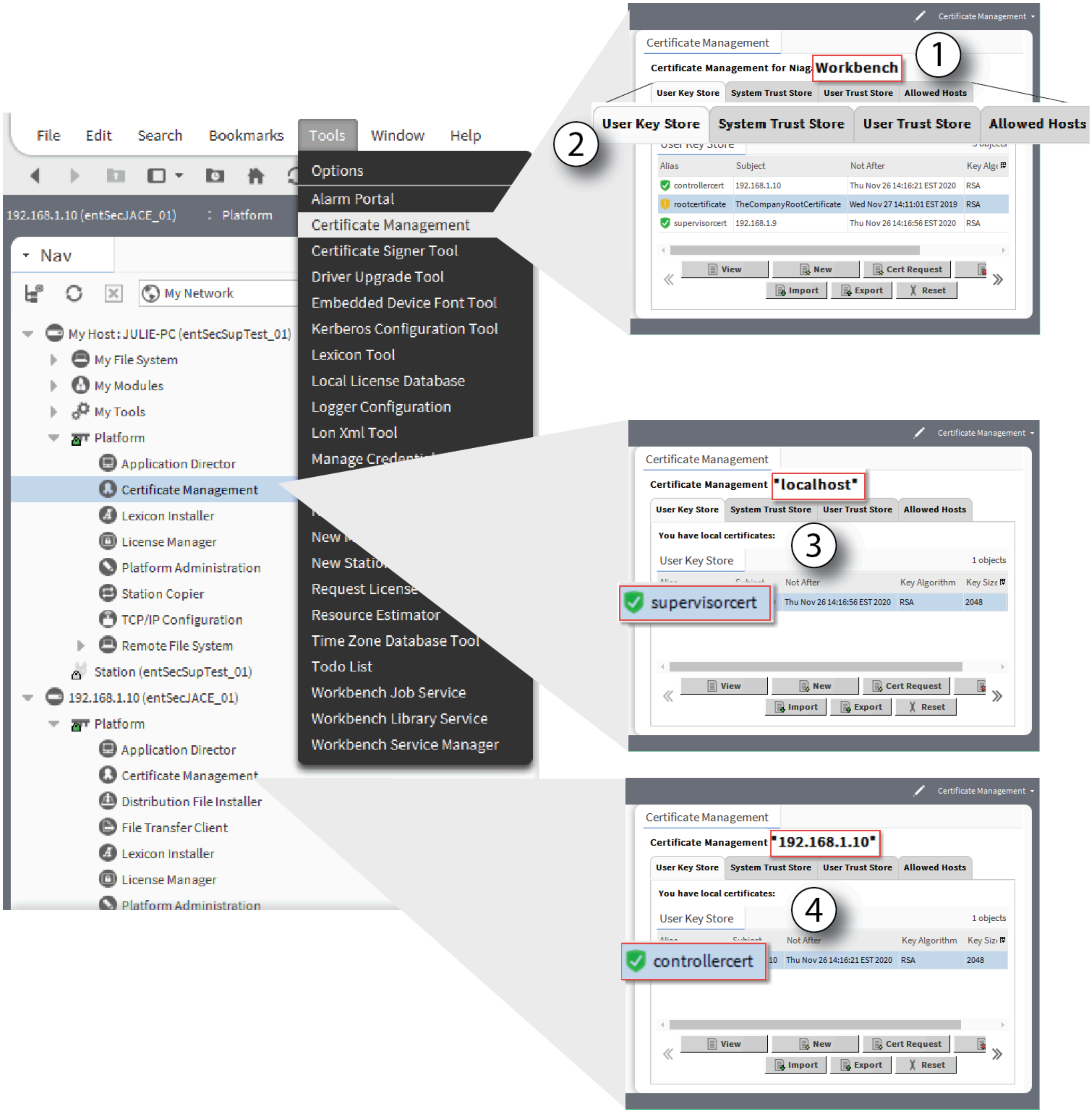
Many connections within a system require security, including:

- Platform/station to Workbench connection (Niagarad)
- Computer to platform (Niagarad)
- Station to local or remote Supervisor (Https)
- Supervisor to local or remote platform/station (Foxs)
- Browser to station (Https)
- Station to station (Foxs)
- Database connection
- Station to DVR/NVR/camera connection (Https)
- Other device connections
- LDAP connection

Certificate stores

Each platform and its station share the same set of certificate stores. A certificate store is where the system and standard Internet browsers keep store certificates.

Figure 5. Certificate Management stores



Certificate Management for Niag Workbench

User Key Store

Alias	Subject	Not After	Key Algo
controllercert	192.168.1.10	Thu Nov 26 14:16:21 EST 2020	RSA
rootcertificate	TheCompanyRootCertificate	Wed Nov 27 14:11:01 EST 2019	RSA
supervisorcert	192.168.1.9	Thu Nov 26 14:16:56 EST 2020	RSA

Certificate Management "localhost"

You have local certificates:

User Key Store 1 objects

Alias	Not After	Key Algorithm	Key Size
supervisorcert	Thu Nov 26 14:16:56 EST 2020	RSA	2048

Certificate Management "192.168.1.10"

You have local certificates:

User Key Store 1 objects

Alias	Not After	Key Algorithm	Key Size
controllercert	Thu Nov 26 14:16:21 EST 2020	RSA	2048

The screen captures show the User Key Store tab for three sets of certificate stores, which you can access from Workbench.

1. Clicking **Tools** > **Certificate Management** opens the Workbench **Certificate Management** view.
2. Four stores populate each Certificate Management view, each with a tab:
   - The User Key Store tab contains the platform/station's server certificate.
   - Each System Trust Store contains the root CA certificates (with only the public key of each) for the

most common external certificate authorities.

- The User Trust Store tab contains the root CA certificate (with only its public key) of the company when it serves as its own CA.
- The Allowed Hosts tab contains the self-signed certificates that require human verification of their authenticity.

Icons identify the state of each certificate in the tabs of the **Certificate Management** view.

- A green shield with a check (tick) mark (✓) identifies signed certificates and approved exceptions (self-signed certificates that have been accepted).
- A yellow shield with an exclamation mark (!) identifies a self-signed certificate. A server certificate is one of these until it gets signed. The root CA certificate is forever one of these. There is no higher authority to sign it!
- A red shield with a white X (✗) identifies a rejected exception.

3. Expanding the localhost **Platform** node and double-clicking **Certificate Management** opens the localhost (PC) **Certificate Management** view. These stores belong to a PC's platform and station.
4. Expanding a controller **Platform** and double-clicking **Certificate Management** opens the controller's **Certificate Management** view. These stores belong to a controller platform and station.

The called-out information above explains how to access the Certificate Management stores from each Workbench and **Platform** node. The same stores for each platform/station are also available under the **Station** node in the Nav tree by expanding **Station** > **Config** > **Services** > **Platform Services**, and double-clicking **CertManagerService**.

To access the same stores using the web UI, click **Controller (System) Setup** > **Remote Devices** > **Certificate Management**.

The goal for each platform/station is for its server certificate, which is visible in the User Key Store, to be signed (green shield) by either a root CA certificate in the System Trust Store or User Trust Store, and for its Allowed Hosts tab to be empty.

To demonstrate all functions, this chapter assumes you are serving as your own CA (Certificate Authority). The steps require administrative privileges and use Workbench to create a root CA certificate, export server certificates, sign server certificate signing requests, import them back into the User Key Store, and import the root CA certificate into the station's User Trust Store.

Getting all your PKI certificates configured up front should make life easier when you start configuring network devices. The *Niagara Station Security Guide* provides more detailed information about how PKI certificates work.

Creating certificate storage

The first time you access a Certificate Management view, the system creates an empty `certManagement` folder in its User Home (Niagara 4 and later) or Sys Home (NiagaraAX).

Prerequisites:
You have admin privileges and are working in Workbench on a PC (Supervisor or otherwise). All controllers have been commissioned.

Step 1. To open the Certificate Management tool, click **Tools** > **Certificate Management**.
This opens the Workbench the User Key Store.

Step 2. To view the `certManagement` folder, expand the Nav tree: **My Host** > **My File System** > **User Home** > **certManagement**.

Step 3. To create a new folder, right-click **certManagement**, and click **New** > **New Folder**.

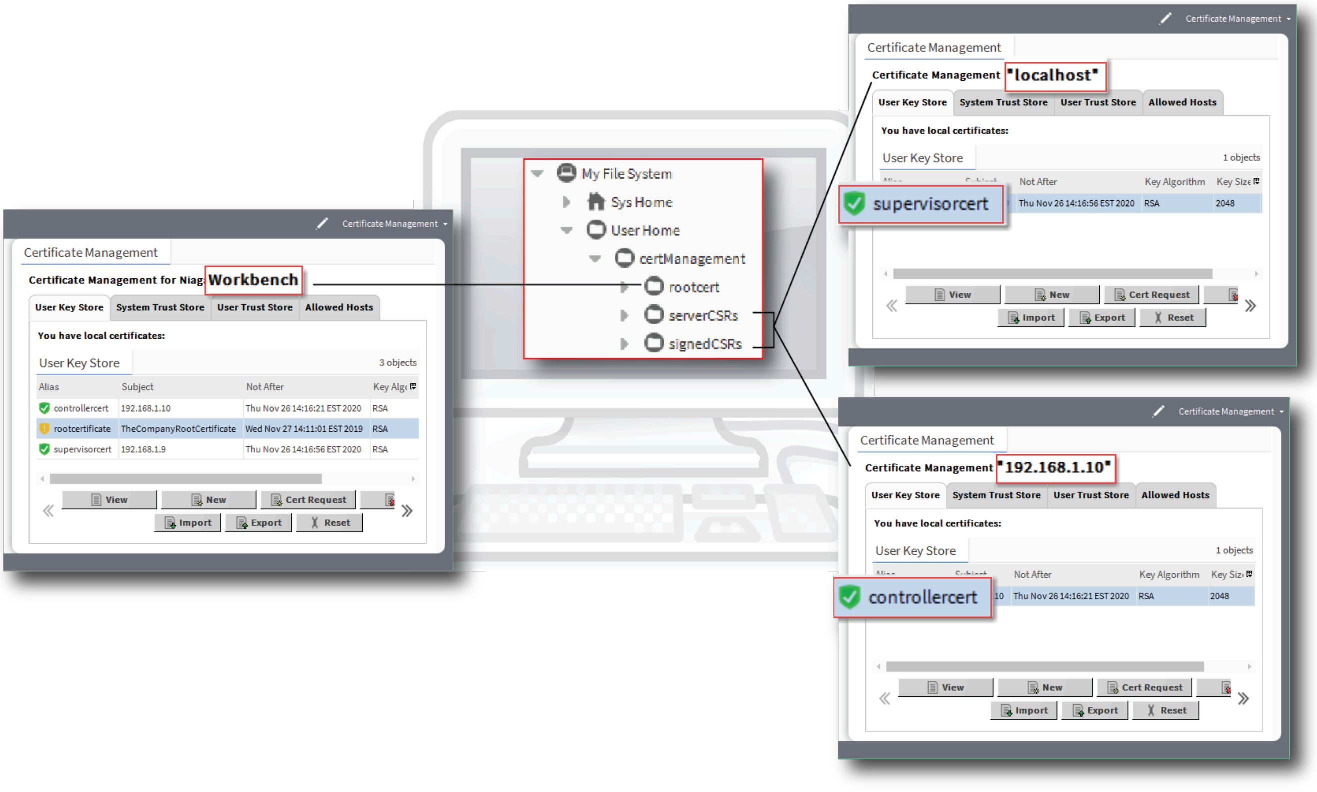
Step 4. Name the folder `rootcert`.

Step 5. Create two more folders naming them `serverCSRs` and `signedCSRs`.

Result

The file system on your PC serves as the central location for setting up PKI certificates.

Figure 6. The central location for certificate management



Certificate Management for Niag: Workbench

You have local certificates:

User Key Store 3 objects

Alias	Subject	Not After	Key Algo
controllercert	192.168.1.10	Thu Nov 26 14:16:21 EST 2020	RSA
rootcertificate	TheCompanyRootCertificate	Wed Nov 27 14:11:01 EST 2019	RSA
supervisorcert	192.168.1.9	Thu Nov 26 14:16:56 EST 2020	RSA

Certificate Management "localhost"

You have local certificates:

User Key Store 1 objects

Alias	Subject	Not After	Key Algorithm	Key Size
supervisorcert		Thu Nov 26 14:16:56 EST 2020	RSA	2048

Certificate Management "192.168.1.10"

You have local certificates:

User Key Store 1 objects

Alias	Subject	Not After	Key Algorithm	Key Size
controllercert	10	Thu Nov 26 14:16:21 EST 2020	RSA	2048

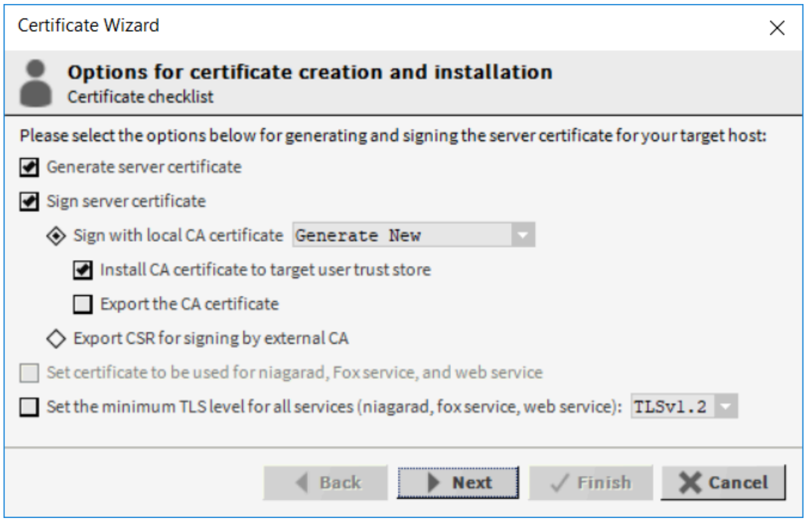
To simplify what can be a complex process, this document encourages you to create a root certificate and server certificate(s) using Workbench and the `certManagement` folders. If your installation involves a single controller, you may not need these folders, but in a large company-wide installation, separating the certificates and CSRs simplifies the task. Using intermediate certificates (refer to the *Niagara Station Security Guide*) only increases the complexity making some type of folder structure unavoidable.

Certificate Wizard

The latest Niagara version supports a **Certificate Wizard**. This wizard, available as a view on the platform root, provides a complete, continuous workflow that helps you properly set up certificates to harden a platform and station against cyber attack.

The wizard assumes prior experience in various types of certificate setup and a reasonable level of confidence in performing such procedures as are commonly done using the **Certificate Management** tool. That being the case, you will find that the **Certificate Wizard** simplifies the certificate setup process for a station by combining several steps into a continuous workflow. If you are unfamiliar with certificates, work through individual setup procedures using the **Certificate Management** tool as described elsewhere in this guide. The individual procedures will help you gain a better understanding of the steps involved.

Figure 7. Certificate Wizard platform tool with default selections


Certificate Wizard

Options for certificate creation and installation
Certificate checklist

Please select the options below for generating and signing the server certificate for your target host:

☑ Generate server certificate

☑ Sign server certificate

◆ Sign with local CA certificate: Generate New

☑ Install CA certificate to target user trust store

□ Export the CA certificate

◇ Export CSR for signing by external CA

□ Set certificate to be used for niagarad, Fox service, and web service

□ Set the minimum TLS level for all services (niagarad, fox service, web service): TLSv1.2

As an alternative to using the **Certificate Management** tabs to create and install a CA root certificate, the **Certificate Wizard** generates the root CA certificate and exports it with only its public key in preparation to install in a browser.

NOTE: The **Certificate Wizard** is intended to be used for a single platform at a time, not for provisioning multiple platforms.

The **Certificate Wizard** may be configured to perform some or all of the following tasks:

- Generate a new root CA certificate on the local host that can be used to sign all server certificates.
- Generate a new server certificate for a host platform.
- Sign a server certificate with a new or existing root CA certificate.
- Export a server certificate CSR (signing request) for signing by an external certificate authority.
- Install a root CA certificate into the **User Trust Store** of a platform/station selected from the daemon directory.

Once the **Certificate Wizard** generates the files, they must still be installed into all of the appropriate devices. This is accomplished via the **Certificate Management** tool found in the Workbench **Tools** menu.

Generating a CA certificate and signed Server certificate using the Certificate Wizard

This procedure describes how to use the **Certificate Wizard** workflow to complete a series of certificate-related steps for a platform and/or station.

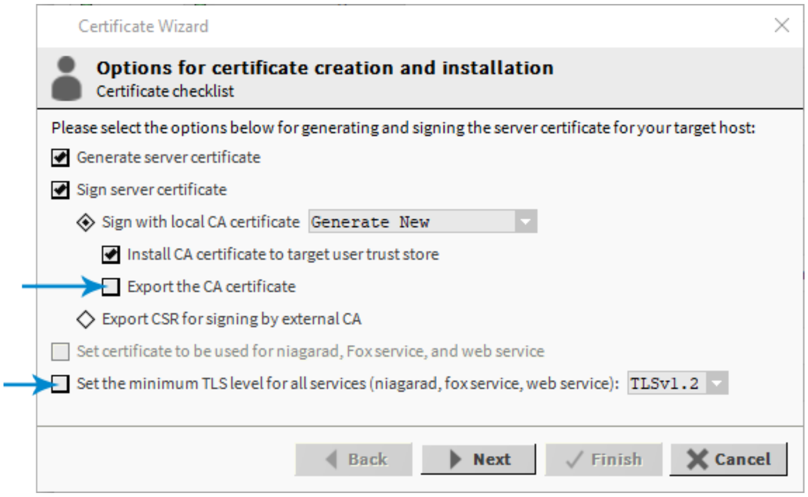
Prerequisites:

You have the required authority to create certificates. You are working in Workbench on a computer that is dedicated to certificate management, is not on the Internet or the company's LAN and is physically secure in a vault or other secure location. You have a thumb drive ready to which to copy the root CA certificate for safe keeping.

Step 1. In Workbench, open a localhost platform connection and in the **Application Director** view click **Stop** to stop any station that is running.

Step 2. In the Nav tree, right-click on the platform and click **Certificate Wizard**.

The **Certificate Wizard** window opens displaying options for certificate creation and installation.



Certificate Wizard

Options for certificate creation and installation
Certificate checklist

Please select the options below for generating and signing the server certificate for your target host:

☑ Generate server certificate

☑ Sign server certificate

◆ Sign with local CA certificate Generate New

☑ Install CA certificate to target user trust store

□ Export the CA certificate

◇ Export CSR for signing by external CA

□ Set certificate to be used for niagarad, Fox service, and web service

□ Set the minimum TLS level for all services (niagarad, fox service, web service): TLSv1.2

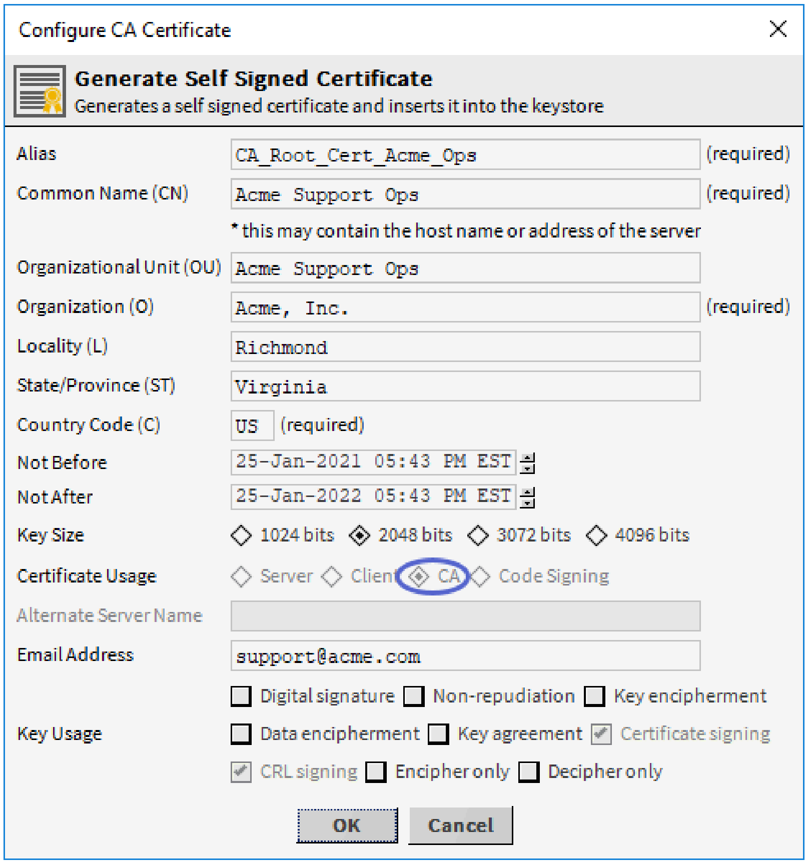
Step 3. In addition to the default selections, configure two optional properties.

- To export the root CA certificate with its private key, click on **Export the CA certificate**. It is a good idea to back up this certificate for archival storage in a secure location.
- To configure the TLS version, **Set minimum TLS level for all services** > **TLSv1.2**.

NOTE:

TLSv1.0 and TLSv1.1 are still supported for backwards compatibility, but it is recommended to use TLSv1.2 and higher.

The **Configure CA Certificate** window opens for you to enter the root CA certificate information.



Configure CA Certificate

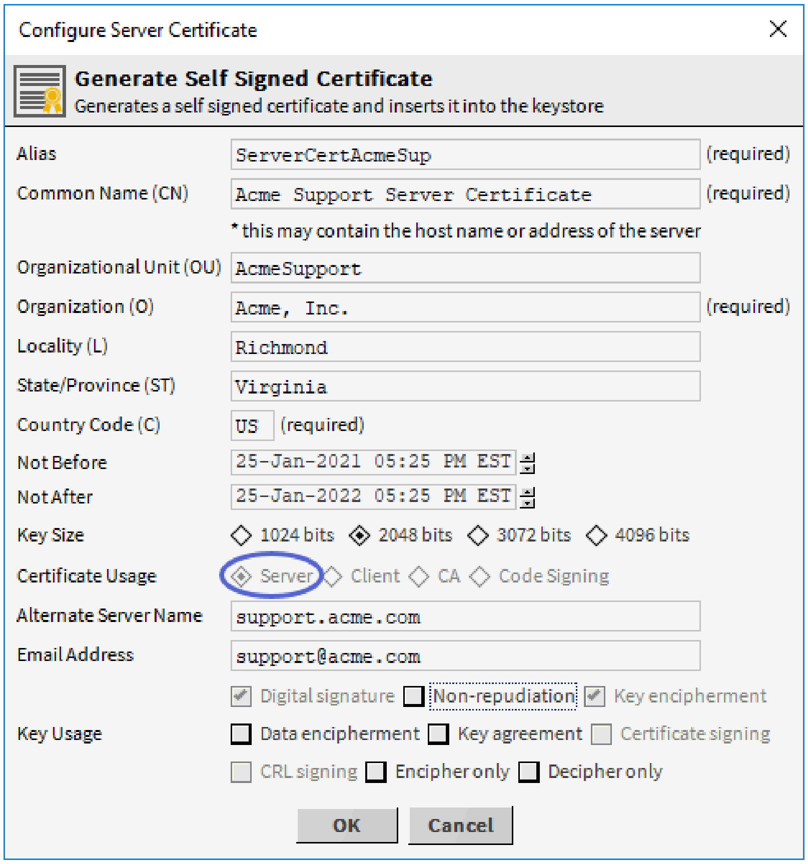
Generate Self Signed Certificate
Generates a self signed certificate and inserts it into the keystore

Alias	CA_Root_Cert_Acme_Ops	(required)
Common Name (CN)	Acme Support Ops	(required)
	* this may contain the host name or address of the server	
Organizational Unit (OU)	Acme Support Ops	
Organization (O)	Acme, Inc.	(required)
Locality (L)	Richmond	
State/Province (ST)	Virginia	
Country Code (C)	US (required)	
Not Before	25-Jan-2021 05:43 PM EST	
Not After	25-Jan-2022 05:43 PM EST	
Key Size	◇ 1024 bits ◈ 2048 bits ◇ 3072 bits ◇ 4096 bits	
Certificate Usage	◇ Server ◇ Client [✓ ◈ CA] ◇ Code Signing	
Alternate Server Name		
Email Address	support@acme.com	
Key Usage	□ Digital signature □ Non-repudiation □ Key encipherment □ Data encipherment □ Key agreement ☑ Certificate signing ☑ CRL signing □ Encipher only □ Decipher only	

Step 4. In the **Configure CA Certificate** window, fill in the form, and click **OK**.

Step 5. When prompted for a **Private Key Password**, enter and confirm a strong password (minimum 10 characters, include at least one of each: a number, lowercase, and uppercase character), and click **OK**. For example, `Private123%`.

The software creates the new root CA certificate in the background. When complete, the wizard opens another **Configure CA Certificate** window. This one is for the server certificate.



Configure Server Certificate

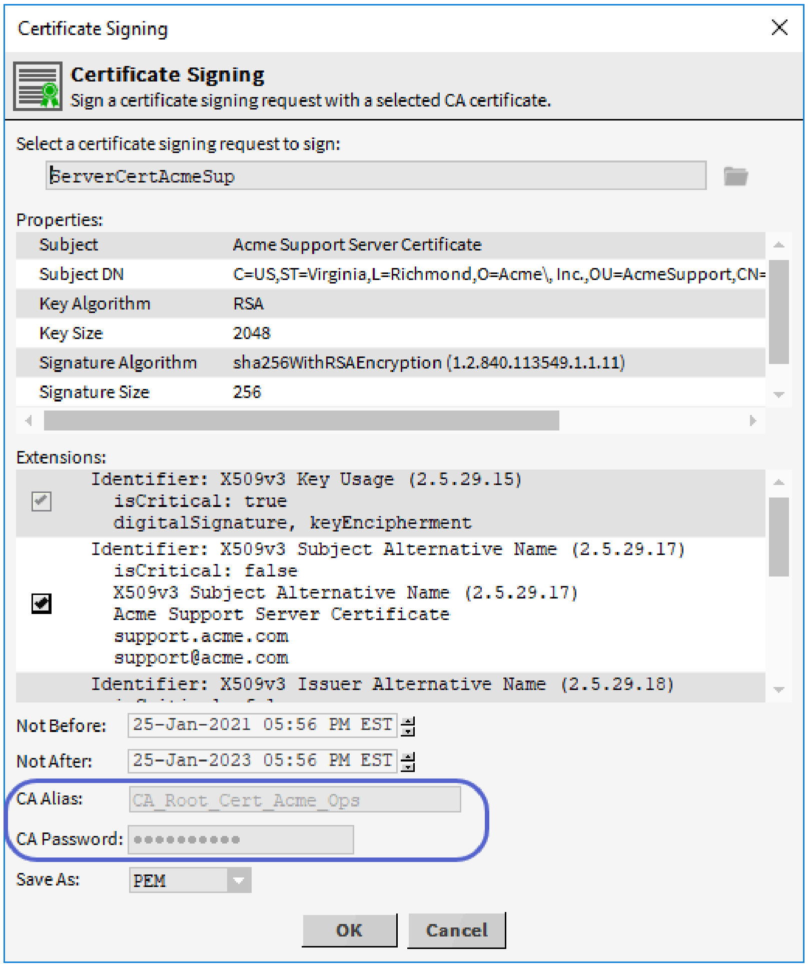
Generate Self Signed Certificate
Generates a self signed certificate and inserts it into the keystore

Alias	ServerCertAcmeSup	(required)
Common Name (CN)	Acme Support Server Certificate	(required)
	* this may contain the host name or address of the server	
Organizational Unit (OU)	AcmeSupport	
Organization (O)	Acme, Inc.	(required)
Locality (L)	Richmond	
State/Province (ST)	Virginia	
Country Code (C)	US (required)	
Not Before	25-Jan-2021 05:25 PM EST	
Not After	25-Jan-2022 05:25 PM EST	
Key Size	◇ 1024 bits ◆ 2048 bits ◇ 3072 bits ◇ 4096 bits	
Certificate Usage	[✓ ◆ Server] ◇ Client ◇ CA ◇ Code Signing	
Alternate Server Name	support.acme.com	
Email Address	support@acme.com	
Key Usage	☑ Digital signature □ Non-repudiation ☑ Key encipherment □ Data encipherment □ Key agreement □ Certificate signing □ CRL signing □ Encipher only □ Decipher only	

Step 6. In the **Configure Server Certificate** window, fill in the form, and click **OK**.

This process generates a server certificate that is ready to be signed. The platform will never be a client, but the station will routinely function as a one, and, since the platform and the station share the same trust store, only one server certificate is required. You will need to run the wizard again when this certificate expires.

Server certificate generation occurs in the background. When complete the wizard opens the **Certificate Signing** window.



Certificate Signing

Certificate Signing

Sign a certificate signing request with a selected CA certificate.

Select a certificate signing request to sign:

ServerCertAcmeSup

Properties:

Subject	Acme Support Server Certificate
Subject DN	C=US,ST=Virginia,L=Richmond,O=Acme\, Inc.,OU=AcmeSupport,CN=
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Size	256

Extensions:

```
☑ Identifier: X509v3 Key Usage (2.5.29.15)
    isCritical: true
    digitalSignature, keyEncipherment
☑ Identifier: X509v3 Subject Alternative Name (2.5.29.17)
    isCritical: false
    X509v3 Subject Alternative Name (2.5.29.17)
    Acme Support Server Certificate
    support.acme.com
    support@acme.com
  Identifier: X509v3 Issuer Alternative Name (2.5.29.18)
```

Not Before: 25-Jan-2021 05:56 PM EST

Not After: 25-Jan-2023 05:56 PM EST

CA Alias: CA_Root_Cert_Acme_Ops

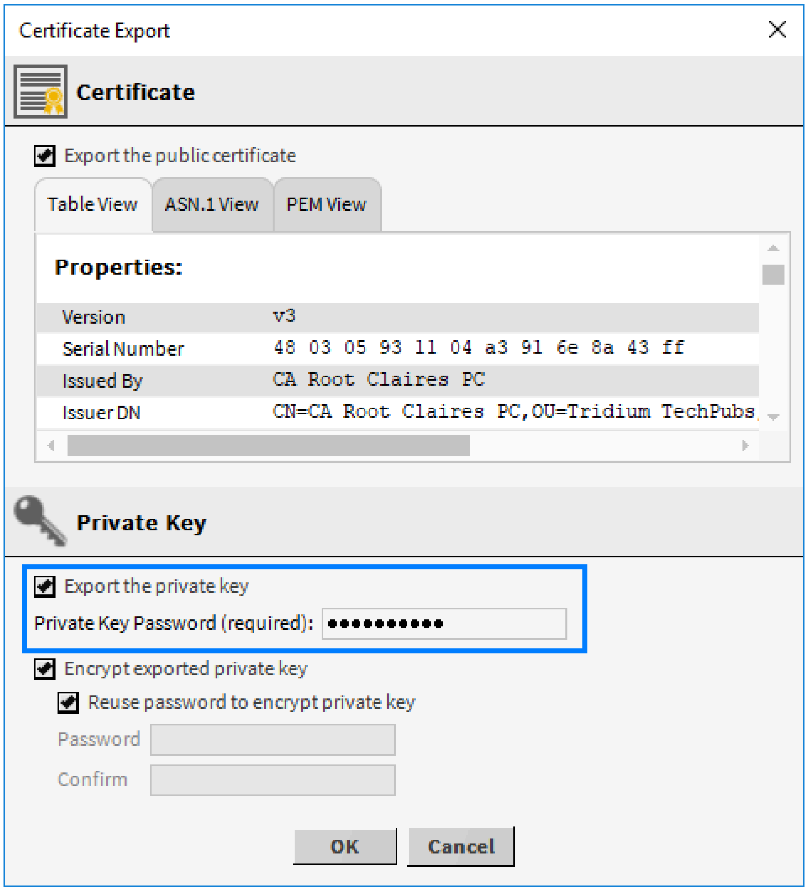
CA Password: ••••••••••

Save As: PEM

NOTE: The server certificate that is about to be signed is already selected. You cannot change the selection. Also, the root CA certificate and the CA password are already identified. There is no need to make other selections or entries.

Step 7. In the **Certificate Signing** window, review the details (similar to the example shown) and click **OK** to continue.

Since we did not choose to export the CSR, the wizard does not display it but proceeds directly to import the signed CSR into the Supervisor station's **User Key Store** and the new root CA certificate into its **User Trust Store**. When complete the wizard opens the **Certificate Export** window.



☑ Export the public certificate

Properties:

Version	v3
Serial Number	48 03 05 93 11 04 a3 91 6e 8a 43 ff
Issued By	CA Root Claires PC
Issuer DN	CN=CA Root Claires PC,OU=Tridium TechPubs,

☑ Export the private key

Private Key Password (required): ●●●●●●●●●●●

☑ Encrypt exported private key

☑ Reuse password to encrypt private key

Password

Confirm

Step 8. In the **Certificate Export** window, in addition to the default selection, click the optional check box: **Export the private key**, enter the private key password, and click **OK**.
By default, the wizard exports the root CA certificate with only its public key. This is appropriate for distributing the root CA certificate, which must be imported to the **User Trust Store** of every platform/station throughout the enterprise, any PC that hosts an instance of the Workbench, and any browser used to monitor and control the system. You export a root CA certificate with its private key only for the purpose of backing it up to a secure location.
The wizard opens the **Certificate Export** window.

Step 9. Use the folder icon to locate the storage location for the exported root CA certificate in the localhost file system, such as an added subfolder in your `certManagement` folder (as shown) or a thumb drive, and click **Save**.
Within the `certManagement` folder, you can create subfolders for storing certificates and certificate signing requests (CSRs). In the above example, the RootCerts folder is a suitable location for the root CA certificate with its public key, while the Vault folder simulates a secure storage location for the root CA certificate with its private key, which should be kept under lock and key.
On completion, the wizard acknowledges that the export was successful.

Step10. To continue, click **OK**.
The **Select Station** window opens.

Step11. In the **Select Station** window, click the drop-down list of all stations in the Platform Daemon Home, and select the station to Set the TLS levels on, and click **OK**.
The wizard displays a progress summary as you complete the various steps.

Step12. When prompted with the message, “All operations are complete”, click **OK** and **Finish**.
The wizard modifies the station’s .bog file in the Platform Daemon Home.

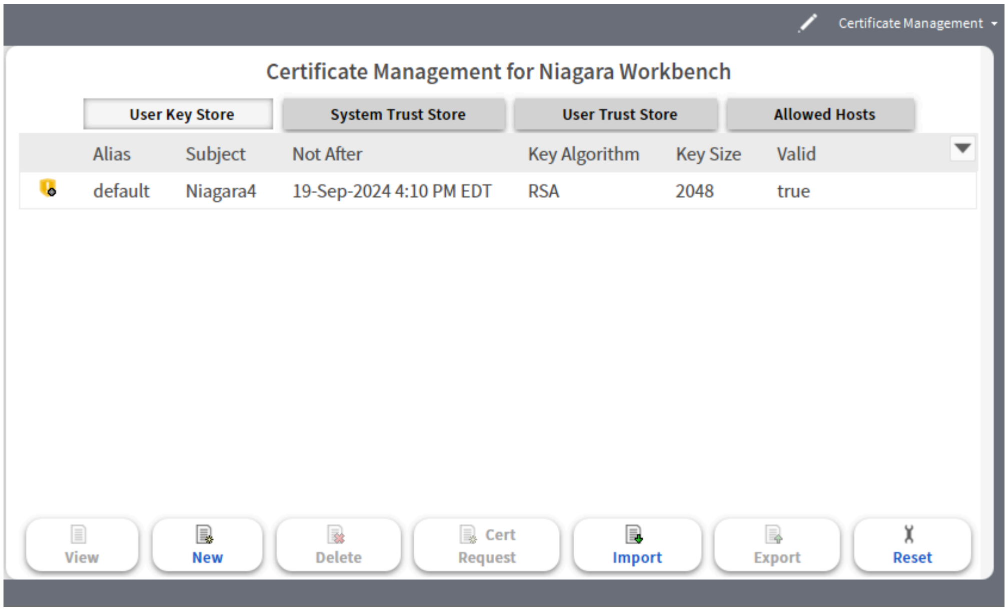
Result
The **Certificate Wizard** successfully generated the new server certificate for the Supervisor PC, and the new root CA certificate for use in signing other server certificates. Those certificates are exported to the certManagment folder in the local file system for subsequent use. Additionally, the wizard set the TLS levels on the selected station to the selected value: TLSv1.2.

Creating a root CA certificate

A company’s root CA certificate is a self-signed certificate. Companies that serve as their own CA use its private key to sign their intermediate, server, client and code-signing certificates. The root CA certificate resides in the Workbench Certificate Management **User Key Store** with both its public and private keys. You export it with only its public key so that you can import it into each platform/station’s **User Trust Store**.

Prerequisites:
You have the required authority to create certificates. You are working in Workbench on a computer that is dedicated to certificate management, is not on the Internet or the company’s LAN and is physically secure in a vault or other secure location.

Step 1. Access the Workbench **Certificate Management** view by clicking **Tools** > **Certificate Management**.
The **Certificate Management** view opens to the **User Key Store**.



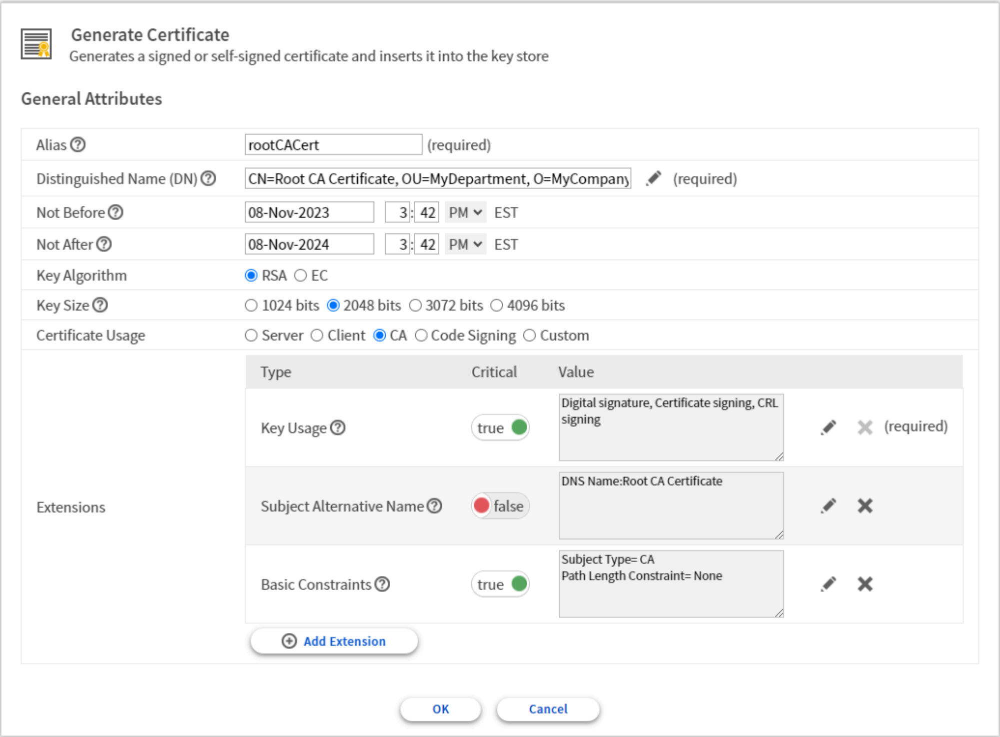
	Alias	Subject	Not After	Key Algorithm	Key Size	Valid
	default	Niagara4	19-Sep-2024 4:10 PM EDT	RSA	2048	true

As of Niagara 4.13, the default `tridium` certificate was replaced by the `default` certificate, which has enhanced features and cannot be deleted. The installation of a new Niagara version will not by default include a `tridium` certificate, but upgrading a system may have both, the `tridium` and the `default` certificate.

Step 2. Confirm that you opened the Workbench **User Key Store** and click the **New** button at the bottom of the view.

NOTE: If you opened the platform/station **Certificate Management** view by mistake, you can still create a root CA certificate, but it will not be available to sign the other certificates.

The **Generate Self Signed Certificate** window opens.



Generate Certificate

Generates a signed or self-signed certificate and inserts it into the key store

General Attributes

Alias	rootCACert (required)
Distinguished Name (DN)	CN=Root CA Certificate, OU=MyDepartment, O=MyCompany (required)
Not Before	08-Nov-2023 3:42 PM EST
Not After	08-Nov-2024 3:42 PM EST
Key Algorithm	● RSA ○ EC
Key Size	○ 1024 bits ● 2048 bits ○ 3072 bits ○ 4096 bits
Certificate Usage	○ Server ○ Client ● CA ○ Code Signing ○ Custom

Extensions

Type	Critical	Value	
Key Usage	true	Digital signature, Certificate signing, CRL signing	(required)
Subject Alternative Name	false	DNS Name:Root CA Certificate	
Basic Constraints	true	Subject Type= CA Path Length Constraint= None	

All certificates begin as self-signed certificates. Only the root CA certificate remains self-signed because it sits at the top of the certificate chain.

Step 3. Fill in the form and click **OK**.

- Use **Alias** to identify this as a root certificate.
- Use the **Distinguished Name (CN)** edit mode to fill in the following information:
  - The **Common Name(CN)** becomes the **Subject** (also known as the Distinguished Name). For a root CA certificate, the **Common Name(CN)** may be the same as the **Alias**.
  - **Organization** should be the name of the company.
  - Although **Locality** and **State/Province** are not required and are arbitrary, leaving them blank generates a warning message.
  - The two-character **Country Code** is required and must be a known value, such as: US, IN, CA, FR, DE, ES, etc. (refer to the ISO CODE column at countrycode.org).
- Based on the **Not Before** and **Not After** dates, certificate validity defaults to a year. A longer period is not recommended and not tolerated by some browsers. Changing to a new certificate annually or even within a year makes it more likely that your certificate contains the latest cryptographic standards, and reduces the number of old, neglected certificates that can be stolen and re-used for phishing and drive-by malware attacks.
- **Key Size** defaults to 2048. A larger key improves security and does not significantly affect communication time. The only impact it has is to lengthen the time it takes to create the certificate initially.
- For **Certificate Usage**, select CA.
- The HTML5 **Generate Certificate** window allows you to add extensions, which specify information such as alternative subject names and usage restrictions to certificates.
  - *Key Usage*: defines the purpose (for example, encipherment, signature, certificate signing) of the key contained in the certificate. You can use it to restrict the usage of a certificate's key only to permitted operations. For example, a key that should only be used for key management should have the keyEncipherment bit set.
  - *Subject Alternative Name*: allows identities to be bound to the subject of the certificate. Defined options include an Internet electronic mail address, a DNS name, an IP address, and a Uniform Resource Identifier (URI).
  - *Extended Key Usage*: indicates one or more purposes for which the certificate may be used in addition to or in place of the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates. You can create a custom key usage extension that must be an OID with numbers separated by decimals (for example, 1.2.3).

The **Private Key Password** window opens.

Step 4. Enter and confirm a strong password, and click **OK**.
The system informs you that the certificate has been submitted. Soon the certificate appears behind the Info message in the User Key Store table.

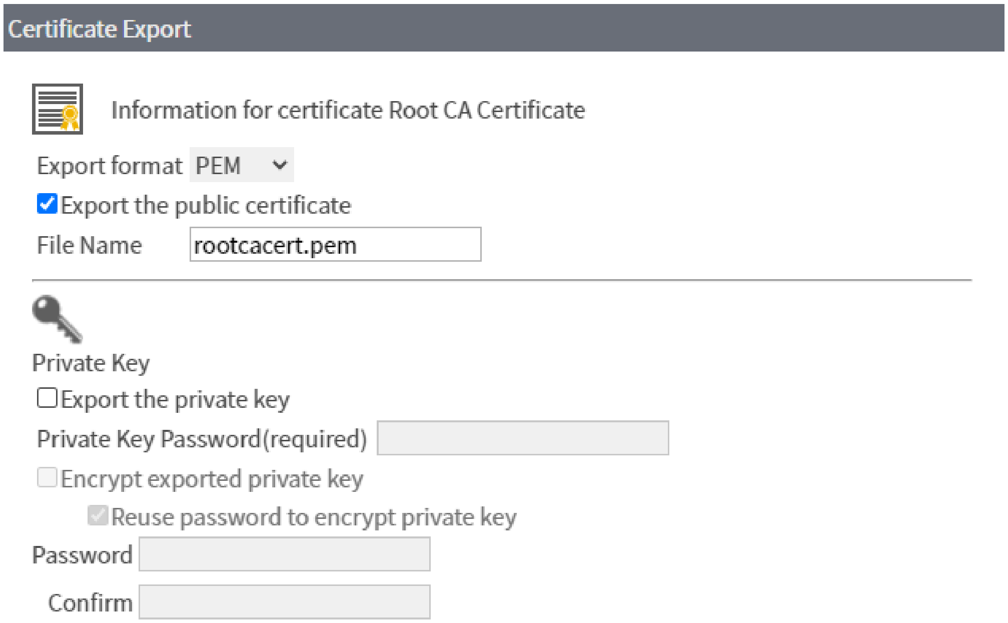
Step 5. To continue, click **OK**.
The root CA certificate now exists with both its keys in the Workbench **User Key Store**. From this location you can use it to sign other certificates (intermediate, server, client and code-signing).

NOTE: The exclamation icon (❗) indicates that the certificate is not signed by a Certificate Authority. For a server, client, or code signing certificate, it means that the certificate will not be trusted by other parties. For a root CA, which itself is the source of trust, this is normal and expected.

For this certificate to authenticate the certificates it signs, you now need to export it with only its public key and import it into the **User Trust Store** of each client computer and platform/station.

Step 6. Select the new root CA certificate and click **Export**.

The **Certificate Export** window opens.



Certificate Export

Information for certificate Root CA Certificate

Export format PEM

☑ Export the public certificate

File Name rootcacert.pem

Private Key

☐ Export the private key

Private Key Password(required)

☐ Encrypt exported private key

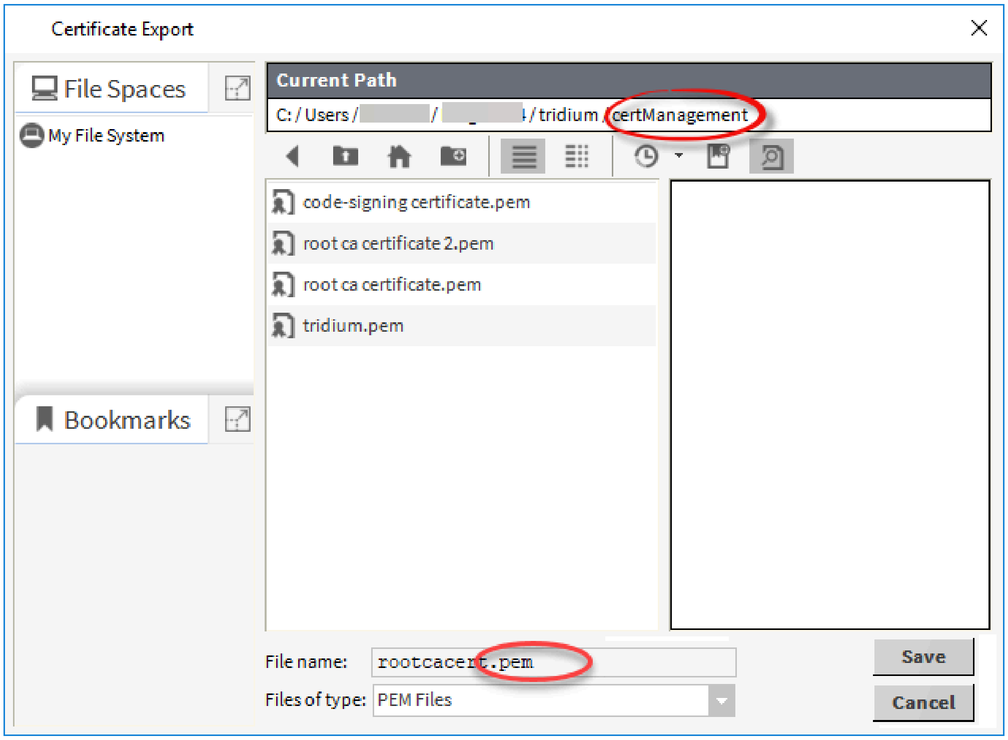
☑ Reuse password to encrypt private key

Password

Confirm

CAUTION: Do not click the check box to **`Export the private key`**.The only time you click this check box is when you are backing up the certificate to another location for safe keeping.

Step 7. To create the root CA certificate that will reside in each client's **User Trust Store**, click **OK**.
The Certificate Export window opens with the file ready to export as a .pem file.



Certificate Export

Current Path

C: / Users / [redacted] / [redacted] / tridium / certManagement

code-signing certificate.pem
root ca certificate 2.pem
root ca certificate.pem
tridium.pem

File name: rootcacert.pem

Files of type: PEM Files

Notice the Current Path. This is where the system stores the exported certificate.

Step 8. Navigate to a `rootcert` folder or location on a thumb drive, and click **Save**.
The system reports that it exported the certificate successfully.

Step 9. To complete the export, click **OK**.

Next steps
When exported with only its public key, the root CA certificate may be freely distributed. You are ready to manually import the root CA certificate with only its public key into the **User Trust Store** of the computer, usually a Supervisor (or engineering) computer, from which to either manually, or with a provisioning job, install this certificate in the **User Trust Store** of all remote platforms/stations.

Creating a server certificate and CSR (Certificate Signing Request)

This procedure creates a server certificate and its CSR. These are the first steps in getting the server certificate signed.

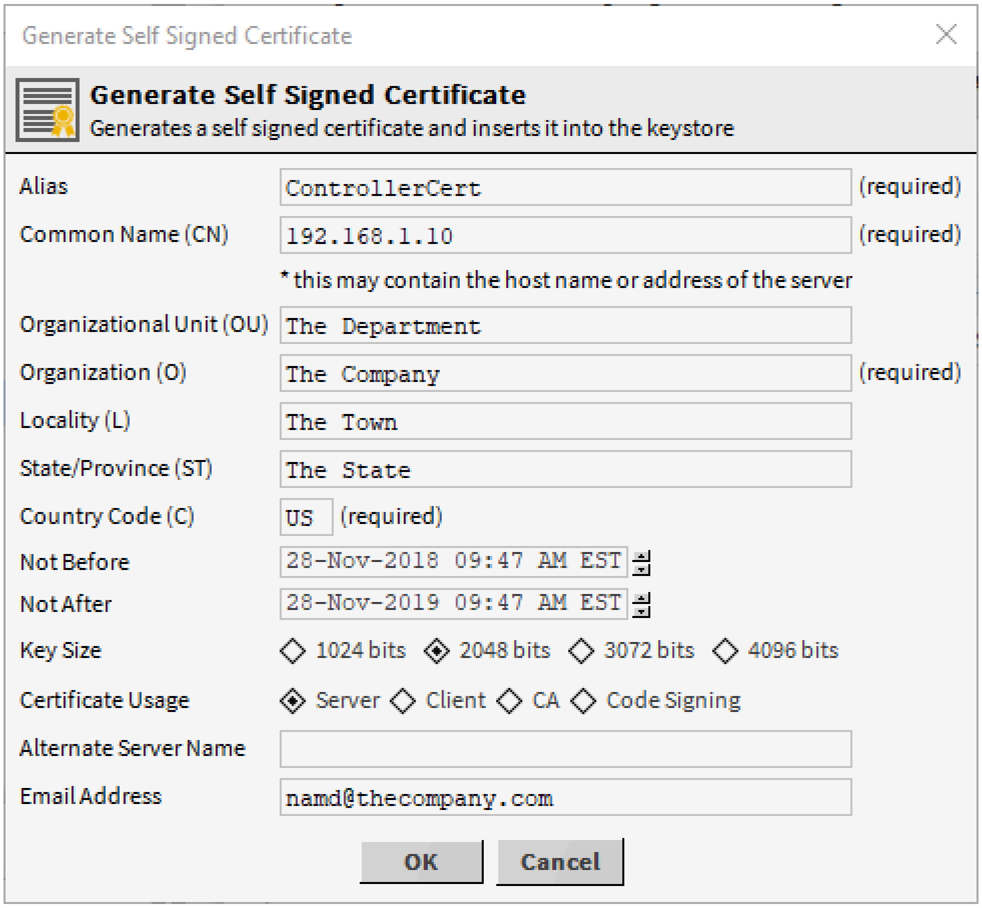
Prerequisites:
You are working in Workbench on a PC (Supervisor or otherwise) and are able to connect to all controllers.

Step 1. Open the Certificate Management view for your localhost or a controller by right-clicking **Platform** > **Views** > **Certificate Management**. If required to connect to the platform, enter the platform credentials, and click **OK**.
The view opens with the focus on the User Key Store.

Step 2. Confirm that you are viewing the correct Certificate Management stores.

Step 3. Click **New**.

A blank **Generate Self Signed Certificate** window opens.



Generate Self Signed Certificate

Generate Self Signed Certificate

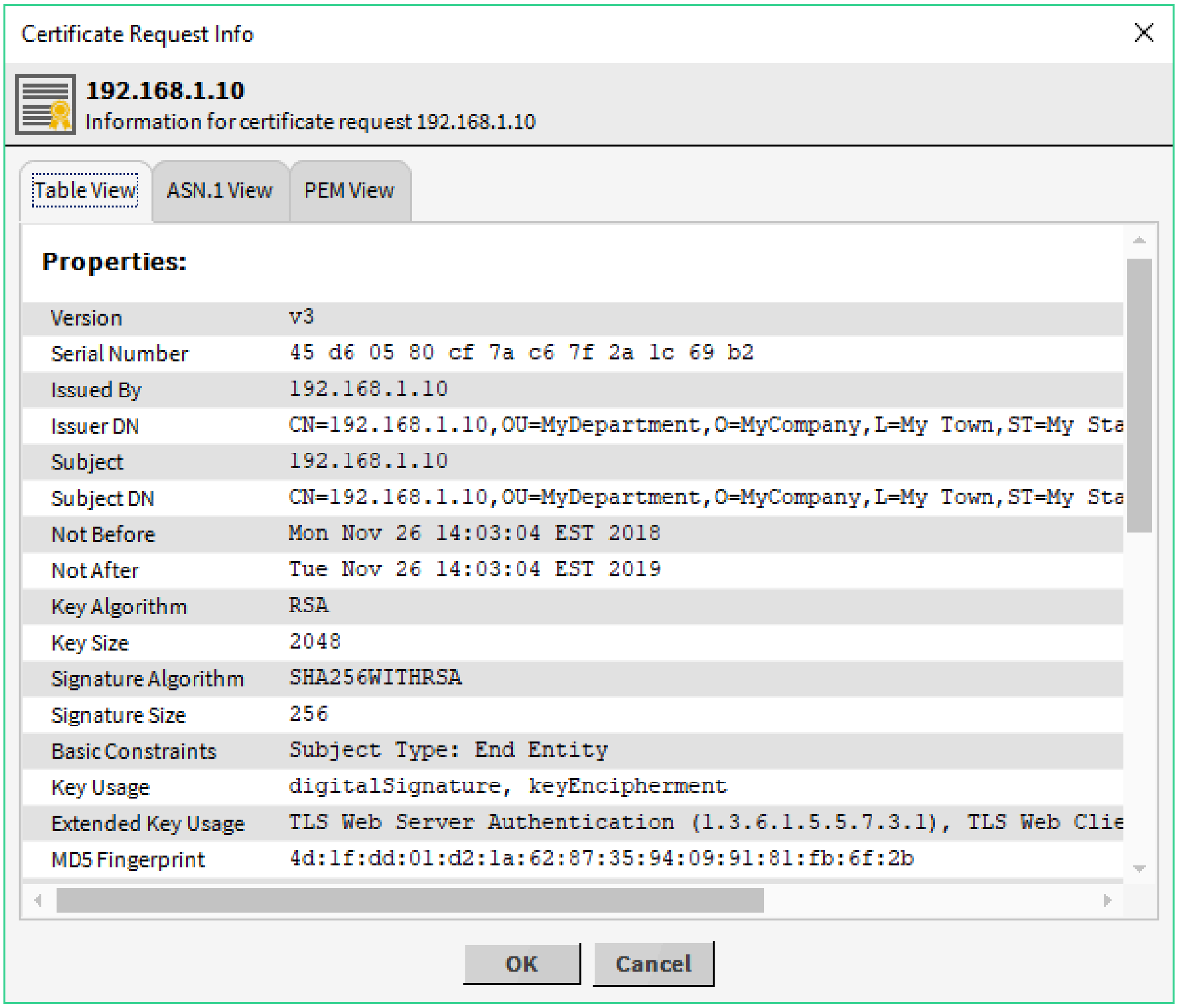
Generates a self signed certificate and inserts it into the keystore

Alias	ControllerCert	(required)
Common Name (CN)	192.168.1.10	(required)
	* this may contain the host name or address of the server	
Organizational Unit (OU)	The Department	
Organization (O)	The Company	(required)
Locality (L)	The Town	
State/Province (ST)	The State	
Country Code (C)	US (required)	
Not Before	28-Nov-2018 09:47 AM EST	
Not After	28-Nov-2019 09:47 AM EST	
Key Size	○ 1024 bits ● 2048 bits ○ 3072 bits ○ 4096 bits	
Certificate Usage	● Server ○ Client ○ CA ○ Code Signing	
Alternate Server Name		
Email Address	namd@thecompany.com	

Step 4. Fill in the form with information for the current platform/station and click **OK**.
Alias identifies the type of certificate and purpose in words. The **Common Name** should be the IP address or domain name of the platform/station. **Organization** is the name of the company. Define **Locality**, **State/Province**, and two-digit **Country Code**. Leave **Certificate Usage** set at the default (Server), and provide an **Email Aeddress**. The rest of the properties can remain at their default values.
After a bit, the system creates a self-signed server certificate, which appears in the User Key Store table with a yellow shield.

Step 5. Select the new server certificate and click **Cert Request**.

The **Certificate Request Info** window opens for the server certificate.



192.168.1.10

Information for certificate request 192.168.1.10

Properties:

Version	v3
Serial Number	45 d6 05 80 cf 7a c6 7f 2a 1c 69 b2
Issued By	192.168.1.10
Issuer DN	CN=192.168.1.10,OU=MyDepartment,O=MyCompany,L=My Town,ST=My Sta
Subject	192.168.1.10
Subject DN	CN=192.168.1.10,OU=MyDepartment,O=MyCompany,L=My Town,ST=My Sta
Not Before	Mon Nov 26 14:03:04 EST 2018
Not After	Tue Nov 26 14:03:04 EST 2019
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	SHA256WITHRSA
Signature Size	256
Basic Constraints	Subject Type: End Entity
Key Usage	digitalSignature, keyEncipherment
Extended Key Usage	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1), TLS Web Clie
MD5 Fingerprint	4d:1f:dd:01:d2:1a:62:87:35:94:09:91:81:fb:6f:2b

Step 6. Confirm that the **Issued By** and **Subject** fields contain the expected IP address (or domain name) and click **OK**.
The **Choose Export Directory** window opens.

Step 7. Navigate to the `serverCSRs` folder you created (**My Host** > **My File System** > **User Home** > **certManagement** > **serverCSRs**), and click **Save**.
You now have a self-signed server certificate in the platform/station User Trust Store and a certificate signing request for that certificate in the `certManagement\serverCSRs` folder.

Step 8. If you are using an external CA, email the certificate request to the external CA, and wait for it to returned signed.

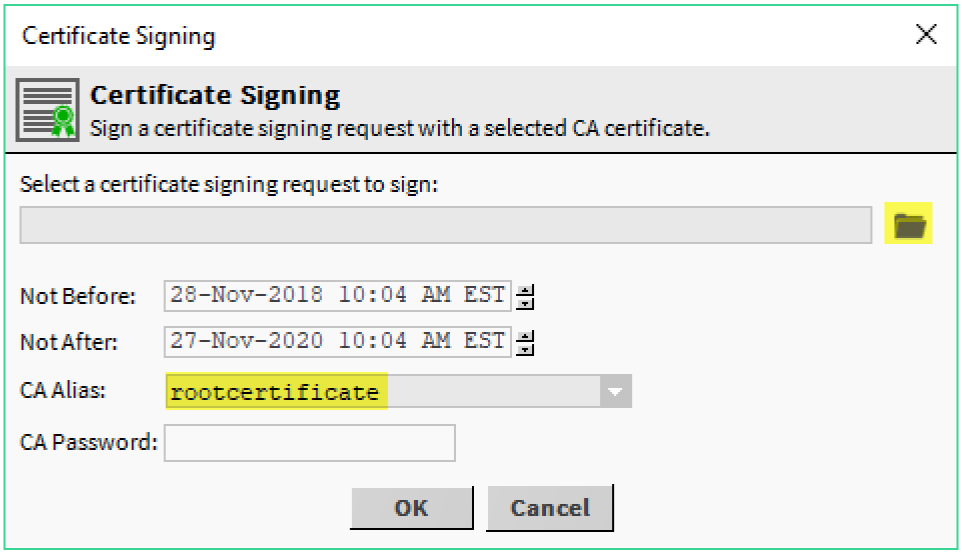
Signing a server certificate

Signing a certificate is a simple procedure. Certificates look a lot alike. The Certificate Management stores look a lot alike Follow the procedure carefully confirming at each step that you are working in the correct stores with the correct root and server certificate

Prerequisites:
You are working in Workbench on the PC (Supervisor or otherwise) that you used to create the root certificate.

Step 1. Click **Tools** > **Certificate Signer Tool**.

The Certificate Signing window opens.



Certificate Signing

Certificate Signing

Sign a certificate signing request with a selected CA certificate.

Select a certificate signing request to sign:

Not Before: 28-Nov-2018 10:04 AM EST

Not After: 27-Nov-2020 10:04 AM EST

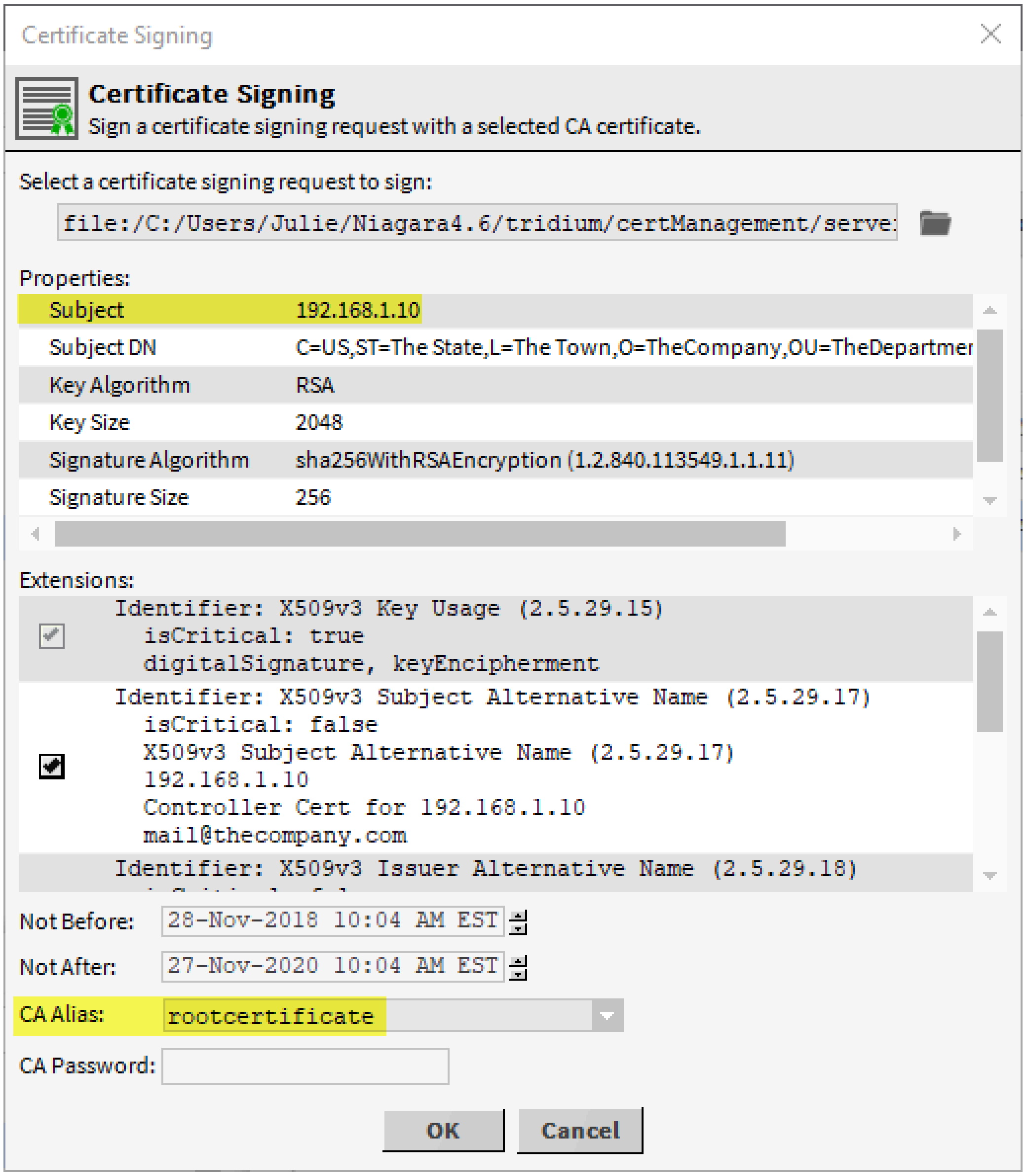
CA Alias: rootcertificate

CA Password:

Notice that the **`CA Alias`** identifies the root certificate.

Step 2. Click the folder icon to the right of **`Select a certificate signing request to sign:`**, navigate to the `serverCSRs` folder you created (**My Host** > **My File System** > **User Home** > **certManagement** > **serverCSRs**), click the server CSR, and click **Open**.

the Certificate Signing window for the server certificate opens.



Certificate Signing

Certificate Signing

Sign a certificate signing request with a selected CA certificate.

Select a certificate signing request to sign:

```
file:/C:/Users/Julie/Niagara4.6/tridium/certManagement/serve
```

Properties:

Subject	192.168.1.10
Subject DN	C=US,ST=The State,L=The Town,O=TheCompany,OU=TheDepartmer
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Size	256

Extensions:

```
☑ Identifier: X509v3 Key Usage (2.5.29.15)
    isCritical: true
    digitalSignature, keyEncipherment
☑ Identifier: X509v3 Subject Alternative Name (2.5.29.17)
    isCritical: false
    X509v3 Subject Alternative Name (2.5.29.17)
    192.168.1.10
    Controller Cert for 192.168.1.10
    mail@thecompany.com
  Identifier: X509v3 Issuer Alternative Name (2.5.29.18)
```

Not Before: 28-Nov-2018 10:04 AM EST

Not After: 27-Nov-2020 10:04 AM EST

CA Alias: rootcertificate

CA Password:

Step 3. Verify that the **Subject** identifies the expected platform/station IP address or domain name and that the **CA Alias** identifies the root certificate.

Step 4. To sign the certificate, enter the root certificate's **CA Password** and click OK.
The `certManagement` folder opens.

Step 5. Double-click the `signedCSRs` folder and click Save.

Result

You now have a signed server certificate request.

Matching a server certificate with its signed CSR

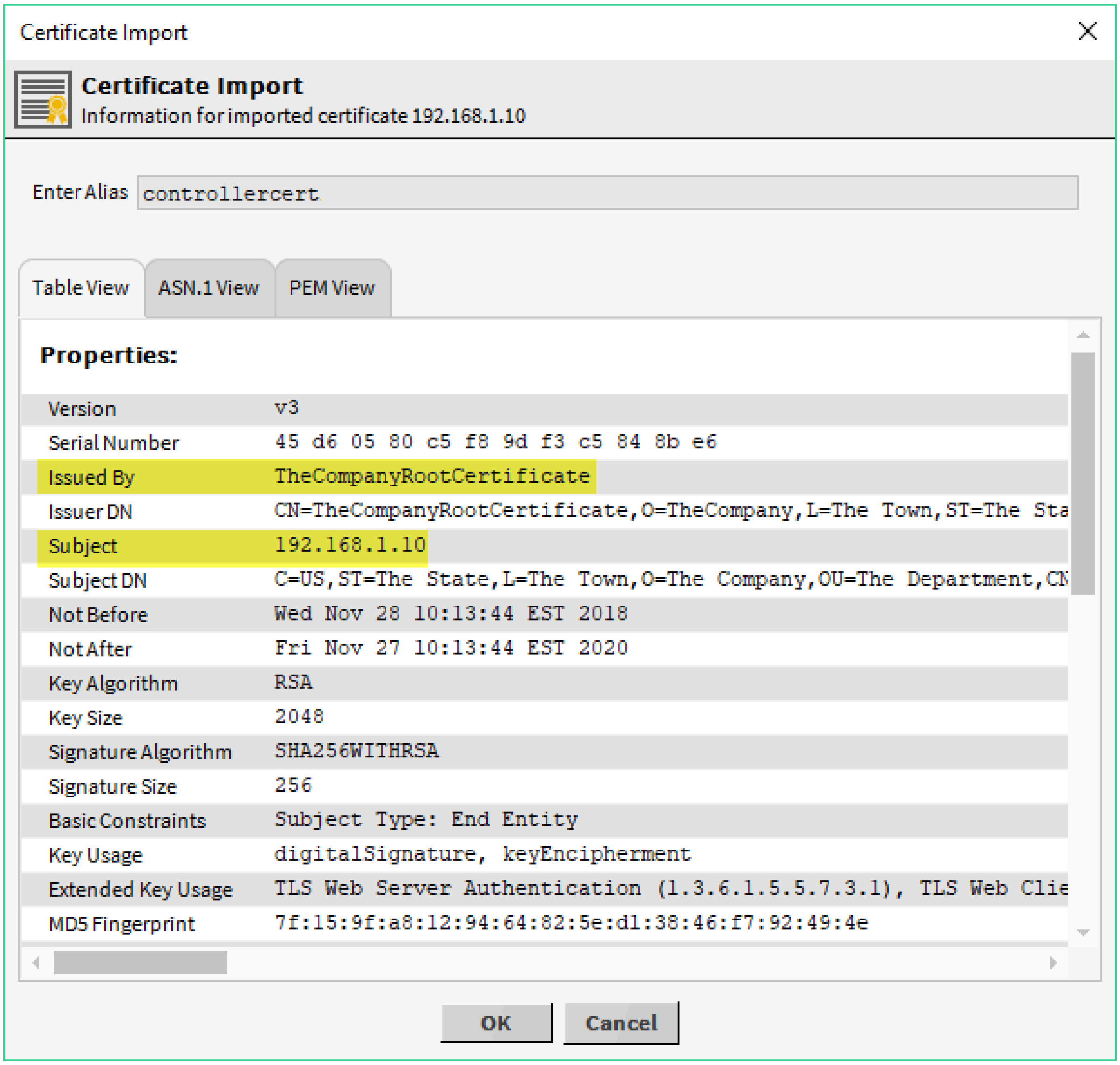
You now import the signed CSR into the User Key Store where it updates the original server certificate you created.

Prerequisites:
You are working in Workbench on a PC (Supervisor or otherwise).

Step 1. Open the Certificate Management view for your localhost or a controller by right-clicking **Platform** > **Views** > **Certificate Management**. If required to connect to the platform, enter the platform credentials, and click **OK**.
The view opens with the focus on the User Key Store.

Step 2. Select the original server certificate and click **Import**.

Step 3. Navigate to the `signedCSRs` folder, select the signed CSR (.pem file), and click **Open**.
the **Certificate Import** window opens.



Enter Alias: controllercert

Properties:

Version	v3
Serial Number	45 d6 05 80 c5 f8 9d f3 c5 84 8b e6
Issued By	TheCompanyRootCertificate
Issuer DN	CN=TheCompanyRootCertificate,O=TheCompany,L=The Town,ST=The Sta
Subject	192.168.1.10
Subject DN	C=US,ST=The State,L=The Town,O=The Company,OU=The Department,CN
Not Before	Wed Nov 28 10:13:44 EST 2018
Not After	Fri Nov 27 10:13:44 EST 2020
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	SHA256WITHRSA
Signature Size	256
Basic Constraints	Subject Type: End Entity
Key Usage	digitalSignature, keyEncipherment
Extended Key Usage	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1), TLS Web Clie
MD5 Fingerprint	7f:15:9f:a8:12:94:64:82:5e:d1:38:46:f7:92:49:4e

Step 4. Confirm that this is no longer a self-signed certificate and click **OK**.
The **Issued By** field contains the name of the root CA certificate. The **Subject** contains the IP address or domain name.
The yellow shield with the exclamation mark changes to a green shield with a check mark.

Result
The platform/station now is not ready to connect to a client presenting its own CA-signed certificate.

Changing TLS settings

Change TLS Settings is a utility under Platform Administration. This utility configures secure communication including defining the server certificate to use for the platform.

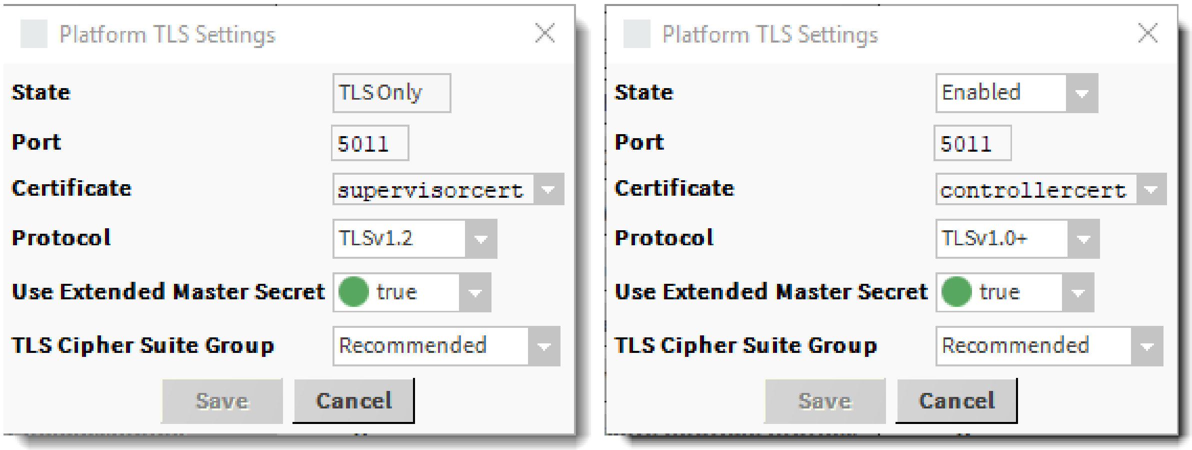
Prerequisites:
You are working in Workbench and can connect to your localhost as well as to each controller.

The server certificate defaults to the self-signed `default` certificate. Before you can make secure connections, you need to change this certificate to the server certificate that you created. You need to do this for the localhost and for each controller on the network.

Step 1. Open a secure platform connection to the controller (port 5011).

Step 2. Double-click the Platform Administration utility.
The **Platform Administration** view opens.

Step 3. Click the **Change TLS Settings** button.
The **Platform TLS Settings** window opens.



	Platform TLS Settings	Platform TLS Settings
State	TLS Only	Enabled
Port	5011	5011
Certificate	supervisorcert	controllercert
Protocol	TLSv1.2	TLSv1.0+
Use Extended Master Secret	● true	● true
TLS Cipher Suite Group	Recommended	Recommended

The window on the left is for the localhost, and that on the right is for a controller.

Step 4. Confirm that:

- **State** is `TLS Only`.
- **Port** is `5011`
- **Certificate** is the server certificate you created for each platform/station.
- The rest of the properties are configured at their defaults.

Importing the root certificate into a platform/station User Trust Store

When serving as your own CA, each client requires the root certificate with its public key in its User Trust Store. If your server certificates are signed by an external CA, its root certificate and public key should already be in the platform/station's System Trust Store

Prerequisites:
You are working in Workbench running on a PC.

Step 1. To open the Certificate Management view for the platform/station, expand **Platform** and double-click Certificate Management.

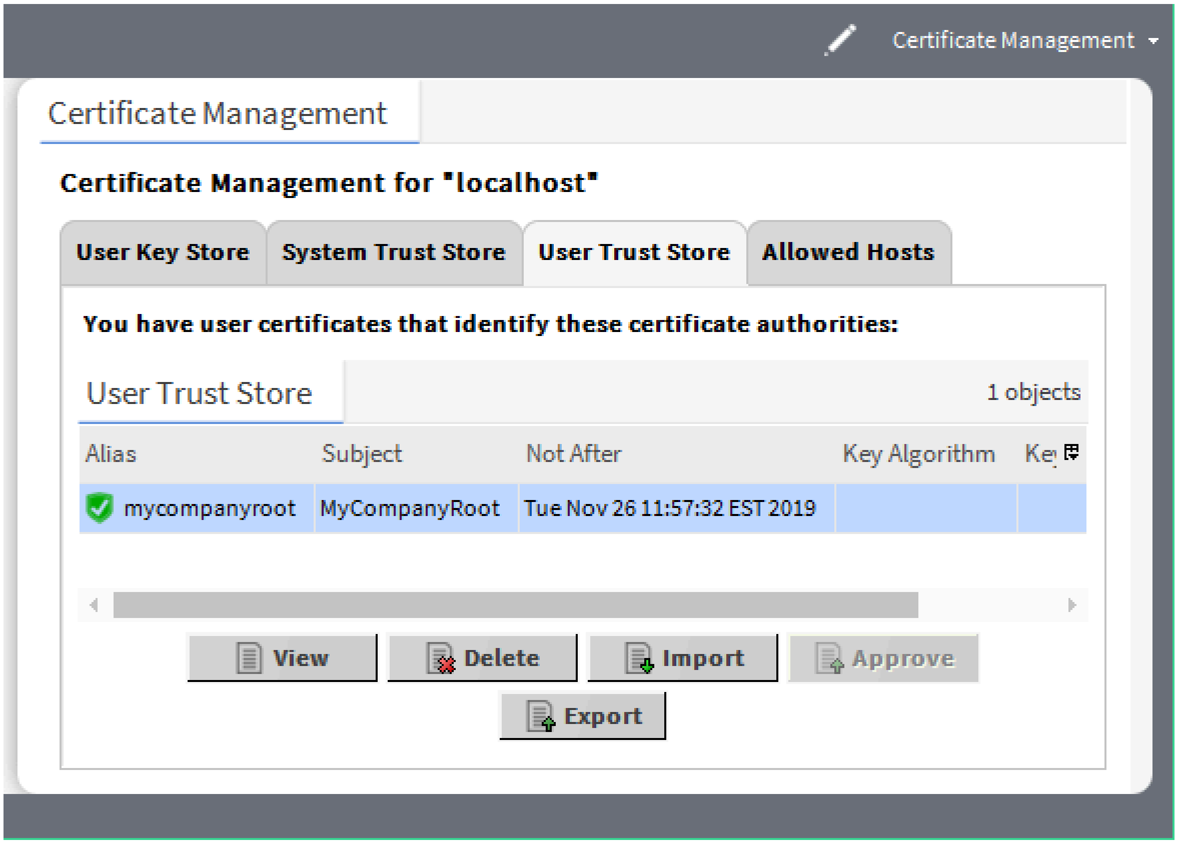
The Certificate Management view opens to the User Key Store tab.

Step 2. Click the User Trust Store tab.

Step 3. Click **Import**.

Step 4. Locate and select the root certificate's .pem file (**My Host** > **My File System** > **User Home** > **certManagement** > **rootcert**, and click **Open**.

Step 5. Confirm that you are importing the correct root certificate (in this chapter it is the only root certificate), and click **OK**.
The system imports the root certificate.



Certificate Management for "localhost"

You have user certificates that identify these certificate authorities:

Alias	Subject	Not After	Key Algorithm	Ke
✓ mycompanyroot	MyCompanyRoot	Tue Nov 26 11:57:32 EST 2019		

The green shield with the check mark indicates that your company's root certificate with its public key is in the client User Trust Store, ready to verify the identify of the server certificates signed by its private key.

Result
Your platform/station is ready to function as a client. Using this certificate it verifies that the server certificates presented to it are valid if, and only if, they were signed by this certificate's private key.

NOTE: You need to do this for the Supervisor platform/station as well as for each controller platform/station.

Importing the root certificate into the Workbench User Trust Store

When serving as your own CA, each client requires the root certificate with its public key in its User Trust Store. If your server certificates are signed by an external CA, its root certificate and public key should already be in the platform/station's System Trust Store.

Prerequisites:
You are working in Workbench running on a PC.

Step 1. To open the Certificate Management view, click **Tools** > **Certificate Management**.
The Workbench Certificate Management view opens to the User Key Store.

Step 2. Click the User Trust Store tab.

Step 3. Click **Import**.

Step 4. Locate and select the root certificate's .pem file (**My Host** > **My File System** > **User Home** > **certManagement** > **rootcert**, and click **Open**.

Step 5. Confirm that you are importing the correct root certificate (in this chapter it is the only root certificate), and click **OK**.
The system imports the root certificate.

The green shield with the check mark indicates that your company's root certificate with its public key is in the client User Trust Store, ready to verify the identify of the server certificates signed by its private key.

Result

Workbench is ready to function as a client. Using this certificate it verifies that the server certificates presented to it are valid if, and only if, they were signed by this certificate's private key.

Installing a root certificate in the Windows trust store

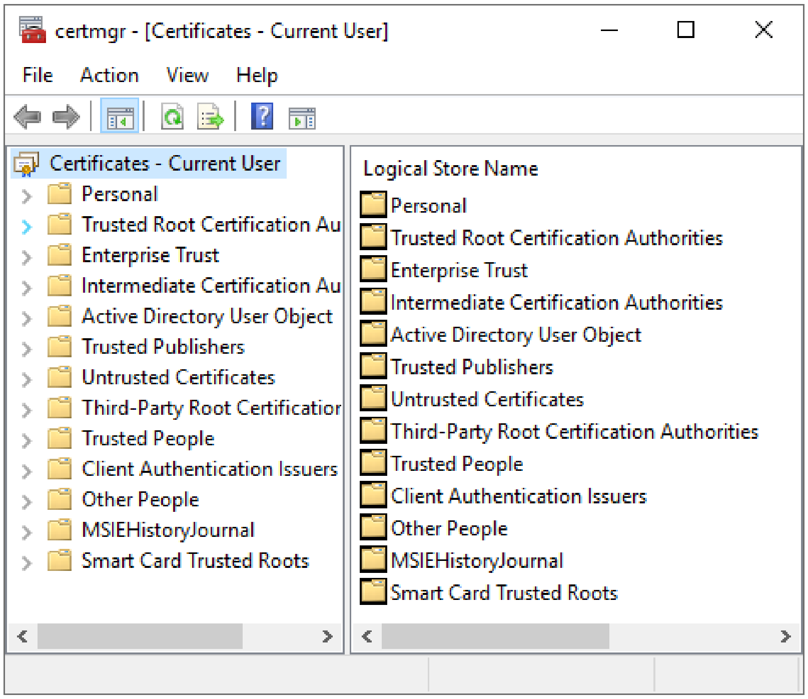
For communication to be secure when accessing a station using the web UI, a company's root certificate must be imported into the Windows trust store.

Prerequisites:

Using Workbench, you exported the root certificate into a directory you can access from the PC. (The extension for a root certificate file name is .pem).

Step 1. On the PC, open a Windows command prompt by clicking **Start** and typing `cmd` .
The **Command Prompt** window opens.

Step 2. Type `certmgr.msc` and press **Enter**.
The certificate manager window opens.



Certificates - Current User
- Personal
- Trusted Root Certification Au
- Enterprise Trust
- Intermediate Certification Au
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certificatior
- Trusted People
- Client Authentication Issuers
- Other People
- MSIEHistoryJournal
- Smart Card Trusted Roots

Logical Store Name
- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Client Authentication Issuers
- Other People
- MSIEHistoryJournal
- Smart Card Trusted Roots

Step 3. In the column to the right, right-click the **Trusted Root Certificate Authorities** folder and click **All Tasks** > **Import**.
the Certificate Import wizard window opens.

Step 4. Follow the steps of the wizard to browse to the User Home where the root certificate .pem file is located, select to view All Files..., select the file and click **Open**.

Step 5. Finish the wizard.

Importing the root certificate into the Java Control Panel

Importing the root certificate into the JAVA Control Panel is necessary to use Java WebStart. Disclaimer: this software may function differently from what is described here.

Prerequisites:
You are working in Windows on a PC. Your root certificate is available either in the User Home folder or on a thumb drive.

Step 1. Click the Windows Start button and open the Windows Control Panel.

Step 2. In the All Control Panel Items list, double-click Java.
The Java Control Panel opens.

Step 3. Select the Security tab, and click **Manage Certificates** (lower-right).

Step 4. If necessary, select `Trusted Certificates` from the drop-down list.

Step 5. To add the new root certificate, click **Import**, navigate to the root certificate, select it, and click Open.
The certificate appears in the list.

Step 6. To complete the import, click **Close** and **OK**.

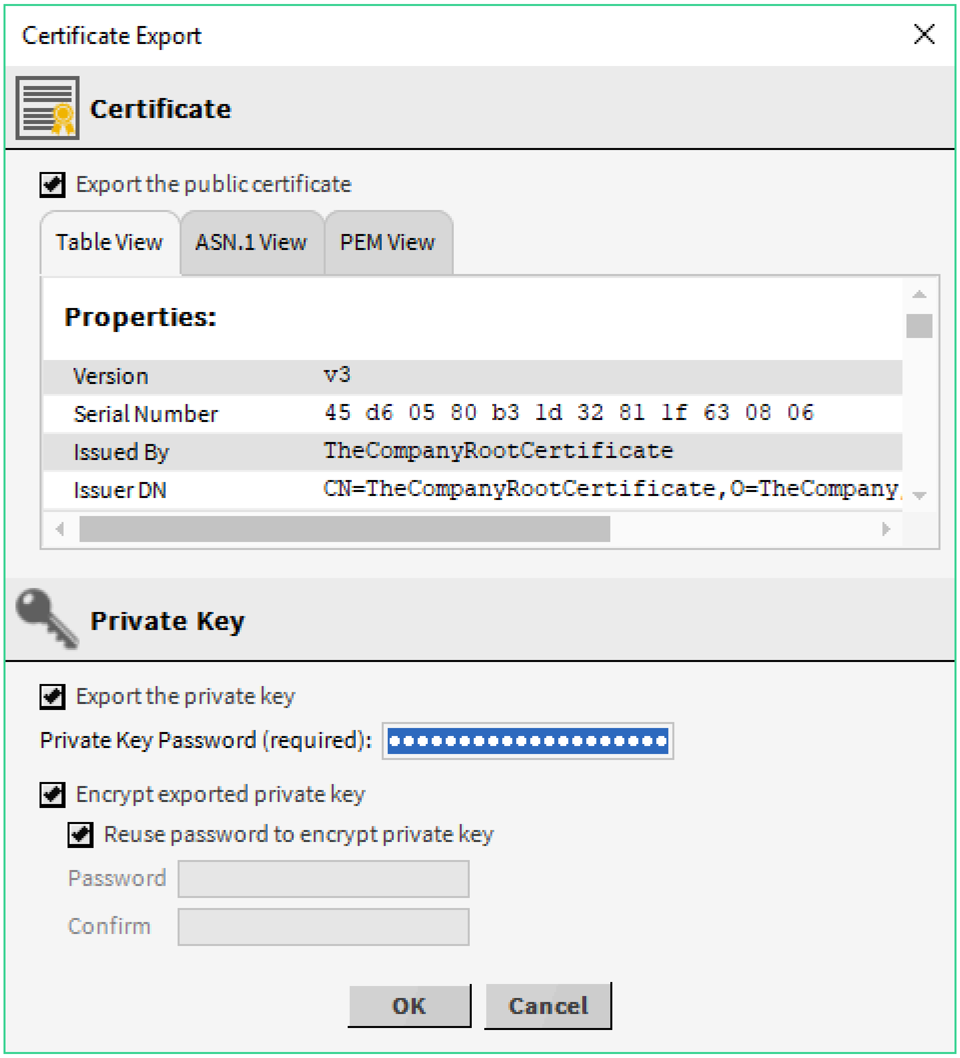
Exporting to back up certificates

Once all certificates are in place, it is a good idea to back up all certificates to a thumb drive or other storage device, such as a completely separate computer that resides in a vault.

Prerequisites:
You are working in Workbench on the PC that you used to set up certificates.

Step 1. Open the Workbench Certificate Management view by clicking **Tools** > **Certificate Management**, in the User Key Store, select the company's root certificate and click **Export**.

The **Certificate Export** window opens.



Certificate

☑ Export the public certificate

Properties:

Version	v3
Serial Number	45 d6 05 80 b3 1d 32 81 1f 63 08 06
Issued By	TheCompanyRootCertificate
Issuer DN	CN=TheCompanyRootCertificate,O=TheCompany,

Private Key

☑ Export the private key

Private Key Password (required): ••••••••••••••••••••

☑ Encrypt exported private key

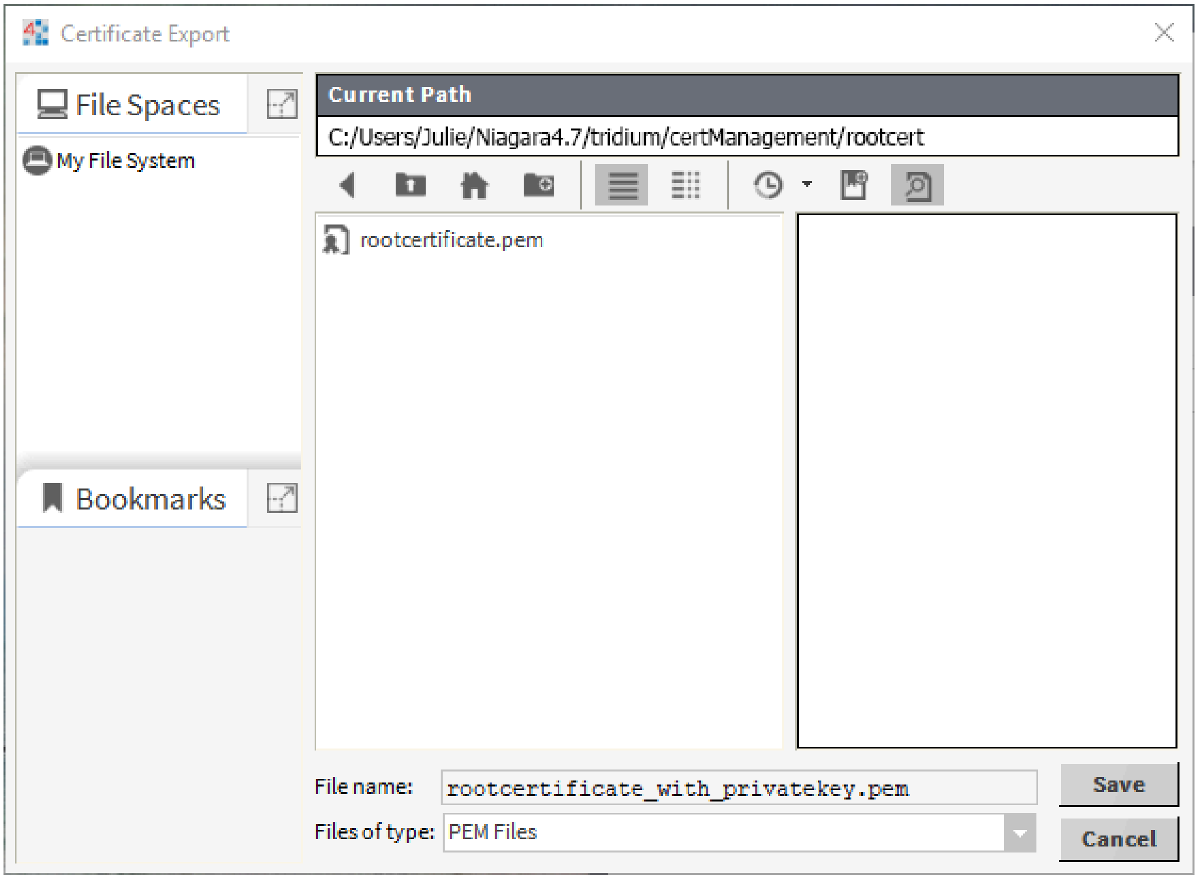
☑ Reuse password to encrypt private key

Password

Confirm

Step 2. Click the option to **Export** the certificate's private key.

Step 3. Create a strong password to protect this private key and click **OK**.



C:/Users/Julie/Niagara4.7/tridium/certManagement/rootcert

rootcertificate.pem

File name: `rootcertificate_with_privatekey.pem`

Files of type: PEM Files

The **Export Certificate** file path window opens.

Step 4. Add to the name text to indicate that this file contains the private key, navigate to the `rootcert` folder, and click **Save**.

Step 5. Create a new folder under `certManagement` called `servercerts`.

Step 6. Navigate to each controller/station Certificate Management folder and save each server certificate with its private key in the new **My File System** > **User Home** > **certManagement** > **servercerts** folder.

Step 7. Using Windows' File Explorer, copy the entire `certManagement` folder to a thumb drive or other location.

Step 8. Delete the contents of the `certManagement` folder.

DANGER: DO NOT LEAVE A ROOT CERTIFICATE OR SERVER CERTIFICATES WITH THEIR PRIVATE KEYS IN A PC FILE SYSTEM THAT MAY BE COMPROMISED! STORE THESE CERTIFICATES ONLY ON A THUMB DRIVE OR PC THAT IS IN A SECURE AND LOCKED VAULT. AS A BEST PRACTICE, AVOID STORING CERTIFICATES IN THE CLOUD.

Result

If you followed these procedures, the company's communication within this system is secure. Bear in mind, that certificates expire. When they expire you may need to sign and import new certificates again.

Cleaning up the stores

As this document explained at the beginning of the chapter, the goal is for each platform/station to have a single CA-signed server certificate in its User Key Store, the root certificate that signed it either in the System Trust Store or User Trust Store, and an Allowed Hosts tab that is empty. After setting up these certificates, this procedure prompts you to delete all self-signed and otherwise unapproved certificates.

Prerequisites:
You are working in Workbench on a PC.

Step 1. To open the Workbench Certificate Management view, click **Tools** > **Certificate Management.**

Step 2. Delete any default `tridium` certificate in the User Key Store.

Step 3. To open a localhost or controller Certificate Management view, do one of the following:

- Open and connect to the platform and click **Platform** > **Certificate Manatement**.
- Open and connect to the running station and click**Station** > **Config** > **Services** > **PlatformServices** > **CertManagerService**.

Step 4. Delete any default `tridium` certificate in the User Key Store.

Step 5. Click the Allowed Hosts tab and delete any certificates in this tab.

Verifying the certificates

After running the Certificate Wizard or manually setting up certificates it is important to confirm that communication within your system is secure.

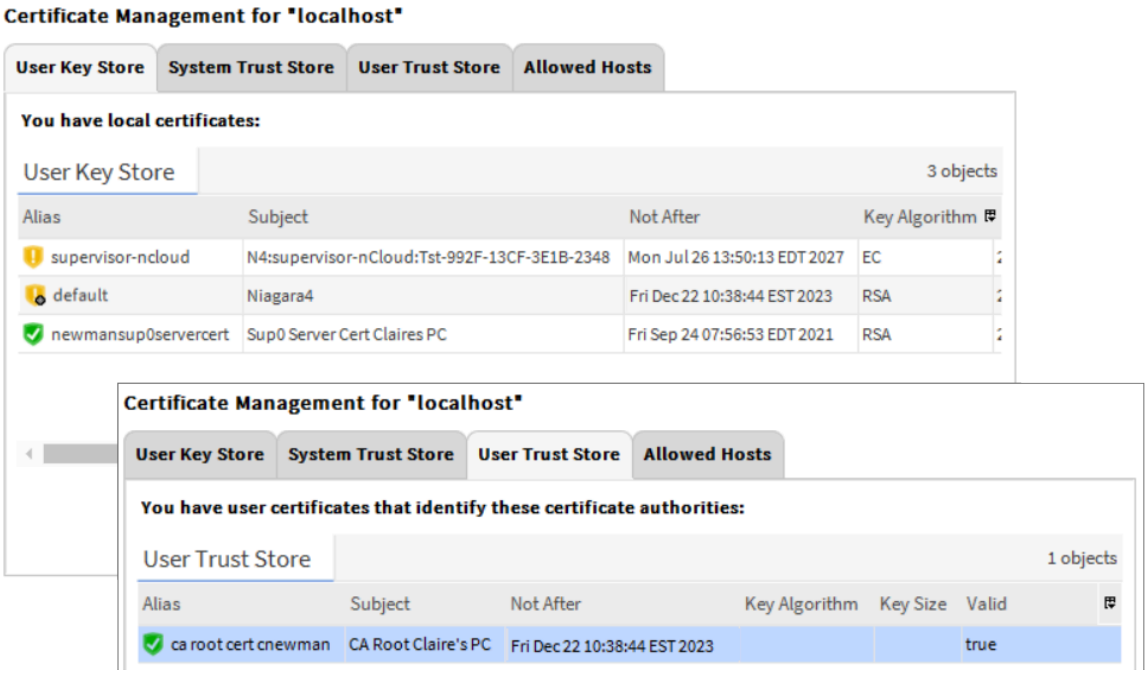
Prerequisites:
You ran the Certificate Wizard or created and imported your own certificates.

NOTE:

The platform and the station share the same trust store, while the Workbench application has its own trust store.

Step 1. From the local platform, double-click on Certificate Management and verify that the certificates were installed:

- The server certificate appears in the **User Key Store**.
- The new root CA certificate appears in the **User Trust Store**. This is a copy of the root CA certificate exported with the public key.



Certificate Management for "localhost"

You have local certificates:

User Key Store — 3 objects

Alias	Subject	Not After	Key Algorithm
supervisor-ncloud	N4:supervisor-nCloud:Tst-992F-13CF-3E1B-2348	Mon Jul 26 13:50:13 EDT 2027	EC
default	Niagara4	Fri Dec 22 10:38:44 EST 2023	RSA
newmansup0servercert	Sup0 Server Cert Claires PC	Fri Sep 24 07:56:53 EDT 2021	RSA

Certificate Management for "localhost"

You have user certificates that identify these certificate authorities:

User Trust Store — 1 objects

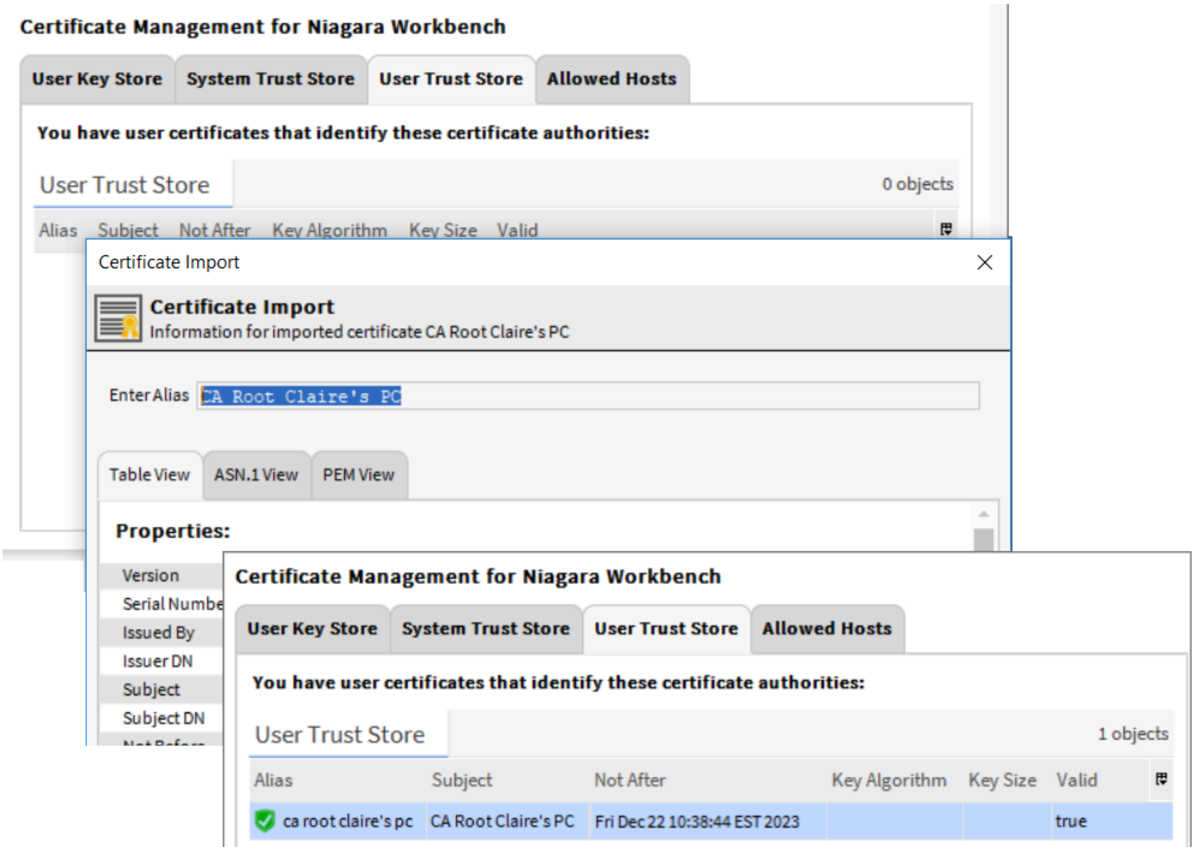
Alias	Subject	Not After	Key Algorithm	Key Size	Valid
ca root cert cnewman	CA Root Claire's PC	Fri Dec 22 10:38:44 EST 2023			true

Step 2. From the Workbench, click **Tools** > **Certificate Management**.

Step 3. Confirm that the new root CA certificate created by this instance of the Workbench (for use by the wizard) is in the Workbench **User Key Store** alongside the self-signed Tridium server certificate. Workbench is a client when connecting to platforms and stations, so it is worth pointing out that this is not a Server Certificate. The root CA certificate is available to Workbench for use in signing Server Certificates.

Notice that the root CA certificate was *not* imported into the Workbench **User Trust Store** by the **Certificate Wizard**. You need to import the root CA certificate into this location to ensure that this instance of the Workbench can validate server certificates while handshaking with platforms and stations on the network.

Step 4. To import the root CA certificate into the Workbench **User Trust Store**, Click **Import**, locate and select the new root CA certificate in `~certManagement`, and click **OK**.



You have user certificates that identify these certificate authorities:

User Trust Store 0 objects

Alias	Subject	Not After	Key Algorithm	Key Size	Valid

Information for imported certificate CA Root Claire's PC

Enter Alias CA Root Claire's PC

Properties:

Version
Serial Numbe
Issued By
Issuer DN
Subject
Subject DN

You have user certificates that identify these certificate authorities:

User Trust Store 1 objects

Alias	Subject	Not After	Key Algorithm	Key Size	Valid
✓ ca root claire's pc	CA Root Claire's PC	Fri Dec 22 10:38:44 EST 2023			true

Step 5. Verify that the TLS level for each of the following is set to TLSv1.2:

- Platform TLS Settings — Using the **Platform Administration** tool, view the `Change TLS Settings` option and verify the **`Protocol`** value.
- Station Web Service — In a station connection open a Property Sheet view on the Web Service and verify the **`Https Min Protocol`** property value.
- Station Fox Service — Open a Property Sheet view on the Fox Service and verify the **`Foxs Min Protocol`** property value.

Step 6. Select the appropriate server certificate for use in secure platform and station connections.

- Set the new server certificate to be used for secure platform (niagarad) communications.
- Set the new server certificate to be used for secure station communications via Fox and Web services.

For details, refer to the *Niagara Station Security Guide*

Accepting a self-signed certificate after a change

Your system is less secure if, instead of implementing signed server certificates, you accept self-signed certificates. If, after acceptance, the self-signed certificate’s public key changes, the system negates the certificate, changes the green shield icon on the **Allowed Hosts** tab to a yellow icon with an exclamation mark (🛡), and denies access, causing an error.

Prerequisites:
You are working in Workbench and are connected to the appropriate station.

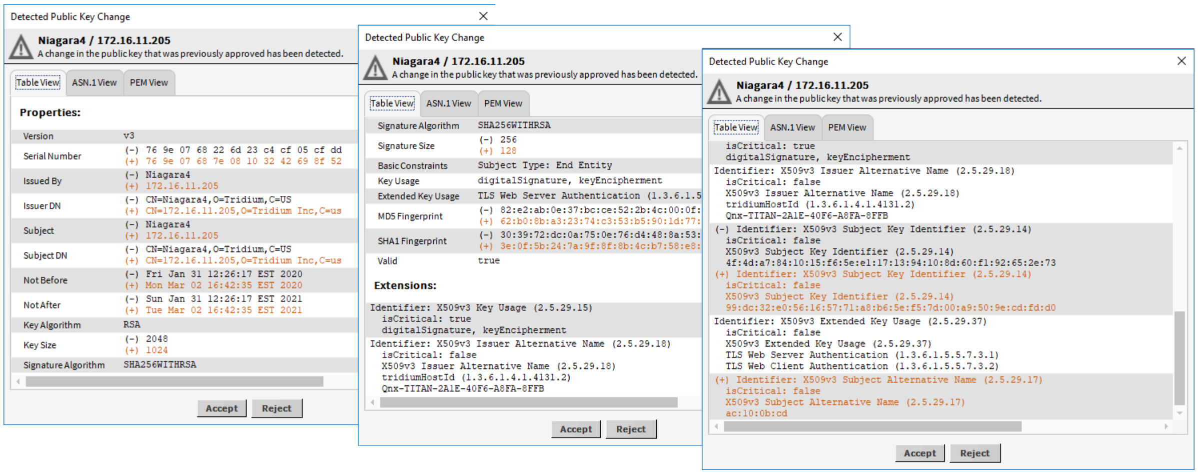
If you trust the new key, follow this procedure to accept the changed certificate. If you suspect something is wrong, investigate further. Do not accept a self-signed certificate with a new public key unless you are confident that it is secure. Better yet, stop using self-signed certificates and implement signed certificates, which provide server authentication as well as encryption.

Step 1. To access an **Allowed Hosts** tab do one of the following:

- To access the Workbench **Allowed Hosts** list, click **Tools** > **Certificate Management**, and click the **Allowed Hosts** tab.
- To access the platform/station **Allowed Hosts** list, expand **Platform** and double-click **Certificate Management** in the Nav tree. Then, click the **Allowed Hosts** tab.
- You may also access the platform/station stores by expanding **Station** > **Config** > **Services** > **PlatformServices** and double-clicking **CertManagerService** in the Nav tree.

The tab opens.

Step 2. To confirm that the public key changed, select the certificate row in the table and click **View**.
The certificate opens in the **Detected Public Key Change** window.



Niagara4 / 172.16.11.205
A change in the public key that was previously approved has been detected.

Properties:

Version	v3
Serial Number	(-) 76 9e 07 68 22 6d 23 c4 cf 05 cf dd (+) 76 9e 07 68 7e 08 10 32 42 69 8f 52
Issued By	(-) Niagara4 (+) 172.16.11.205
Issuer DN	(-) CN=Niagara4,O=Tridium,C=US (+) CN=172.16.11.205,O=Tridium Inc,C=us
Subject	(-) Niagara4 (+) 172.16.11.205
Subject DN	(-) CN=Niagara4,O=Tridium,C=US (+) CN=172.16.11.205,O=Tridium Inc,C=us
Not Before	(-) Fri Jan 31 12:26:17 EST 2020 (+) Mon Mar 02 16:42:35 EST 2020
Not After	(-) Sun Jan 31 12:26:17 EST 2021 (+) Tue Mar 02 16:42:35 EST 2021
Key Algorithm	RSA
Key Size	(-) 2048 (+) 1024
Signature Algorithm	SHA256WITHRSA

Signature Algorithm	SHA256WITHRSA
Signature Size	(-) 256 (+) 128
Basic Constraints	Subject Type: End Entity
Key Usage	digitalSignature, keyEncipherment
Extended Key Usage	TLS Web Server Authentication (1.3.6.1.5
MD5 Fingerprint	(-) 82:e2:ab:0e:37:bc:ce:52:2b:4c:00:0f: (+) 62:b0:8b:a3:23:74:c3:53:b5:90:1d:77:
SHA1 Fingerprint	(-) 30:39:72:dc:0a:75:0e:76:d4:48:8a:53: (+) 3e:0f:5b:24:7a:9f:8f:8b:4c:b7:58:e8:
Valid	true

Extensions:

```
Identifier: X509v3 Key Usage (2.5.29.15)
  isCritical: true
  digitalSignature, keyEncipherment
Identifier: X509v3 Issuer Alternative Name (2.5.29.18)
  isCritical: false
  X509v3 Issuer Alternative Name (2.5.29.18)
  tridiumHostId (1.3.6.1.4.1.4131.2)
  Qnx-TITAN-2A1E-40F6-A8FA-8FFB
```

```
  isCritical: true
  digitalSignature, keyEncipherment
Identifier: X509v3 Issuer Alternative Name (2.5.29.18)
  isCritical: false
  X509v3 Issuer Alternative Name (2.5.29.18)
  tridiumHostId (1.3.6.1.4.1.4131.2)
  Qnx-TITAN-2A1E-40F6-A8FA-8FFB
(-) Identifier: X509v3 Subject Key Identifier (2.5.29.14)
  isCritical: false
  X509v3 Subject Key Identifier (2.5.29.14)
  4f:4d:a7:84:10:15:f6:5e:e1:17:13:94:10:8d:60:f1:92:65:2e:73
(+) Identifier: X509v3 Subject Key Identifier (2.5.29.14)
  isCritical: false
  X509v3 Subject Key Identifier (2.5.29.14)
  99:dc:32:e0:56:16:57:71:a8:b6:5e:f5:7d:00:a9:50:9e:cd:fd:d0
Identifier: X509v3 Extended Key Usage (2.5.29.37)
  isCritical: false
  X509v3 Extended Key Usage (2.5.29.37)
  TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
  TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
(+) Identifier: X509v3 Subject Alternative Name (2.5.29.17)
  isCritical: false
  X509v3 Subject Alternative Name (2.5.29.17)
  ac:10:0b:cd
```

The screen captures show an example certificate after scrolling down to the mid-scroll and end-scroll regions.

Step 3. Confirm at least the `Issued By` and `Subject` properties.
The two names should be names you recognize as belonging to your company.

Step 4. Accept the self-signed certificate with the new public key, click **Accept**.
The certificate icon changes to a green shield with a check mark.

Setting up HTTP Authentication scheme for third party application

Any Third party software that requires communication through Https port, require HTTPBasicScheme authentication. If this authentication scheme is not available in the web UI, this procedure documents how to use Workbench to add this scheme to your Supervisor station.

Prerequisites:
Using Workbench you are connected to the Supervisor station.

Step 1. To confirm the authentication schemes, navigate to **Config** > **Services** > **AuthenticationService** > **Authentication Schemes**.

Step 2. If `HTTPBASICScheme` is not a listed option, open the baja palette and expand **AuthenticationSchemes** > **WebServicesSchemes**.

Step 3. Drag HTTPBasicScheme to **Config** > **Services** > **AuthenticationService** > **Authentication Schemes** in the Nav tree.

Step 4. Using the web UI, create a web user.

Related tasks

- Setting up the Obix role
- Setting up an Easy Lobby user

Preparing a secure MySQL database

Data encryption server authentication are important aspects of secure communication.

Prerequisites:
You downloaded MySQL, set up a database, created a separate unique user (not root), and assigned a password. MySQL Workbench is open.

MySQL refers to the secure communication as SSL (Secure Socket Layer). While this term is still used, the actual technology is now TLS (Transport Layer Security). Recent MySQL program files default to TLS (SSL) support. Older versions, such as version 5.7 offer secure communication, but do not enable it by default.

This procedure sets configures a MySQL database and the database user to require secure communication.

Step 1. To confirm that MySQL version 8.0 defaults to secure communication, click **Database** > **Manage Server Connections** in MySQL Workbench, click the **SSL** tab and confirm that **`Use SSL`** is configured to enable secure communication.
MySQL version 8.0 defaults to `If available`, which means that it supports TLS.

Step 2. To confirm that an earlier version of MySQL is configured for secure communication, use the Windows Command Prompt.

a. Change directories to `C:\Program Files\MySQL\MySQL Server n.n\bin` (replace `n.n` with the MySQL version number).

b. Run this command to open the MySQL Console: `mysql -u<name> -p` (replace `<name>` with your MySQL user name).

```
C:\Program Files\MySQL\MySQL Server 5.7\bin>mysql —uentsecuser —p
```

c. Enter your password.
The MySQL Console opens.

```
Enter password: **********
```

```
Welcome to the MySQL monitor. ...
```
etc.

d. From within the console, run this command: `mysql> show global variables like ‘%ssl%’;`.
The monitor displays a table of variables.

e. Confirm that value of have openssl is YES and the value of have ssl is YES
"YES" mean that the database is configured for secure communication.

Step 3. If MySQL does not default to secure communication, either use MySQL Workbench to enable SSL or download a more recent version.

Step 4. To update a MySQL user to require secure communication, enter these commands at the Command Prompt:
mysql> UPDATE mysql.<user> SET ssl type = 'ANY'; where <user> is the name of a user you created in MySQL Workbench.

mysql> FLUSH PRIVILEGES;

Result
The database is ready for you to install a client and the CA root certificates.

Using OpenSSL to create certificates

While Niagara provides its own Certificate Manager, which is capable of creating and signing certificates, some applications and browsers cannot use the resulting certificates. This procedure ensures that the three certificates it creates will work to secure communication with a MySQL database.

Prerequisites:
The MySQL monitor is open using the Windows Command Prompt

IMPORTANT: The CN (Common Name) for each certificate must be unique. Two certificates cannot share the same name.

Step 1. Download OpenSSL from here: https://www.openssl.org/source/ and install it on your Supervisor PC.

Step 2. To create a folder for the certificates enter:
mkdir C:\<path> where <path> defines a folder name.

Step 3. In Windows, set up an environment variable for OpenSSL as follows:
OPENSSL_CONF=c:\OpenSSL-Win64\bin\openssl.cfg

Step 4. Open the MySQL monitor.
For specific steps, refer to the previous topic.

Step 5. Create three certificates: root CA (Certificate Authority), server certificate signed by the root CA certificate and a client certificate also signed by the root CA:

Your file names can be different from the example names.

Certificate	Example file names	Command
root CA certificate	ca-key.pemca-cert.pem	openssl genrsa 2048 > "C:/mysqlCerts/ca-key.pem" openssl req -new -x509 -nodes -days 3600 -key "C:/mysqlCerts/ca-key.pem" > "C:/mysqlCerts/ca-cert.pem"
server certificate	server-cert.pemserver-key.pemserver-req.pem	openssl req -newkey rsa:2048 -days 3600 -nodes -keyout "C:/mysqlCerts/server-key.pem" > "C:/mysqlCerts/server-req.pem" openssl x509 -req -in "C:/mysqlCerts/server-req.pem" -days 3600 -CA "C:/mysqlCerts/ca-cert.pem" -CAkey "C:/mysqlCerts/ca-key.pem" -set_serial 01 > "C:/mysqlCerts/server-cert.pem"
client certificate	client-cert.pemclient-key.pemclient-req.pem	openssl req -newkey rsa:2048 -days 3600 -nodes -keyout "C:/mysqlCerts/client-key.pem" > "C:/mysqlCerts/client-req.pem" openssl x509 -req -in "C:/mysqlCerts/client-req.pem" -days 3600 -CA "C:/mysqlCerts/ca-cert.pem" -CAkey "C:/mysqlCerts/ca-key.pem" -set_serial 01 > "C:/mysqlCerts/client-cert.pem"

Step 6. To update the MySQL config file (my.ini) change directories to: C:\ProgramData\MySQL\MySQL Server 5.7\, open my.ini using Notepad and add this command in the [mysqld] section and add these commands.

```
ssl-ca = "C:/mysqlCerts/ca-cert.pem"
ssl-cert = "C:/mysqlCerts/server-cert.pem"
ssl-key = "C:/mysqlCerts/server-key.pem"
```

Step 7. Restart the MySQL service/server and confirm that communication with the MySQL database is now secure using the MySQL monitor again with the ssl command.

```
mysql> show global variables like '%ssl%';
```

Both have openssl and have ssl should report YES.

Step 8. Another way to confirm that MySQL is configured for secure communication is to issue the status command in the monitor.

```
mysql> status
```

This row in the list reports that SSL is in use:

```
SSL: Cipher in use is DHE-RSA-AES256-SHA
```

Step 9. To connect to the database using a user that requires a secure connection, enter this command in the monitor:

```
mysql.exe -<ussluser> -p --ssl-mode=REQUIRED
```

where <ussluser> is a user that requires a secure connection.

Step10. To double-check, you should get an error if you attempt to connect this same user without the ssl-mode=Required option.

```
mysql.exe -ussluser -p --ssl=0
```

Chapter 5. Controller commissioning

A controller platform may come with a station already installed, or you may be required to install the station distribution software yourself. There are multiple ways to install and create stations using Workbench. This chapter assumes the majority circumstance. Installing a stand-alone controller represents a single instance of the procedures in this chapter.

You initialize and configure a controller after placing it on the network and applying power to it. Initialization using Workbench includes:

- Logging in to the controller platform.
- If the controller needs a station, using the distribution installer to create the station.
- Commissioning the station.
- Installing the license.

After completing procedures in Workbench, you log in to the station and configure devices using the web UI.

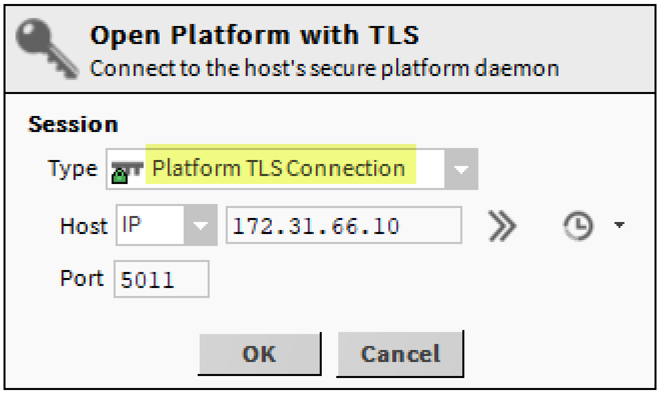
Opening a platform connection to a controller (niagarad)

Connecting to the controller using Workbench demonstrates that the controller is on line and functioning. Workbench provides tools for installing software and commissioning the controller station.

Prerequisites:
The controller is new from the factory. The only software on it are factory defaults. It is connected to the same network as the Supervisor PC, has a valid IP address, and its power is on. You are running Workbench on your Supervisor PC.

Step 1. To open a connection to the platform daemon that is running on the controller, click **File** > **Open** > **Open Platform**.

The **Connect/Open Platform** window opens.



Open Platform with TLS

Connect to the host's secure platform daemon

Session

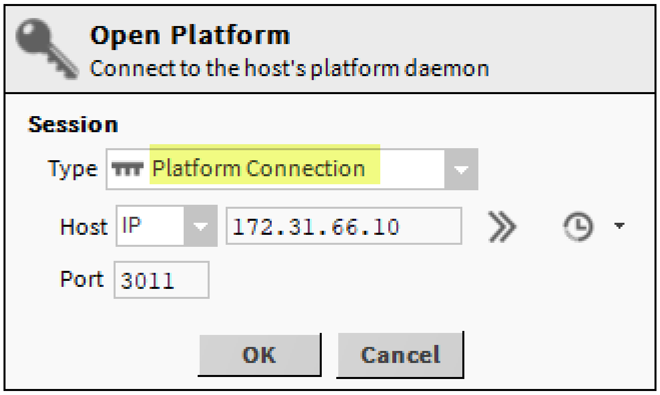
Type Platform TLS Connection

Host IP 172.31.66.10

Port 5011

The daemon runs automatically when the controller is powered up. As shown above, the connection defaults to a secure **Type** `Platform TLS Connection`. After initial platform configuration you will always access the platform using this type of secure connection. (TLS stands for Transport Layer Security.)

For this initial installation purposes only, the system requires a regular platform connection.



Open Platform

Connect to the host's platform daemon

Session

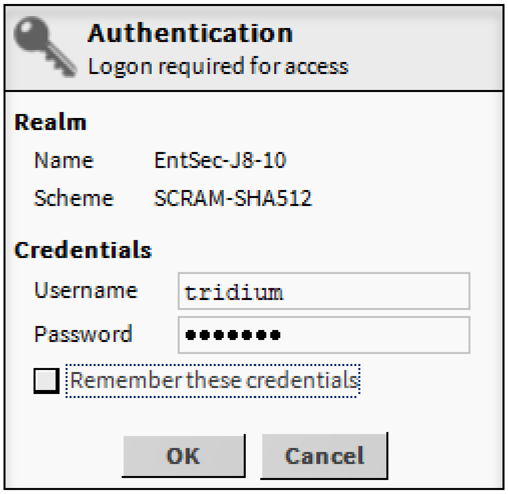
Type Platform Connection

Host IP 172.31.66.10

Port 3011

Step 2. Change **Type** to `Platform Connection` and click **OK**.

The **Authentication** window opens and prompts you for your credentials.



Authentication

Logon required for access

Realm

Name EntSec-J8-10

Scheme SCRAM-SHA512

Credentials

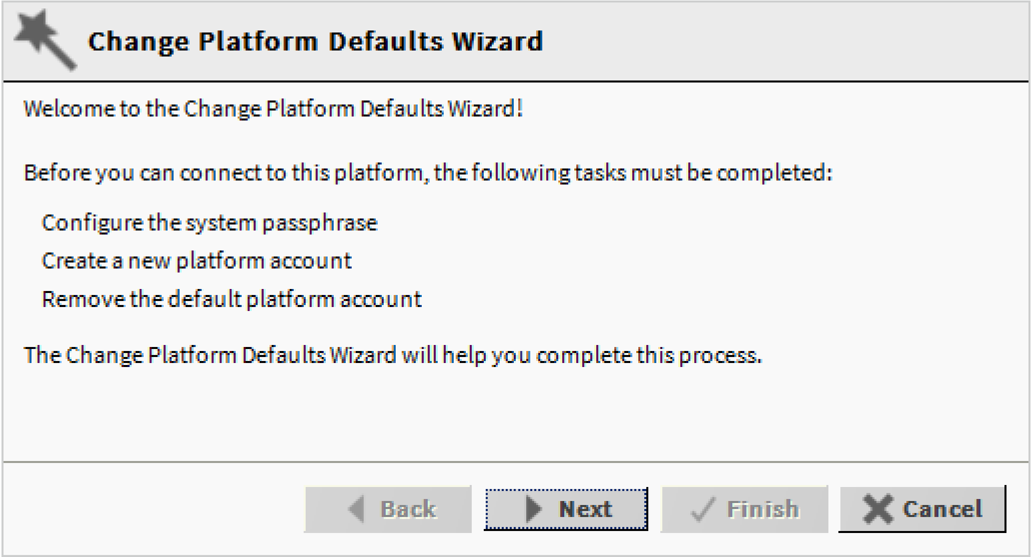
Username tridium

Password •••••••

□ Remember these credentials

The factory default **Username** is tridium. The factory default **Password** is niagara.

Step 3. Confirm the factory default credentials, and click **OK**.
The platform detects the default credentials and opens the Change Platform Defaults Wizard.



Change Platform Defaults Wizard

Welcome to the Change Platform Defaults Wizard!

Before you can connect to this platform, the following tasks must be completed:

Configure the system passphrase
Create a new platform account
Remove the default platform account

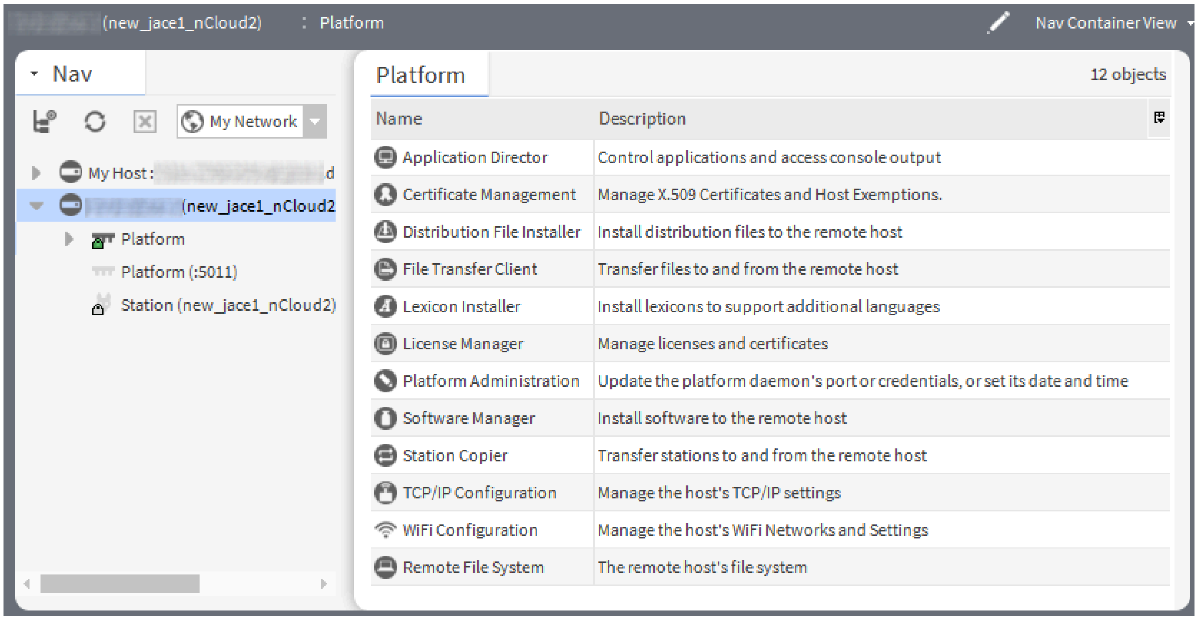
The Change Platform Defaults Wizard will help you complete this process.

The system will not let you continue with default credentials. User names and passwords form the front-line of defense against unauthorized system access.

Step 4. Follow the wizard, which includes creating a **Passphrase**, **Username** and strong **Password**. Click **Next**, followed by clicking **Finish**.
The passphrase protects the platform's file system, encrypting the HSQL database when you create a station copy. The Distribution File Installer requires the system passphrase to restore a backup .dist file. The Station Copier requires the same system passphrase to transfer a local file.

Best practice: Use the same Passphrase for your Supervisor and controller platforms.

The system completes making the connection between the host and Workbench, and displays the Nav Container View



[redacted] (new_jace1_nCloud2) : Platform

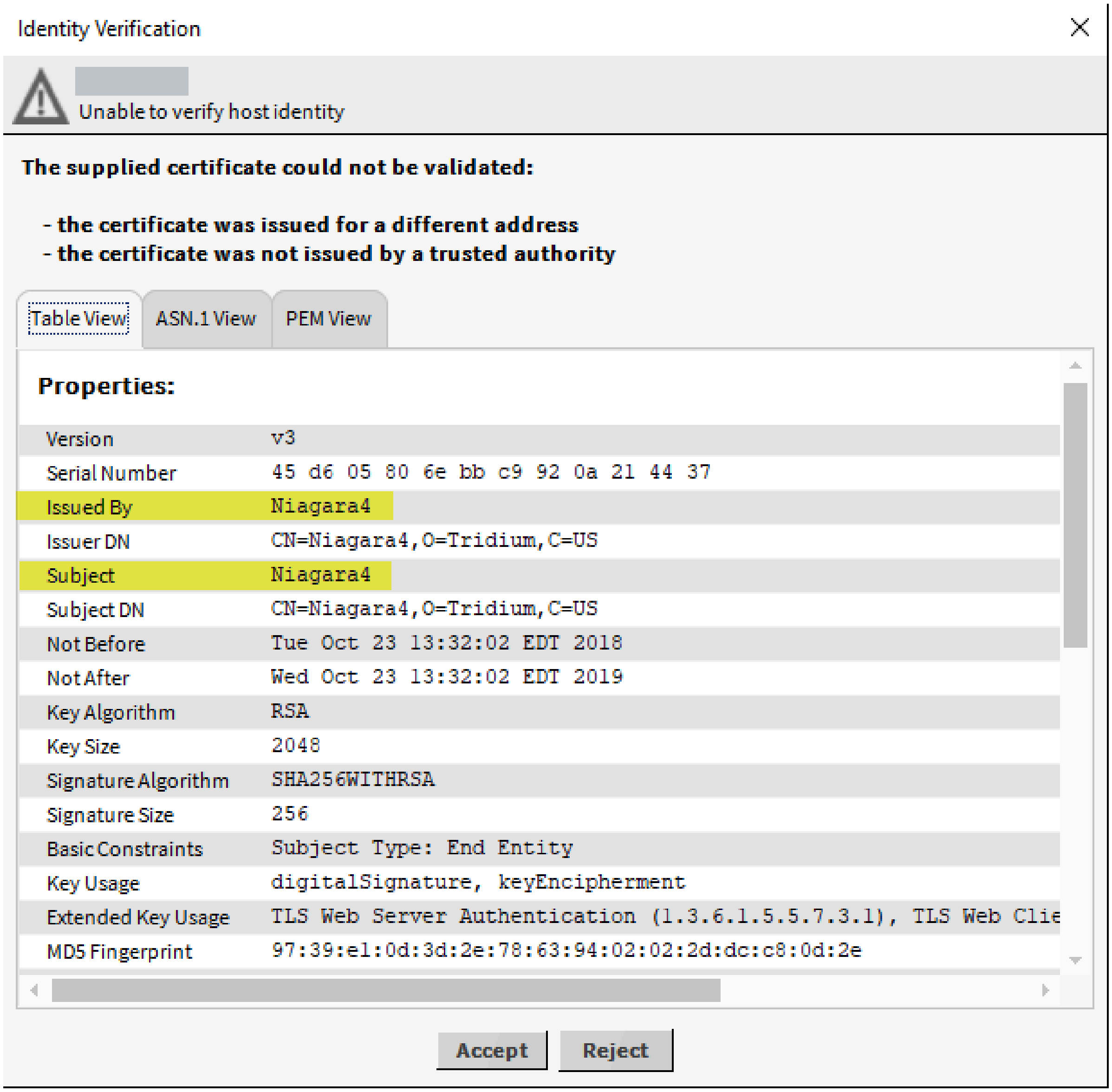
Nav Container View

Platform — 12 objects

Name	Description
Application Director	Control applications and access console output
Certificate Management	Manage X.509 Certificates and Host Exemptions.
Distribution File Installer	Install distribution files to the remote host
File Transfer Client	Transfer files to and from the remote host
Lexicon Installer	Install lexicons to support additional languages
License Manager	Manage licenses and certificates
Platform Administration	Update the platform daemon's port or credentials, or set its date and time
Software Manager	Install software to the remote host
Station Copier	Transfer stations to and from the remote host
TCP/IP Configuration	Manage the host's TCP/IP settings
WiFi Configuration	Manage the host's WiFi Networks and Settings
Remote File System	The remote host's file system

Step 5. Make sure that for **`Type`** the `Platform TLS Connection` is selected from the drop-down list; for **`Host IP`**, enter the IP address for the controller; then click OK.
A secure TLS connection is the default. This protocol provides data encryption and server authentication to prevent malicious hacks into the system.

The **Identify Verification** window opens with an error message.



Identity Verification

[redacted]

Unable to verify host identity

The supplied certificate could not be validated:

- **the certificate was issued for a different address**
- **the certificate was not issued by a trusted authority**

Properties:

Version	v3
Serial Number	45 d6 05 80 6e bb c9 92 0a 21 44 37
Issued By	Niagara4
Issuer DN	CN=Niagara4,O=Tridium,C=US
Subject	Niagara4
Subject DN	CN=Niagara4,O=Tridium,C=US
Not Before	Tue Oct 23 13:32:02 EDT 2018
Not After	Wed Oct 23 13:32:02 EDT 2019
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	SHA256WITHRSA
Signature Size	256
Basic Constraints	Subject Type: End Entity
Key Usage	digitalSignature, keyEncipherment
Extended Key Usage	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1), TLS Web Clie
MD5 Fingerprint	97:39:e1:0d:3d:2e:78:63:94:02:02:2d:dc:c8:0d:2e

The error message indicates that the controller's server certificate is self-signed. As such, it can encrypt data communication, but it cannot authenticate the server (the controller) to its client (Workbench). This is because none of the root certificates in the Workbench Trust Store recognize this certificate. Since you know that the controller is a valid server you can accept the self-signed certificate temporarily so as to continue with the login.

Commissioning a controller

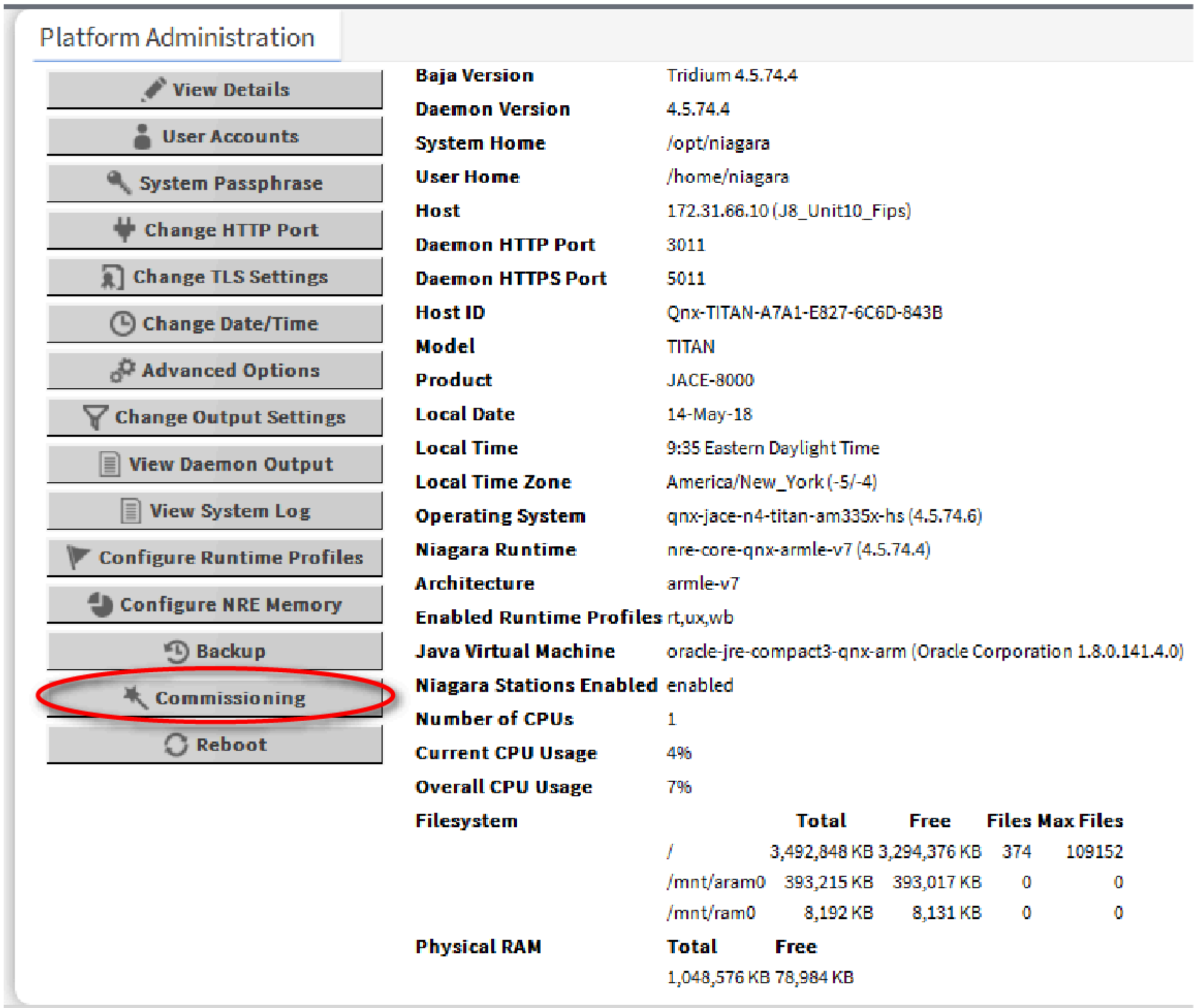
Commissioning installs the software on a controller. This procedure works for commissioning a new controller or upgrading an existing controller.

Prerequisites:
You are working in Workbench. You are connected to the controller platform.

Step 1. Double-click the **Platform** node for the controller in the Nav tree.
The **Authentication** window opens.

Step 2. Enter the credentials you just created when you connected to the platform for the first time, enable **Remember these credentials**, and click **OK**.
The Nav Container View opens.

Step 3. Double-click **Platform Administration** row in the table.
The **Platform Administration** view opens.



Baja Version	Tridium 4.5.74.4
Daemon Version	4.5.74.4
System Home	/opt/niagara
User Home	/home/niagara
Host	172.31.66.10 (J8_Unit10_Fips)
Daemon HTTP Port	3011
Daemon HTTPS Port	5011
Host ID	Qnx-TITAN-A7A1-E827-6C6D-843B
Model	TITAN
Product	JACE-8000
Local Date	14-May-18
Local Time	9:35 Eastern Daylight Time
Local Time Zone	America/New_York (-5/-4)
Operating System	qnx-jace-n4-titan-am335x-hs (4.5.74.6)
Niagara Runtime	nre-core-qnx-armle-v7 (4.5.74.4)
Architecture	armle-v7
Enabled Runtime Profiles	rt,ux,wb
Java Virtual Machine	oracle-jre-compact3-qnx-arm (Oracle Corporation 1.8.0.141.4.0)
Niagara Stations Enabled	enabled
Number of CPUs	1
Current CPU Usage	4%
Overall CPU Usage	7%

Filesystem

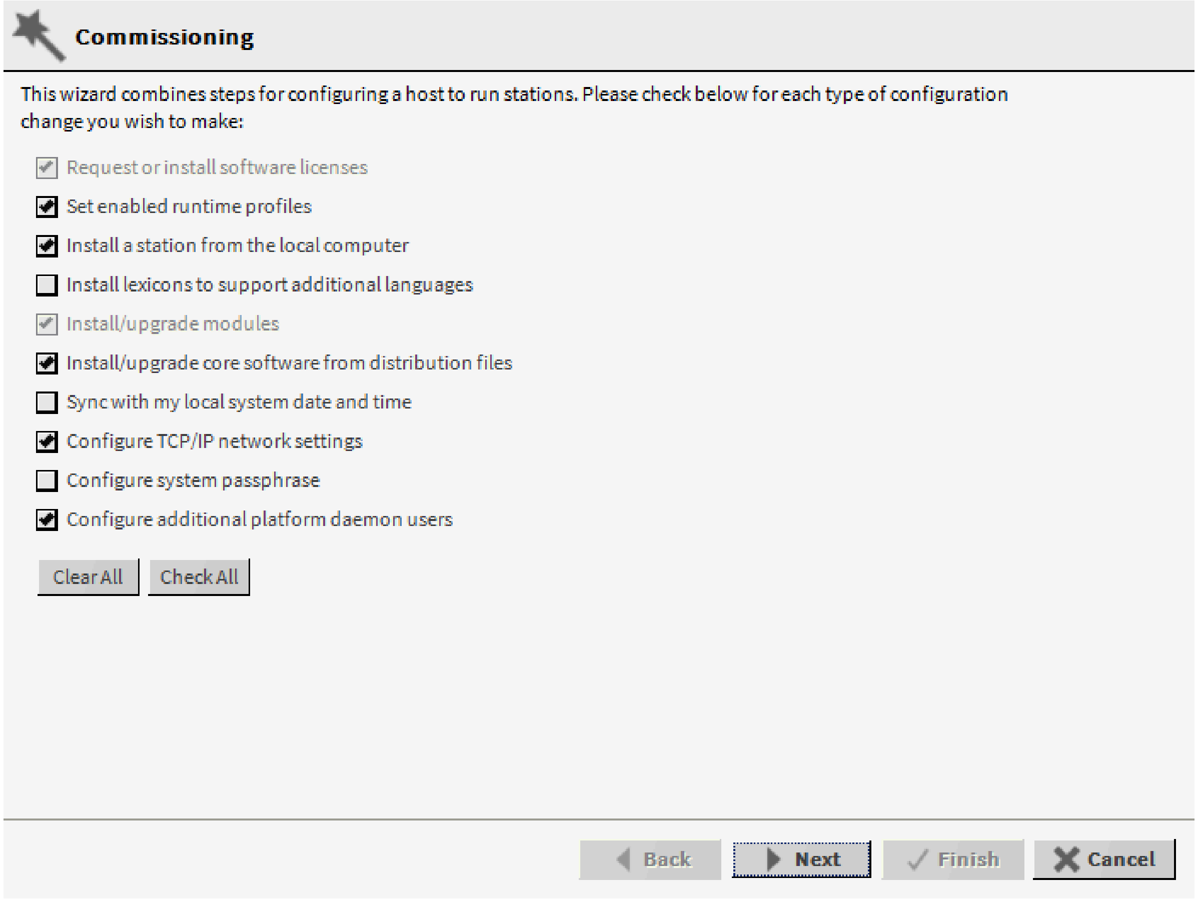
	Total	Free	Files	Max Files
/	3,492,848 KB	3,294,376 KB	374	109152
/mnt/aram0	393,215 KB	393,017 KB	0	0
/mnt/ram0	8,192 KB	8,131 KB	0	0

Physical RAM

Total	Free
1,048,576 KB	78,984 KB

Step 4. Click the **Commissioning** button.

The **Commissioning** wizard opens.



Commissioning

This wizard combines steps for configuring a host to run stations. Please check below for each type of configuration change you wish to make:

☑ Request or install software licenses

☑ Set enabled runtime profiles

☑ Install a station from the local computer

☐ Install lexicons to support additional languages

☑ Install/upgrade modules

☑ Install/upgrade core software from distribution files

☐ Sync with my local system date and time

☑ Configure TCP/IP network settings

☐ Configure system passphrase

☑ Configure additional platform daemon users

This wizard is intended for a remote controller only. This button is not available when connected to any Windows platform. For commissioning details, refer to the appropriate installation and startup guide for your particular controller.

NOTE: If the Workbench FIPS property **`Show FIPS Options`** is set to `true` certain FIPS options become visible in this window. If selected, the framework enforces FIPS-strength password requirements.

Step 5. Follow the wizard, clicking **Next** until you configure all options.

Step 6. After reviewing all changes, click **Finish**.
Commissioning begins.

CAUTION: Do not interrupt the commissioning process. If you interrupt, you may not be able to restore the station.

After the commissioning process is complete, the controller boots.

Step 7. When prompted, click **Close**.
The wizard installs the software and reboots the controller.

Installing a controller license

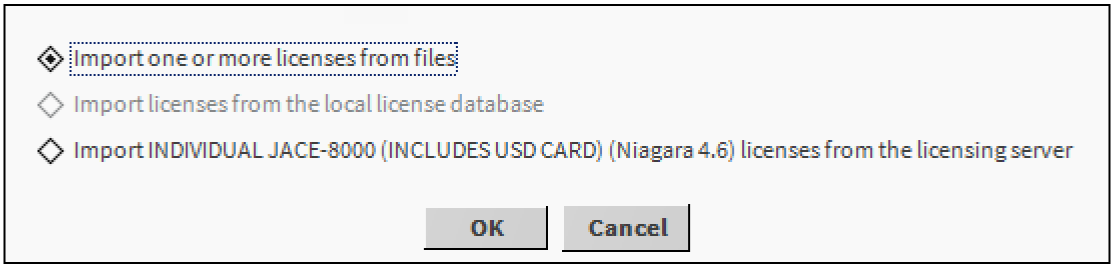
If you did not license the controller during commissioning, you either need to access the licensing server over the Internet or have downloaded the license from the server in advance. You may use Workbench or the web UI to install a license in a remote controller. This procedure documents installation using Workbench.

Prerequisites:
Your PC is connected to the controller platform and running Workbench. The PC is connected to the Internet, or you downloaded and have available the license file.

Initial licensing needs to be done with a platform connection because the station will not run until it is licensed.

Step 1. Connect to the controller platform and double-click the **License Manager** row in the Nav Container View.
The License Manager view opens.

Step 2. Click the **Import** button under the Licenses pane.
The **Import License** window opens.

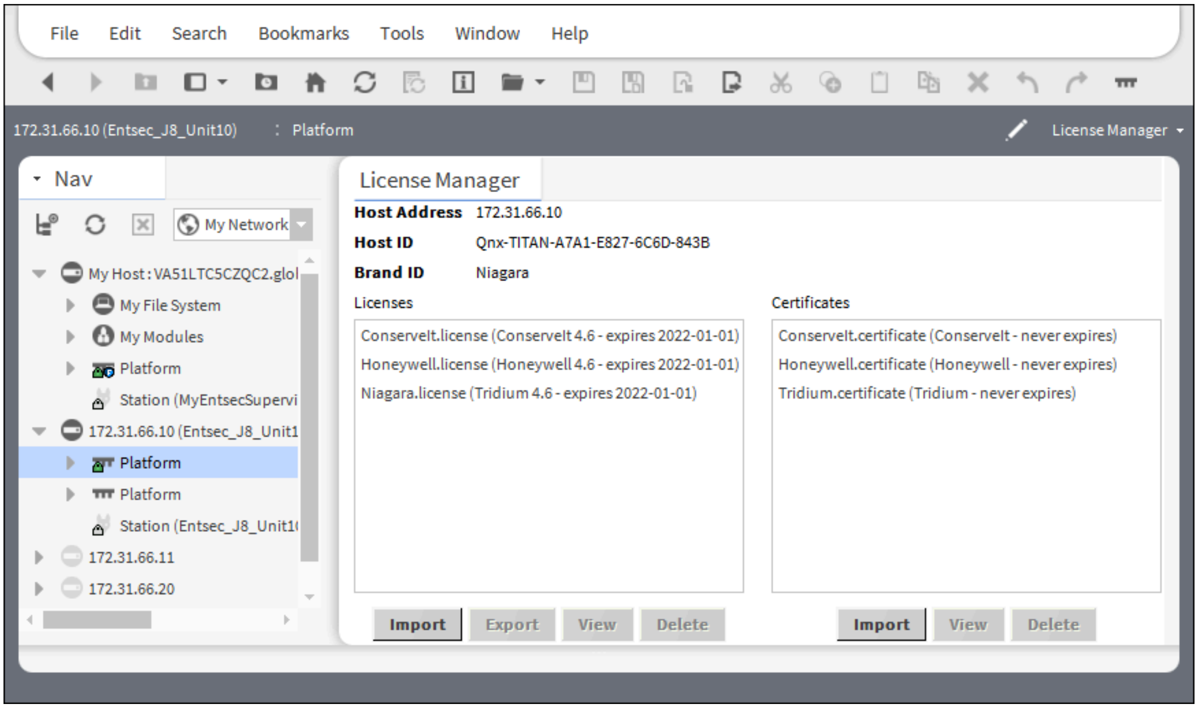


◈ Import one or more licenses from files

◇ Import licenses from the local license database

◇ Import INDIVIDUAL JACE-8000 (INCLUDES USD CARD) (Niagara 4.6) licenses from the licensing server

Step 3. Select the import option to use and click **OK**.
After the software imports the license you see it in the License Manager.



Host Address 172.31.66.10

Host ID Qnx-TITAN-A7A1-E827-6C6D-843B

Brand ID Niagara

Licenses

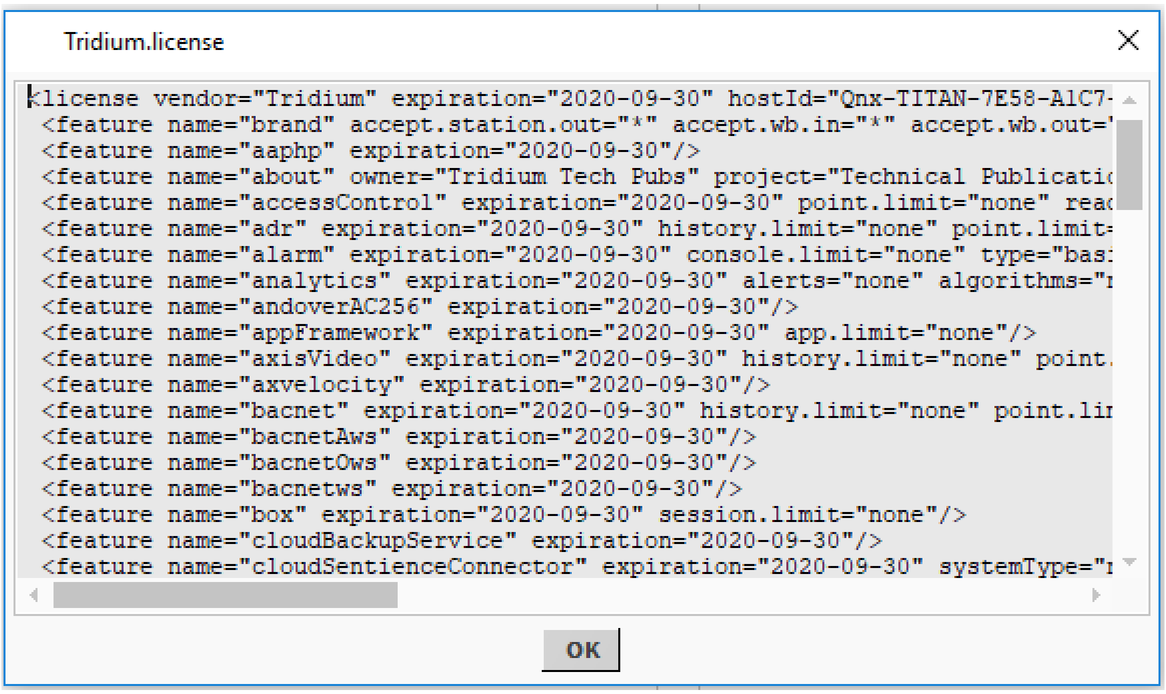
Conservelt.license (Conservelt 4.6 - expires 2022-01-01)
Honeywell.license (Honeywell 4.6 - expires 2022-01-01)
Niagara.license (Tridium 4.6 - expires 2022-01-01)

Certificates

Conservelt.certificate (Conservelt - never expires)
Honeywell.certificate (Honeywell - never expires)
Tridium.certificate (Tridium - never expires)

Step 4. To view a license, select it and click **View** or double-click the license in the table.

The license file opens.



```
<license vendor="Tridium" expiration="2020-09-30" hostId="Qnx-TITAN-7E58-A1C7-
  <feature name="brand" accept.station.out="*" accept.wb.in="*" accept.wb.out="
  <feature name="aaphp" expiration="2020-09-30"/>
  <feature name="about" owner="Tridium Tech Pubs" project="Technical Publicati
  <feature name="accessControl" expiration="2020-09-30" point.limit="none" reac
  <feature name="adr" expiration="2020-09-30" history.limit="none" point.limit=
  <feature name="alarm" expiration="2020-09-30" console.limit="none" type="basi
  <feature name="analytics" expiration="2020-09-30" alerts="none" algorithms="r
  <feature name="andoverAC256" expiration="2020-09-30"/>
  <feature name="appFramework" expiration="2020-09-30" app.limit="none"/>
  <feature name="axisVideo" expiration="2020-09-30" history.limit="none" point.
  <feature name="axvelocity" expiration="2020-09-30"/>
  <feature name="bacnet" expiration="2020-09-30" history.limit="none" point.lir
  <feature name="bacnetAws" expiration="2020-09-30"/>
  <feature name="bacnetOws" expiration="2020-09-30"/>
  <feature name="bacnetws" expiration="2020-09-30"/>
  <feature name="box" expiration="2020-09-30" session.limit="none"/>
  <feature name="cloudBackupService" expiration="2020-09-30"/>
  <feature name="cloudSentienceConnector" expiration="2020-09-30" systemType="r
```

A license and a certificate are each a digitally-signed text file, with differences briefly as follows:

- A license file is unique to a specific host, and enables a set of vendor features. All hosts require a branded Tridium license. If third-party modules are installed, one or more additional licenses may be needed.
- A certificate file varies by vendor, and matches that vendor to a public key used for encryption and to verify the authenticity of license file. All hosts require a default certificate. If third-party modules are installed, one or more additional certificates may be needed.

  CAUTION: Do not delete an existing license or certificate without a specific reason, as you will likely render the controller inoperable until a proper license or certificate is reinstalled!

Step 5. After installing a license, open the Application Director, confirm that both **Auto Start** and **Restart on Failure** are selected, then start the station by clicking **Start**.

Creating a new station in a controller

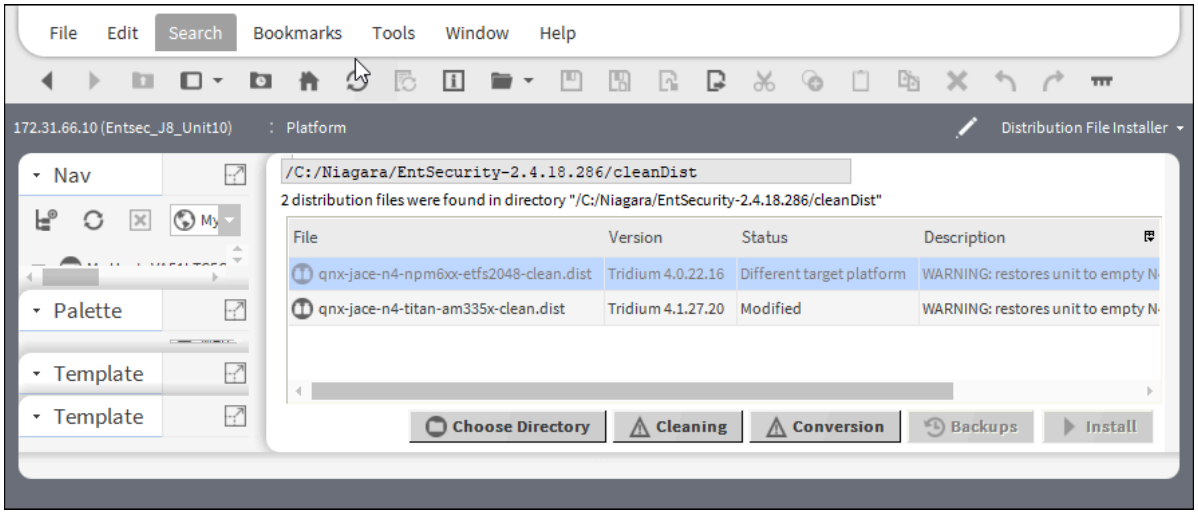
If the controller you are using already has a station on it, you can bypass this procedure. If your controller is brand new and contains no station, this procedure uses Workbench to install the distribution file.

Prerequisites:
You successfully commissioned the controller. There is no station in the controller.

Step 1. Make a platform connection to the controller.

Step 2. Right-click the controller's **Platform** node in the Nav tree and click **Views** > **Distribution File Installer**.

By default, this view opens to the `cleanDist` folder.



/C:/Niagara/EntSecurity-2.4.18.286/cleanDist

2 distribution files were found in directory "/C:/Niagara/EntSecurity-2.4.18.286/cleanDist"

File	Version	Status	Description
qnx-jace-n4-npm6xx-etfs2048-clean.dist	Tridium 4.0.22.16	Different target platform	WARNING: restores unit to empty N
qnx-jace-n4-titan-am335x-clean.dist	Tridium 4.1.27.20	Modified	WARNING: restores unit to empty N

The .dist (distribution) files that are available in this folder return the controller to near factory defaults. Do not use these files unless you need to start completely from scratch.

If a distribution file is not available, the Status message reports the error. Refer to *Troubleshooting*.

Step 3. Click **Choose Directory**, navigate to the `~sw\restore` folder and click **OK**.

Step 4. Select the system .dist file and click **Install**.
The Distribution File Installer wizard opens.

Step 5. Click **Finish** to follow the wizard.
The wizard installs the distribution file, and reboots the controller.

Step 6. When prompted, click **Close** and wait for the controller to reboot.
This could take a few minutes.

Related information

- Maintenance

Configuring the Application Director to restart

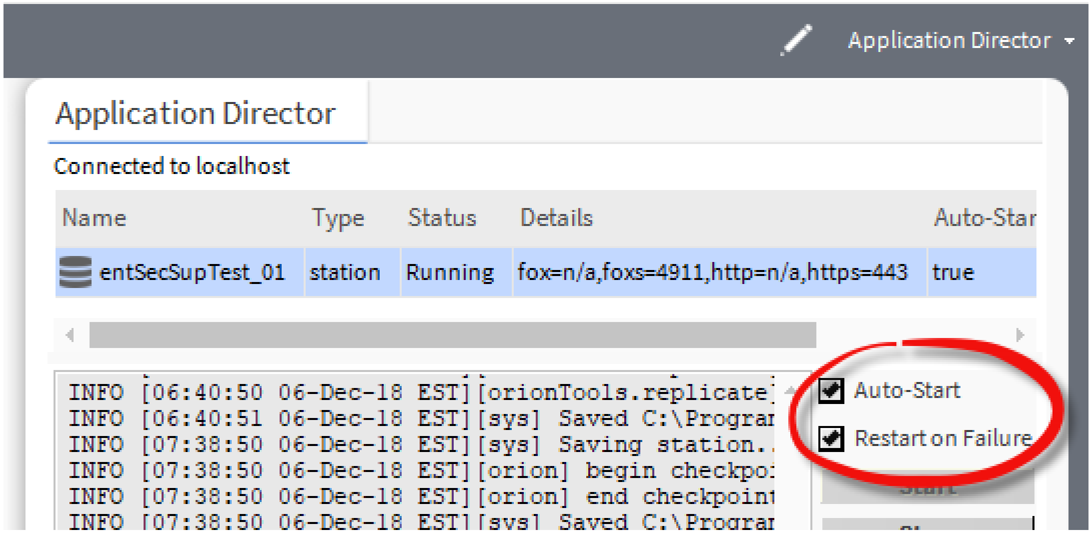
There are any number of reasons that a controller station my stop running. As a best practice, you should configure the Application Director to restart the station automatically.

Prerequisites:
You are working in Workbench running on a PC.

Step 1. Open a platform connection to the Supervisor or controller platform.

Step 2. Double-click Application Director.

Step 3. If needed, drag the window down so you can see the station, and confirm you are working with the expected station.



Connected to localhost

Name	Type	Status	Details	Auto-Star
entSecSupTest_01	station	Running	fox=n/a,foxs=4911,http=n/a,https=443	true

```
INFO [06:40:50 06-Dec-18 EST][orionTools.replicate]
INFO [06:40:51 06-Dec-18 EST][sys] Saved C:\Prograr
INFO [07:38:50 06-Dec-18 EST][sys] Saving station..
INFO [07:38:50 06-Dec-18 EST][orion] begin checkpo:
INFO [07:38:50 06-Dec-18 EST][orion] end checkpoint
INFO [07:38:50 06-Dec-18 EST][sys] Saved C:\Prograr
```

☑ Auto-Start

☑ Restart on Failure

Step 4. Enable **Auto-Start** and **Restart on Failure**.

Result

If you are debugging an issue, disable **Restart on Failure** so you can view the log.

Creating and updating the HSQL database password

Each controller ships from the factory with a default HSQL database password and upgrading an AX station to an N4 station resets the HSQL database password back to the factory default. While the default password initially works, as soon as you install or upgrade a controller and its software, you should change this password to a unique and strong string. The password is automatically generated and successfully stored in the key ring.

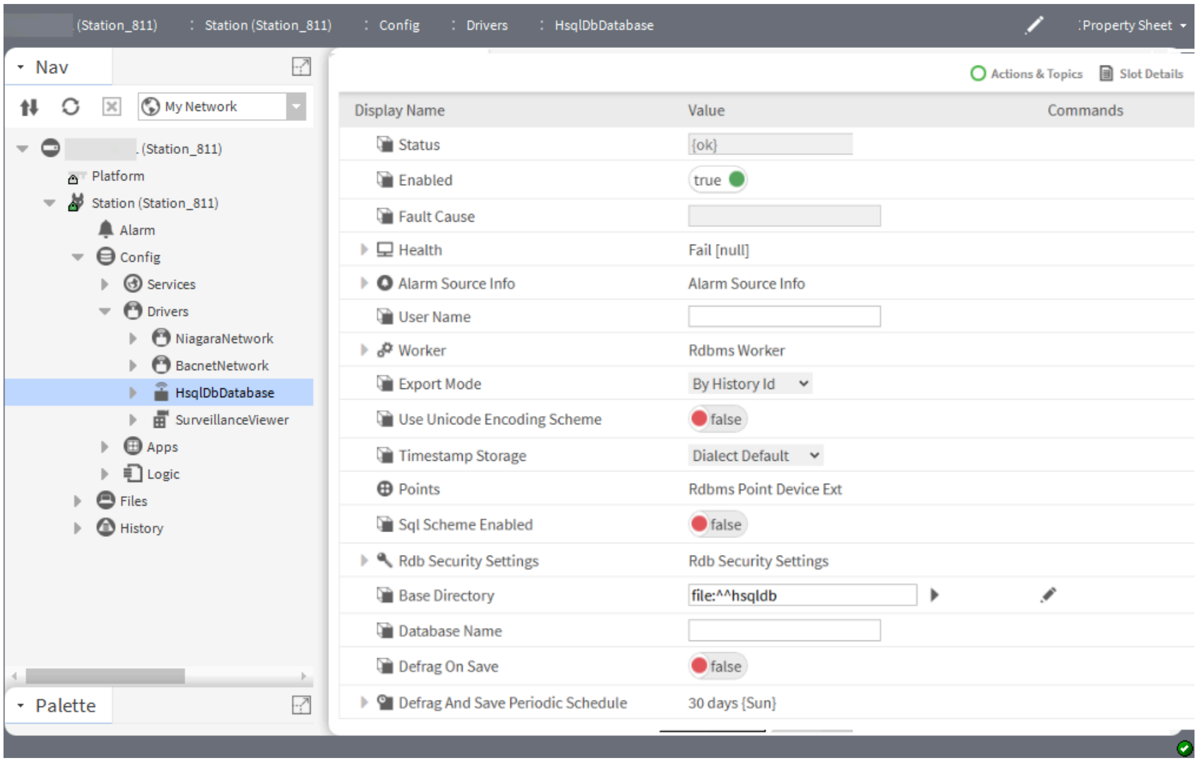
Prerequisites:

You have just installed a new controller or upgraded an existing controller from AX to N4. You are using Workbench running on a PC that is connected to the network that services the controller.

Step 1. Connect to the controller station using Workbench.

Step 2. Expand **Config** > **Drivers** > **RdbmsNetwork**.

Step 3. Right-click **HsqlDbDatabase** and click **Actions** > **Ping**. The health property is updated based on the ping results.



Display Name	Value	Commands
Status	{ok}	
Enabled	true ●	
Fault Cause		
Health	Fail [null]	
Alarm Source Info	Alarm Source Info	
User Name		
Worker	Rdbms Worker	
Export Mode	By History Id	
Use Unicode Encoding Scheme	● false	
Timestamp Storage	Dialect Default	
Points	Rdbms Point Device Ext	
Sql Scheme Enabled	● false	
Rdb Security Settings	Rdb Security Settings	
Base Directory	file:^^hsqldb	
Database Name		
Defrag On Save	● false	
Defrag And Save Periodic Schedule	30 days {Sun}	

NOTE: Starting in Niagara 4.14, the HsqlDbDatabase component properties **Use Encrypted Connection**, **User Name**, and **Password** are replaced with a single **Privileged Username** property. The HSQL database is automatically generated and not editable or visible. When using HSQL, if the station keyring is corrupted, you need to load a backup station, as this instance of the HSQL database is no longer operational.

Step 4. To access a new HSSQL database instance in the N4 station, right-click the HsqlDbDatabase, navigate to **Views** > **Property Sheet**.
The device’s Property Sheet opens.

Step 5. Enter the **User Name** as `SA` and click **Save**.

Step 6. Right-click **HsqlDbDatabase** and click **Actions** > **Ping**. The health property is updated based on the ping results.

Connecting to the controller station using Workbench

This procedure documents how to connect the controller for the first time using Workbench.

Prerequisites:
You commissioned the controller and installed the distribution file.

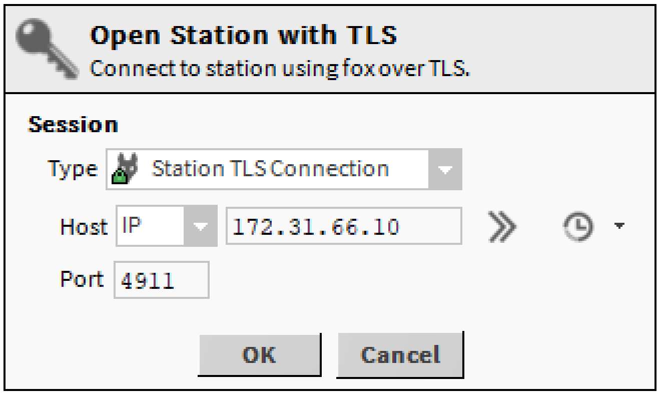
Step 1. Right-click the controller platform in the Nav tree and click **Connect**.
The **Authentication** window opens.

Step 2. Enter your platform credentials and click **OK**, or just click **OK** if **Remember these credentials** is enabled.
The **Nav Container View** opens.

Step 3. Double-click the Application Director.
The **Application Director view** opens.

Step 4. If the station Status reports `Idle`, confirm that **`Auto-Start`** and **`Restart on Failure`** are enabled and click the **Start** button.
The station is on line when its Status reports `Running`.

Step 5. Click **File** > **Open** > **Open Station**.
The **Connect** window opens.



Open Station with TLS
Connect to station using fox over TLS.

Session

Type: Station TLS Connection

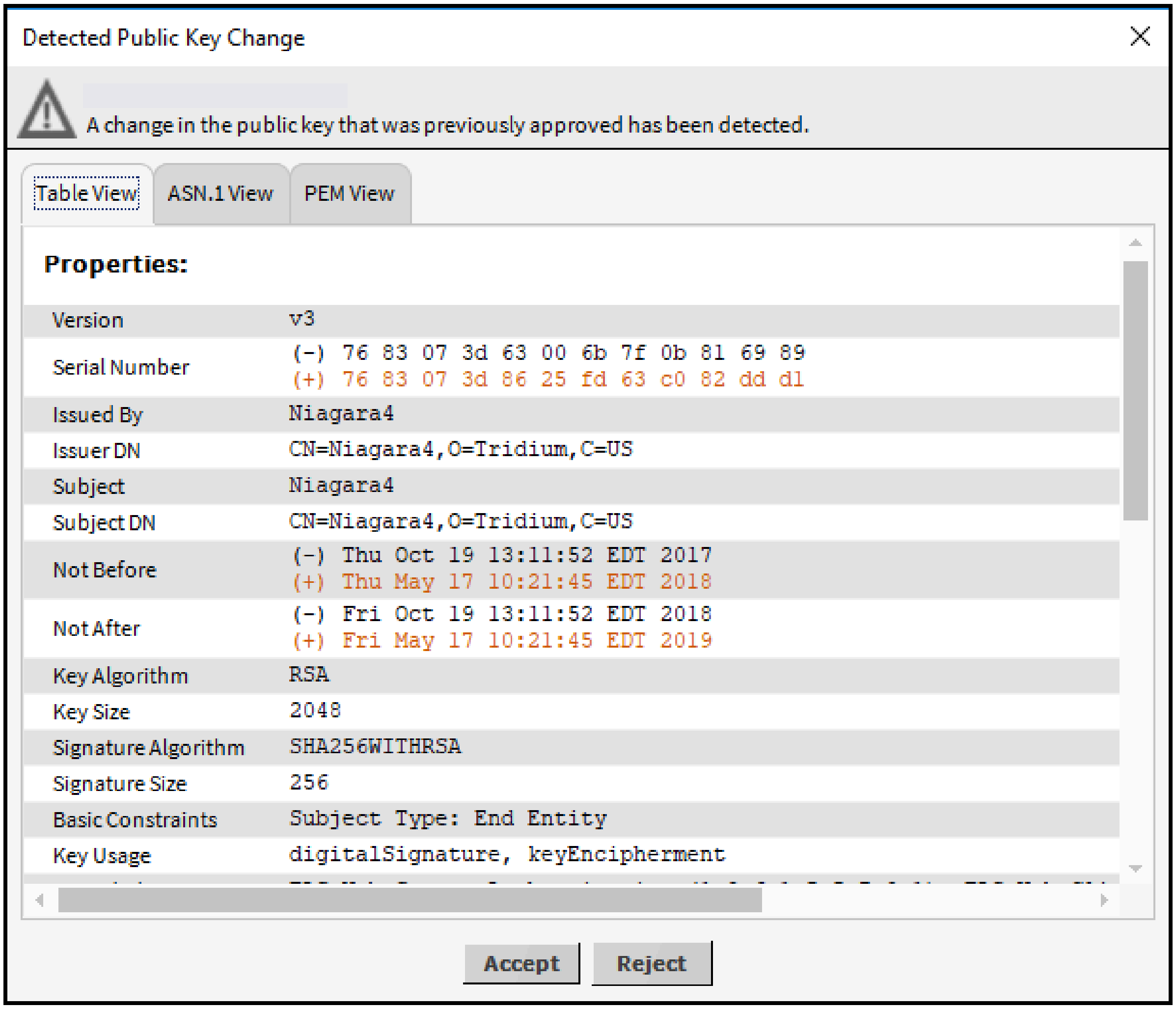
Host: IP 172.31.66.10

Port: 4911

As the station starts, observe the Application Director log. Watch for errors and warnings.

Step 6. Select `Station TLS Connection` for **`Type`**, enter the **`Host IP`**, and click **OK**.

The system may open the **Detected Public Key Change** window.



Detected Public Key Change

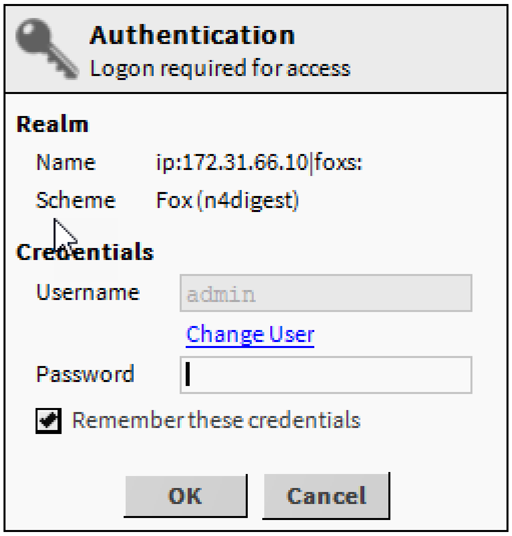
A change in the public key that was previously approved has been detected.

Properties:

Version	v3
Serial Number	(-) 76 83 07 3d 63 00 6b 7f 0b 81 69 89 (+) 76 83 07 3d 86 25 fd 63 c0 82 dd d1
Issued By	Niagara4
Issuer DN	CN=Niagara4,O=Tridium,C=US
Subject	Niagara4
Subject DN	CN=Niagara4,O=Tridium,C=US
Not Before	(-) Thu Oct 19 13:11:52 EDT 2017 (+) Thu May 17 10:21:45 EDT 2018
Not After	(-) Fri Oct 19 13:11:52 EDT 2018 (+) Fri May 17 10:21:45 EDT 2019
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	SHA256WITHRSA
Signature Size	256
Basic Constraints	Subject Type: End Entity
Key Usage	digitalSignature, keyEncipherment

Step 7. Click **Accept**.

The **Authentication** window opens.



Authentication
Logon required for access

Realm

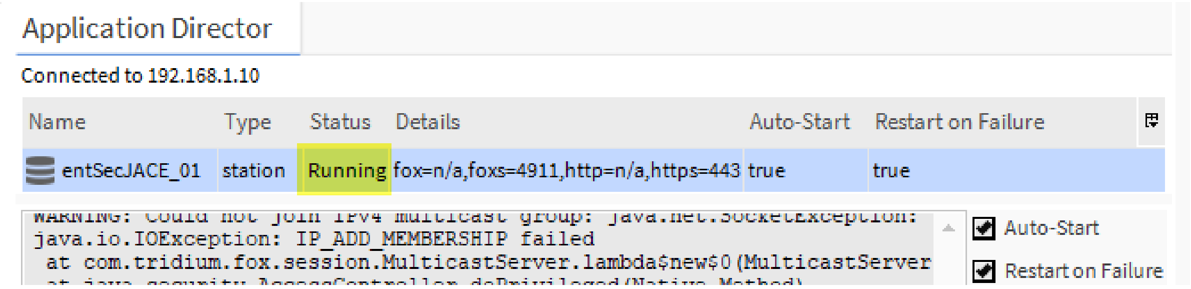
Name ip:172.31.66.10|foxs:
Scheme Fox (n4digest)

Credentials

Username admin

Password
☑ Remember these credentials

The default **`Username`** is `admin` , and the factory default **`Password`** is `Admin12345` .



Application Director

Connected to 192.168.1.10

Name	Type	Status	Details	Auto-Start	Restart on Failure
entSecJACE_01	station	Running	fox=n/a,foxs=4911,http=n/a,https=443	true	true

```
WARNING: Could not join IPv4 multicast group: java.net.SocketException:
java.io.IOException: IP_ADD_MEMBERSHIP failed
 at com.tridium.fox.session.MulticastServer.lambda$new$0(MulticastServer
 at java.security.AccessController.doPrivileged(Native Method)
```

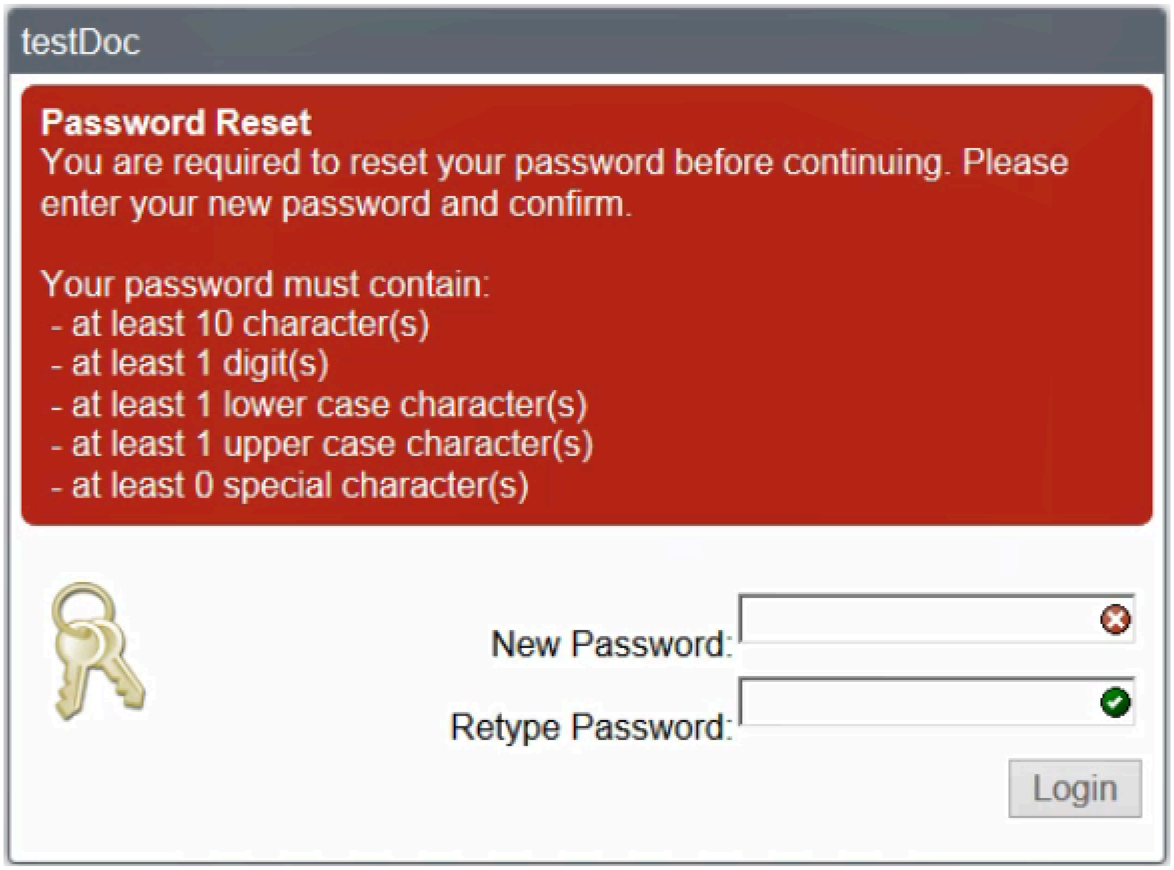
☑ Auto-Start
☑ Restart on Failure

Auto-Start enabled ensures that the station restarts after stopping. A Status of Running indicates that you can connect to the station using the web UI.

Step 8. Do one of the following:

- If you are logging in to this station for the first time, enter the default password, if enabled, disable **`Remember these credentials`**, and click OK.
- If you already changed the password using the web UI, enter your password.

If you entered the default password, the system displays the Password Reset window.



testDoc

Password Reset
You are required to reset your password before continuing. Please enter your new password and confirm.

Your password must contain:
- at least 10 character(s)
- at least 1 digit(s)
- at least 1 lower case character(s)
- at least 1 upper case character(s)
- at least 0 special character(s)

Step 9. Change the default password to a new, strong password that includes special characters, numbers, and lowercase and uppercase letters.

IMPORTANT: The password provides the front line of protection for your controller station. Share this credential with only those who need to know. Change the password on a regular basis. Store it in a secure location, preferably under lock and key.

Once you have created your own unique password, the next time you log in to the station you can enable `Remember these credentials` before you click OK.

The **Station Summary** view opens. This view indicates that you are connected to the controller station.

Step10. As the station starts, observe the Application Director log. Watch for errors and warnings.

Chapter 6. Controller setup, users, access rights, and schedules

This work takes place in a controller using the web UI.

The options configured in this chapter prepare the way for configuring devices in the next chapter.

Best Practice: During station configuration it is a good idea to save a station frequently. To save the current station, click **Miscellaneous** > **Controller Maintenance**, and click **Save Station**.

Connecting to a station using Workbench

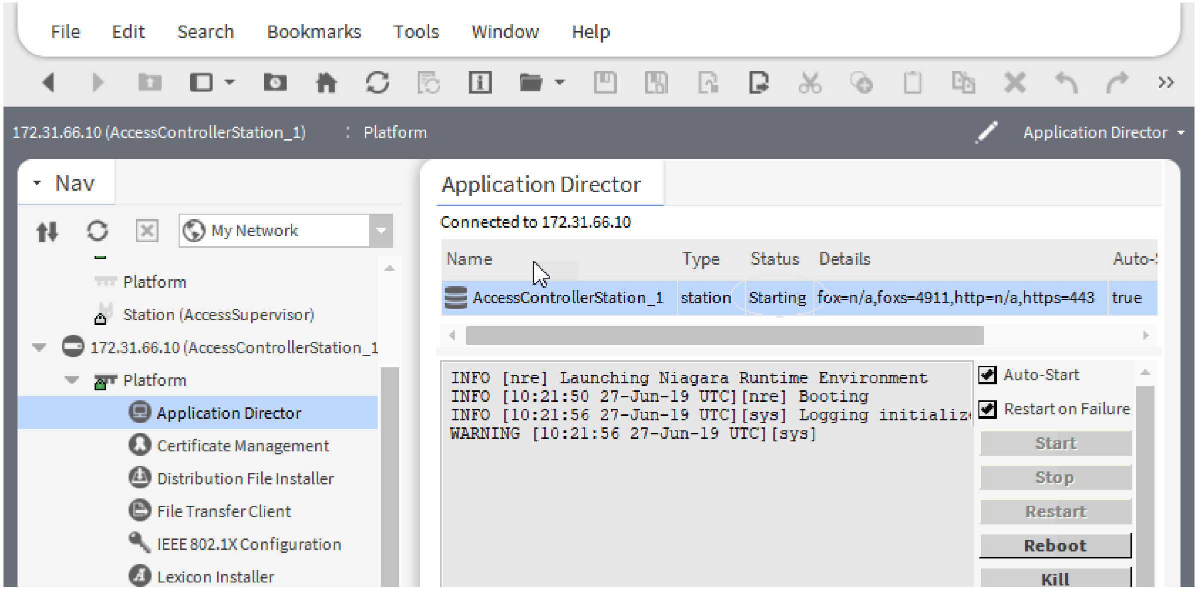
There are any number of reasons that a station may be idle. A common troubleshooting step is to open the Application Director and confirm that the station is running. If not, follow this procedure, which works the same for a Supervisor or a remote controller station.

Prerequisites:
The platform connection is open.

Step 1. Open the Application Director tool. (One way to do this is to right-click Platform and click **Views** > **Application Director**.)

Step 2. Stop any other stations.

Step 3. Select the station to start and click the **Start** button.



Connected to 172.31.66.10

Name	Type	Status	Details	Auto-
AccessControllerStation_1	station	Starting	fox=n/a,foxs=4911,http=n/a,https=443	true

```
INFO [nre] Launching Niagara Runtime Environment
INFO [10:21:50 27-Jun-19 UTC][nre] Booting
INFO [10:21:56 27-Jun-19 UTC][sys] Logging initializ
WARNING [10:21:56 27-Jun-19 UTC][sys]
```

☑ Auto-Start
☑ Restart on Failure

Step 4. Notice any errors and warnings as the station starts.

Step 5. Confirm that the station has started (Status reports `Running`).

Step 6. To configure the station to start automatically in the event of an unexpected failure, enable the **`Auto-Start`** property.

`Auto-Start`

- If the electrical grid drops power to the building, an UPS (Uninterruptible Power Supply) or other backup battery can maintain power to the controller and its access network as long as is practical.
- If an emergency generator starts, the controller, access network, door locks and sensors should be powered by critical circuits to the extent that the company considers physical security to be a priority.
- If power to the controller ultimately fails, the system backs up the station automatically.
- When power is restored, the platform should automatically start the station and restore physical security to the building (unless the building's occupants over-road the door locks) with no operator action.

`Restart on Failure`

- If the station fails, it automatically attempts to restart.
- A **`Failure Reboot Limit`** (defaults to three attempts) defines how many times a station attempts to restart within a specific **`Failure Reboot Limit Period`** (defaults to 10 minutes). You can configure both.

Connecting to the controller station using the web UI

This procedure documents logging in to a controller station for the first time or after upgrading software.

Prerequisites:
The station has been commissioned and is running. You are using the web UI.

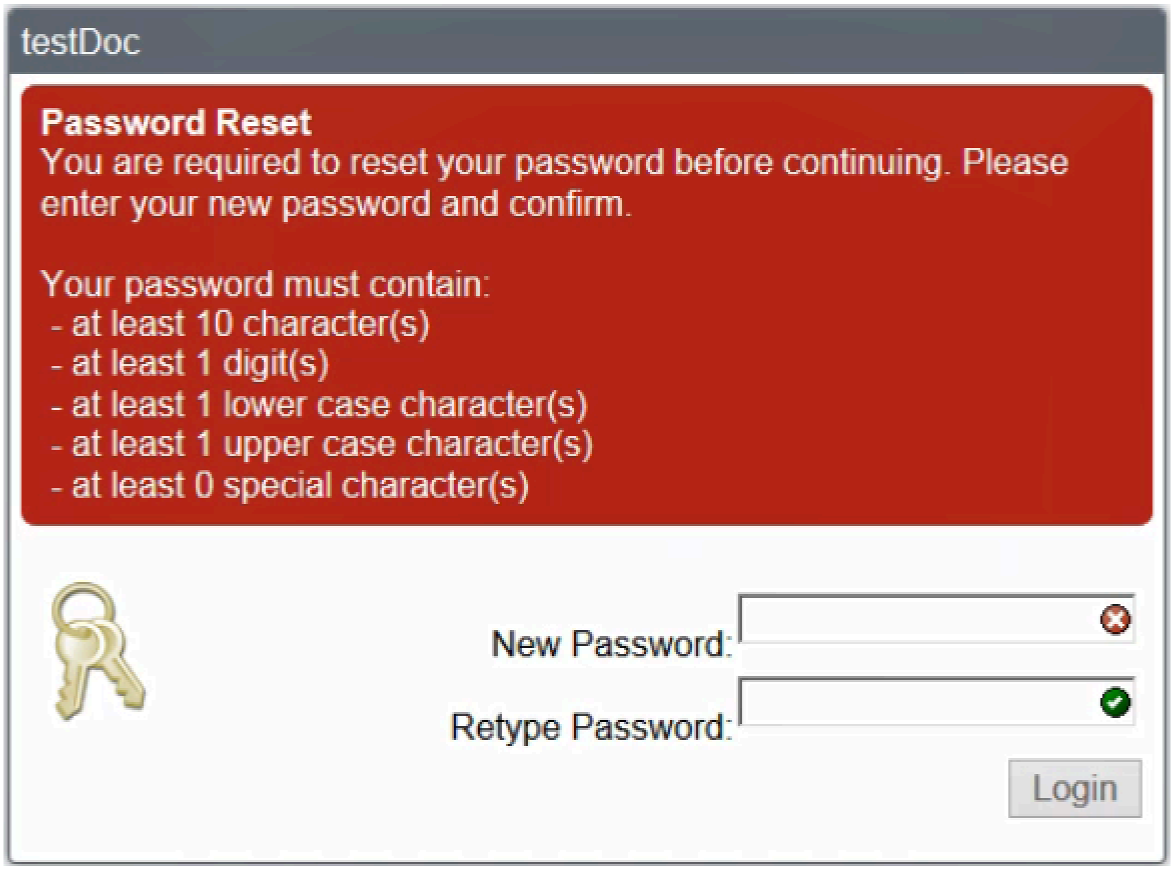
Step 1. Open a supported web browser.

Step 2. In the address bar, type the address of the remote controller (the default IP address is: `https://192.168.1.120`) and press the **Enter**.
The **Login** window opens. The **`Username`** defaults to `admin` . The password defaults to `Admin12345`.

Step 3. Do one of the following:

- If you are logging in to this station for the first time, and did not connect to the station using Workbench, enter the factory default **`Password`**, if enabled, disable **`Remember these credentials`**, and click **OK**.
- If you already logged in to the station using Workbench and changed the password, enter your password.

If you entered the default password, the system displays the Password Reset window.



testDoc

Password Reset
You are required to reset your password before continuing. Please enter your new password and confirm.

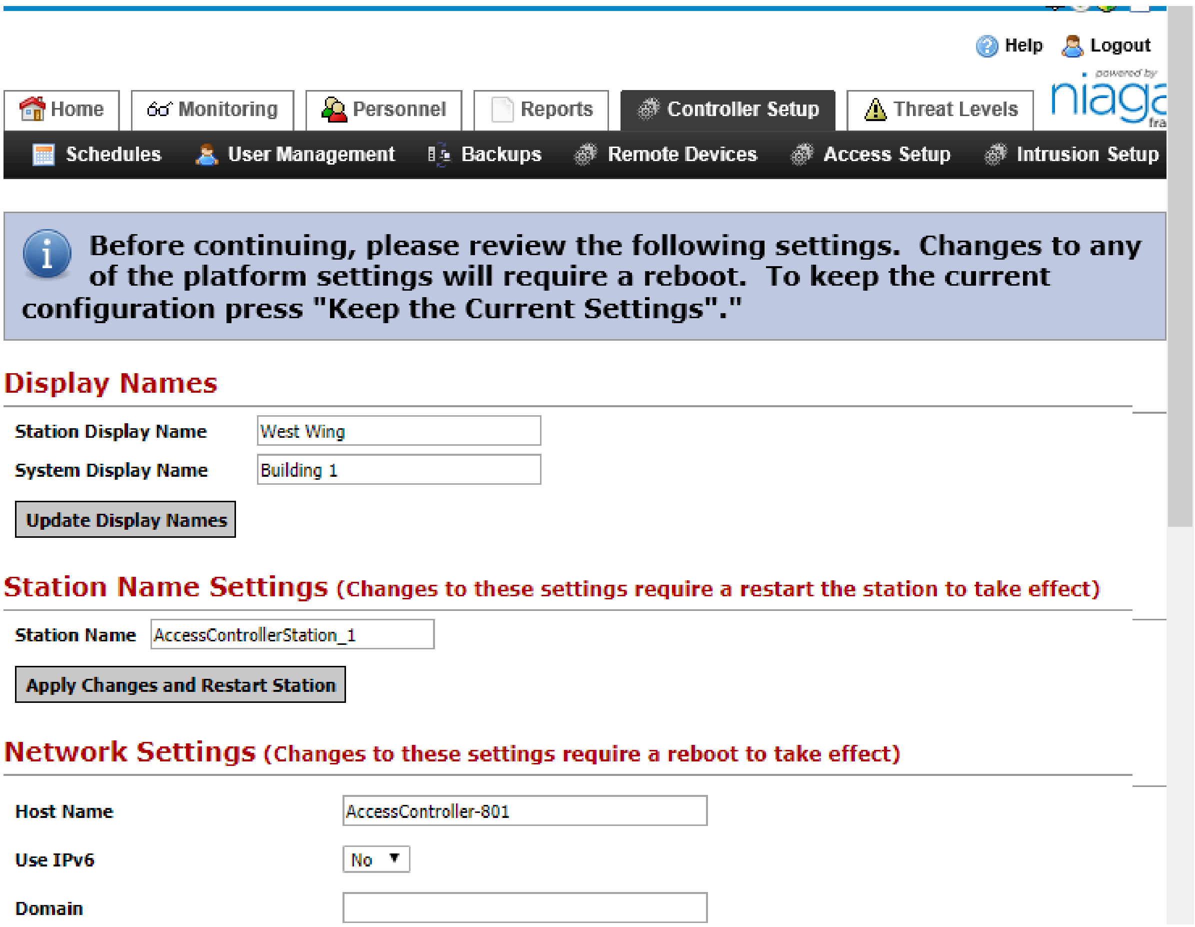
Your password must contain:
- at least 10 character(s)
- at least 1 digit(s)
- at least 1 lower case character(s)
- at least 1 upper case character(s)
- at least 0 special character(s)

Step 4. Change the default password to a new, strong password that includes special characters, numbers, and lowercase and uppercase letters.

IMPORTANT: The password provides the front line of protection for your controller station. Share this credential with only those who need to know. Change the password on a regular basis. Store it in a secure location, preferably under lock and key.

Once you have created your own unique password, the next time you log in to the station you can enable `Remember these credentials` before you click OK.

The interface opens and you are asked to confirm the station and system display name and the network settings.



Before continuing, please review the following settings. Changes to any of the platform settings will require a reboot. To keep the current configuration press "Keep the Current Settings".

Display Names

Station Display Name: West Wing

System Display Name: Building 1

Update Display Names

Station Name Settings (Changes to these settings require a restart the station to take effect)

Station Name: AccessControllerStation_1

Apply Changes and Restart Station

Network Settings (Changes to these settings require a reboot to take effect)

Host Name: AccessController-801

Use IPv6: No

Domain:

The Station and System names display in the top right corner of the web UI. For example: the station name might be: `Second Floor`, and the system name: `Building 10`. You can change these values later by navigating to **Controller (System) Setup** > **Network TCP/IP Settings**. The *Reference* explains the many properties you can configure in this view.

Step 5. Scroll down and configure any of the many properties, then click **Apply Changes and Reboot** (at the bottom of the page), and wait for the station to restart.
If the station does not restart, go back to Workbench, confirm that Auto-Start is enabled, click Start, and log in using the web UI again.

Step 6. If the Guided Setup Tour does not open, and you wish to use it, click the **Guide** button at the top of the **Home** view.
The **Guided Setup Tour** window opens.

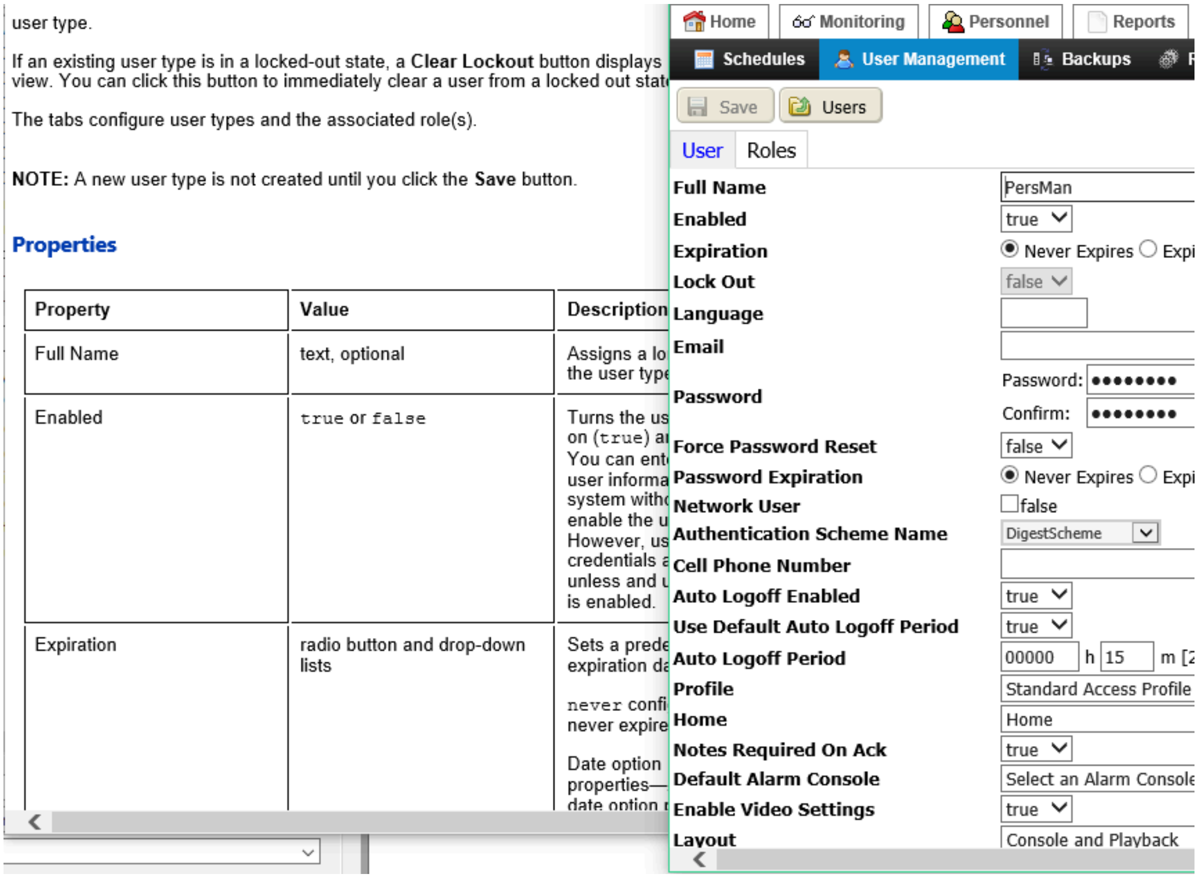
Accessing the help system

Help is available on each view. This procedure demonstrates how to open a second pop-up window for the help topic while retaining the view.

Prerequisites:
You are accessing a controller station using the web UI.

Step 1. Click the **Help** icon in the upper right corner of the screen.
The help topic for the view replaces the view.

Step 2. Click the popup icon ( ) in the upper right corner of the screen.
This opens a new browser window for the web UI that contains the help text.



user type.

If an existing user type is in a locked-out state, a **Clear Lockout** button displays view. You can click this button to immediately clear a user from a locked out stat

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
Full Name	text, optional	Assigns a lo the user type
Enabled	`true` or `false`	Turns the us on (`true`) a You can ent user informa system with enable the u However, us credentials a unless and u is enabled.
Expiration	radio button and drop-down lists	Sets a prede expiration d `never` confi never expire Date option properties— date option

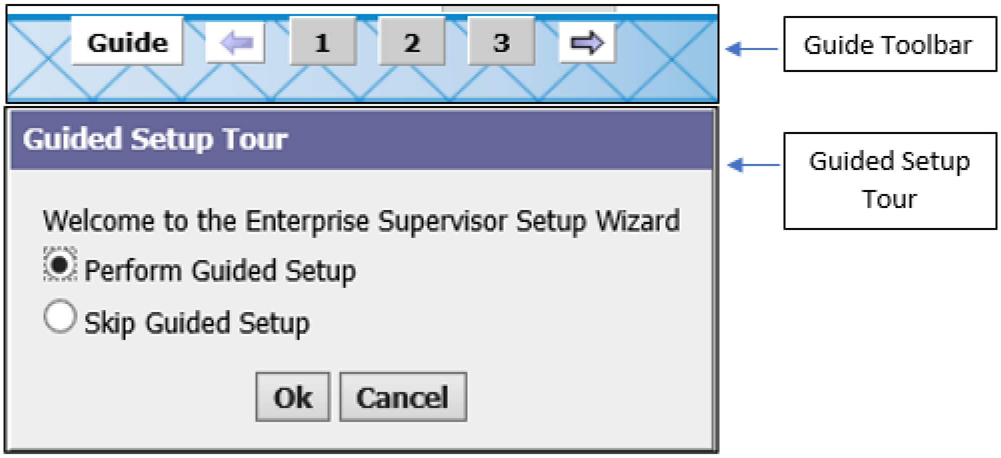
Full Name	PersMan
Enabled	true
Expiration	● Never Expires ○ Expi
Lock Out	false
Language	
Email	
Password	Password: •••••••• Confirm: ••••••••
Force Password Reset	false
Password Expiration	● Never Expires ○ Expi
Network User	□false
Authentication Scheme Name	DigestScheme
Cell Phone Number	
Auto Logoff Enabled	true
Use Default Auto Logoff Period	true
Auto Logoff Period	00000 h 15 m [2
Profile	Standard Access Profile
Home	Home
Notes Required On Ack	true
Default Alarm Console	Select an Alarm Console
Enable Video Settings	true
Layout	Console and Playback

Step 3. Go back to the primary view and click the browser’s go-back button or otherwise navigate to the view you need.
The browser displays the view while the help topic remains open in the pop-up window.

Guided Setup Wizard

This utility is comprised of a Guide Toolbar and a series of windows designed to direct you through the initial setup process.

Figure 8. Guided Setup Wizard



Welcome to the Enterprise Supervisor Setup Wizard

● Perform Guided Setup

○ Skip Guided Setup

Guide Toolbar

Guided Setup Tour

The Guided Setup Wizard serves as a checklist and navigation aid. It directs you to the proper screen for setting up your system. It does not assign any values or configure properties automatically for you. For example, on initial setup, you are directed to the Access Device Manager view in step three of the Guided Setup Wizard. If no modules are in your database, you must discover and add modules, as required, before proceeding. As you complete each step and save changes, re-open the wizard and note that the step is completed. If you have questions about the setup process or any of the properties, refer to the procedures in this section.

As you complete each step of the setup, **Step Indicator** buttons change color to indicate the status of the step relative to the completion of the Guided Setup Wizard.

You can cancel the Guided Setup Wizard at any time by using one of the following three methods.

- Click the **Guide** button and select the `Skip Guided Setup` option in the Guided Setup Welcome window.
- In the final step, select the `...Completed` option and click **Ok**.
- Set the **`Show Guided Tour`** property to `true` (to display) or to `false` (to hide) the Guided Setup Wizard and Guide Toolbar. This property is located here:
  - Supervisor: **System Setup** > **Miscellaneous** > **Server Maintenance**
  - Controller: **System Setup** > **Miscellaneous** > **Controller Maintenance**

Each step of the wizard process is tracked by monitoring its status. Each step may be in one of the following four states:

- Next required step

  Since the steps must be accomplished in a sequential order, only one step is available at any point during the Guided Setup Wizard process. The Guide toolbar indicates the next required step by the white color of the step indicator button.
- Step initiated but not complete

  The system initiates a step when you access a view Guide window. The step indicator button turns yellow when the step is initiated and stays yellow until the "`...Completed`" option is selected from the associated Guide window.
- Step completed

Completed steps display as green step indicator buttons. A step must be completed before you can go to the next step.

NOTE: A step is completed when you select the ...Completed option in the associated step window. There is no programmatic verification that you performed a step.

- Step not available

  A step is unavailable until you complete the previous step. The step indicator button displays as gray (or dimmed) when the step is not available.

Starting the Guided Setup Tour

The Guided Setup Tour serves as a checklist to make sure that you configure all the important station components. Rather than use the checklist, you can configure each component individually. The advantage of the tour for first-time users is that using it helps you remember what needs configuring.

Prerequisites:
The **`Show Guided Tour`** property is set to `true` in the **Controller Maintenance** window (**Controller Setup** > **Miscellaneous** > **Controller Maintenance**.

Step 1. If the tour does not open automatically, you can start it by clicking the **Guide** button at the top of the view.
The **Guided Setup Tour** window opens.

Step 2. Confirm that `Perform Guided Setup` is enabled and click **OK**.
The background for the **Guide** button at the top of the view turns green and the background of the **1** indicator turns white to indicate that you are on Step 1. This is an important step because this is where you set up the station password for the admin user.

Step 3. Ensure that `Go to Change Password` is enabled and click **OK**.
The wizard navigates to **Controller Setup** > **User Management** , and opens the Password view.

Step 4. Enter the current password, create a strong new password, and click **Save**.
The **Password Changed** window opens.

Step 5. Click **done**.
The background of the step **1** button at the top of the view turns yellow.

Step 6. To restart the station, click **Ok**.
The station restarts. This could take a couple minutes. If you have the Application Director in Workbench open, you can watch it restart. When Status reports `Running`, you can log in again to the station using the web UI.

Step 7. Log in to the station and, to continue the rest of the Guided Setup Tour, click step **2**.
The tour opens the **Setup NTPPlatformService TimeServers** window.

Step 8. Continue with the rest of the steps, which guide you to:

- Step 4: Add Connected Modules with Network Discovery
- Step 5: Set Up Schedules for Card Access
- Step 6: Set Up Wiegand Formats
- Step 7: Create Tenants
- Step 8: Create Access Rights
- Steps 9, 10 and 11: Set Up Personnel and Badges
- Step 12: Create New System Users

To continue after each step, click the yellow step button.

One of the options when you get to step 13 is Save System Configuration. When you click Save Configuration Complete, the tour opens the 14th step for viewing the End User License Agreement (EULA). Step 15 is for viewing third-party licenses. It provides the option to `End Guided Wizard Setup`.

Step 9. Click `End Guided Wizard Setup` and click **OK**.
If you configured properties at each step of the tour, your station is well prepared to begin operations.

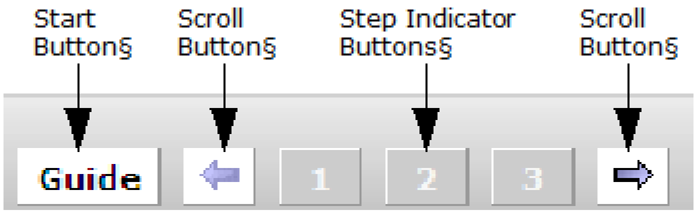
Result

The rest of this guide provides tasks in a similar order with the exception of creating personnel records and badges, which are documented in the *Facility Manager's Guide*.

About the Guided setup wizard Toolbar

The Guide Toolbar appears, by default, the first time you log in to the system.

Figure 9. Guide Toolbar controls and indicators



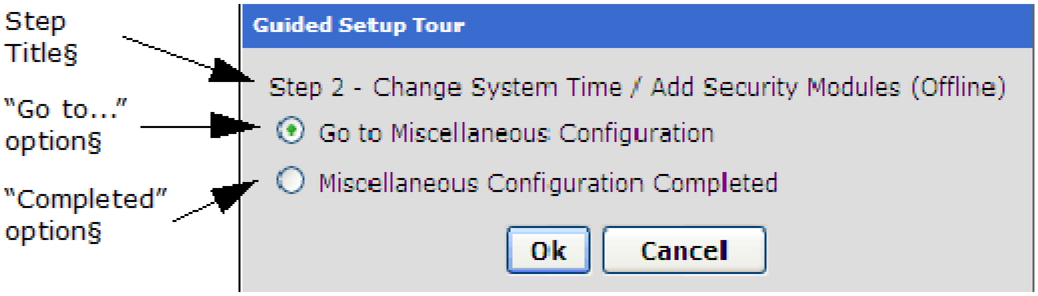
This toolbar is located at the top of the application user interface (on the Title Bar) and displays control and indicator buttons. These controls and indicators allow you to navigate and visually track the progress of the guided setup. The following list describes each Guide Toolbar control button:

- Guide Start initiates the Guided Setup Wizard by opening the Guided Setup Welcome window. This button may be white or green. white indicates that the guided setup process has not started yet. Green indicates that the guided setup process has started, and is not yet complete.
- Scroll buttons are located to the left and right of the **Step Indicator** buttons. The Scroll buttons move the visible step indicator buttons left and right so that you can view any set of three contiguous buttons.
- **Step Indicator** buttons, numbered: 1-11 or 1-12, indicate the step number and window. Each button may display any one of four possible colors to indicate the status of the associated step.
  - 10 White indicates that this is the next step to be taken.
  - 3 Yellow indicates that the step has been initiated but not completed.
  - 2 Green indicates that the step has been completed.
  - 4 Gray indicates that the step is not available.

About the Guided setup wizard windows

Guide windows display when you initiate a step in the Guided Setup Wizard.

Figure 10. Guide window



Guided Setup Tour

Step 2 - Change System Time / Add Security Modules (Offline)

● Go to Miscellaneous Configuration

○ Miscellaneous Configuration Completed

Each window has an instructional title that describes the step and two options:

- `Go to ...` displays the view associated with the next step that needs to be performed in the setup.
- `... Completed` displays the window for the next step in the Guided Setup Wizard.

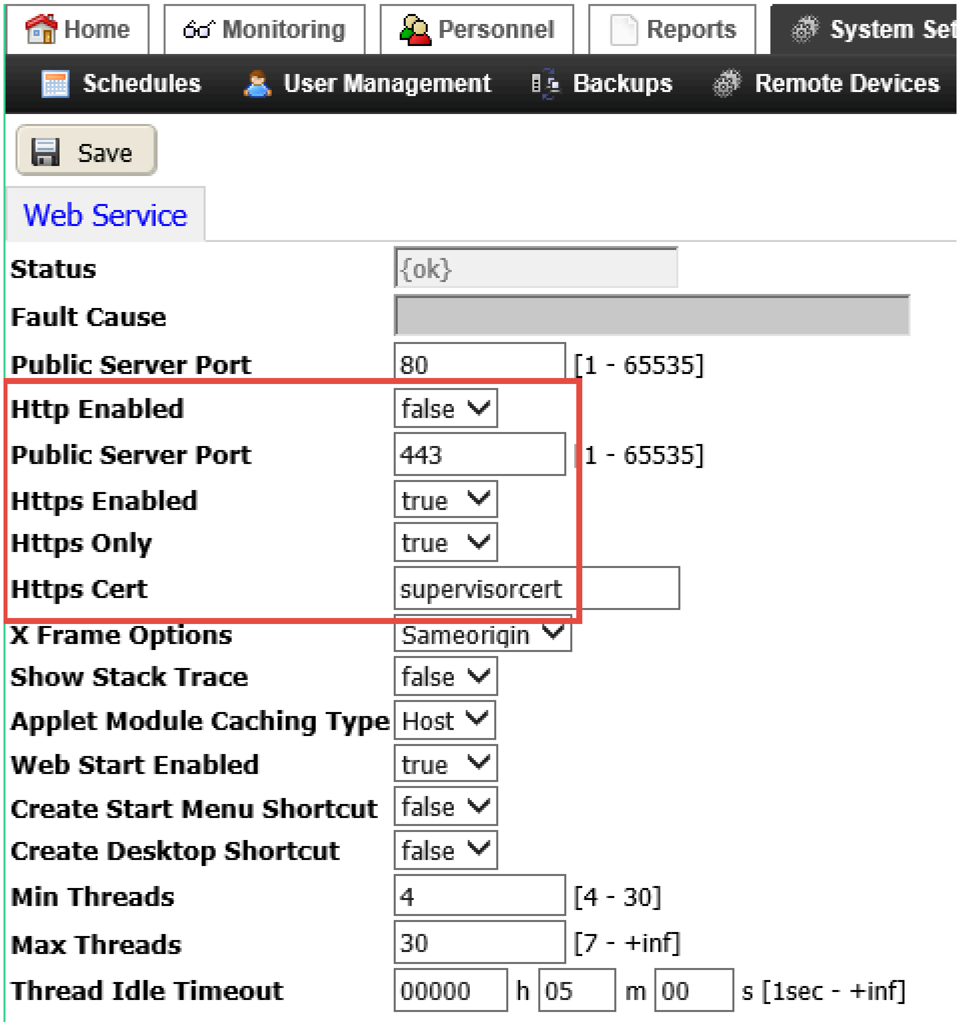
Configuring a secure browser connection

Secure communication with the browser is controlled through the Web Service.

Prerequisites:
You are using the Web UI.

Step 1. To configure a secure connection through a browser, access the Web Service by clicking **Controller Setup** > **Miscellaneous** > **Web Service**.

The Web Service properties tab opens.



Status	{ok}
Fault Cause	
Public Server Port	80 [1 - 65535]
Http Enabled	false
Public Server Port	443 [1 - 65535]
Https Enabled	true
Https Only	true
Https Cert	supervisorcert
X Frame Options	Sameorigin
Show Stack Trace	false
Applet Module Caching Type	Host
Web Start Enabled	true
Create Start Menu Shortcut	false
Create Desktop Shortcut	false
Min Threads	4 [4 - 30]
Max Threads	30 [7 - +inf]
Thread Idle Timeout	00000 h 05 m 00 s [1sec - +inf]

Step 2. Set **Http Enabled** to false, **Https Enabled** to true, and **Https Only** to true.
If you are upgrading your installation, you may have pointers to old Http ports. When **Https Only** is set to true, the system automatically redirects any Http connections to secure connections (Https). This saves having to manually change each occurrence of an Http port in legacy installations.

Step 3. Change **Https Cert** to identify the root CA-signed server certificate you created for this platform/station, and click **Save**.
When you enable Https in the Web Service, the system automatically enables Foxs in the Fox Service.

Step 4. If you did not import the company's root certificate into the browser's trust store, go back to the *Secure Communication* chapter and set it up.

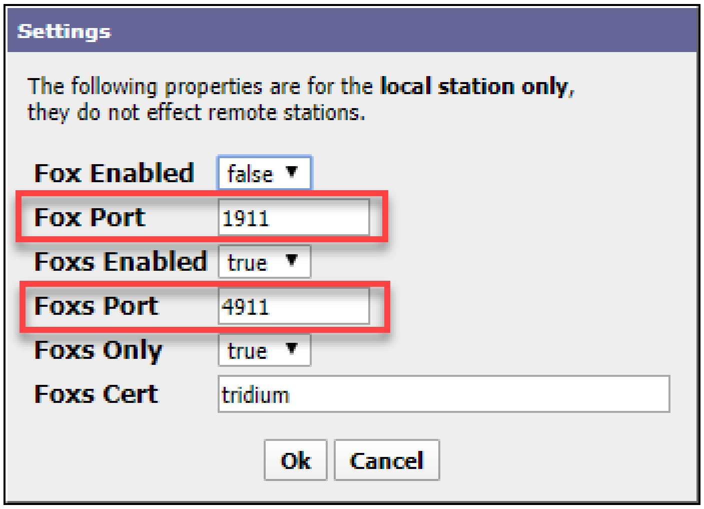
Result
Any communication using the browser is secure.

Configuring the platform/station's network connection

Establishing the connection between the controller platform/station and the local area network involves configuring the port and connection security.

Prerequisites:
You made a browser connection to the controller and are using the web UI.

Step 1. To access connections, click **Controller Setup** > **Remote Devices** > **Station Manager**, and click the settings icon (🔧).
The **Settings** window opens.



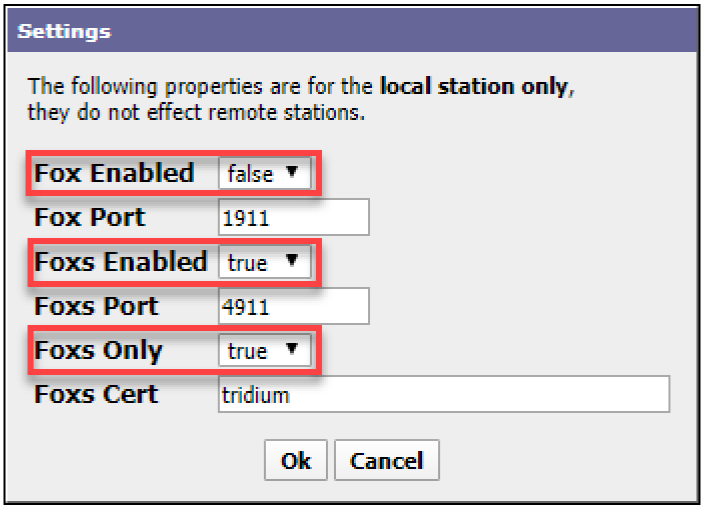
Settings

The following properties are for the **local station only**, they do not effect remote stations.

Fox Enabled	false ▼
Fox Port	1911
Foxs Enabled	true ▼
Foxs Port	4911
Foxs Only	true ▼
Foxs Cert	tridium

Step 2. Configure the station’s `Fox Port` or `Foxs Port` based on whether or not the configuration requires security and fox streaming.
If your configuration uses fox streaming for video, this port (Fox or Foxs) should be different from the port used to connect a video device (camera, DVR, NVR or server) to the network. If your configuration does not use fox streaming, this port should be the same as the port used to connect the video device.

Step 3. To continue configuring a secure connection, confirm the following configuration:



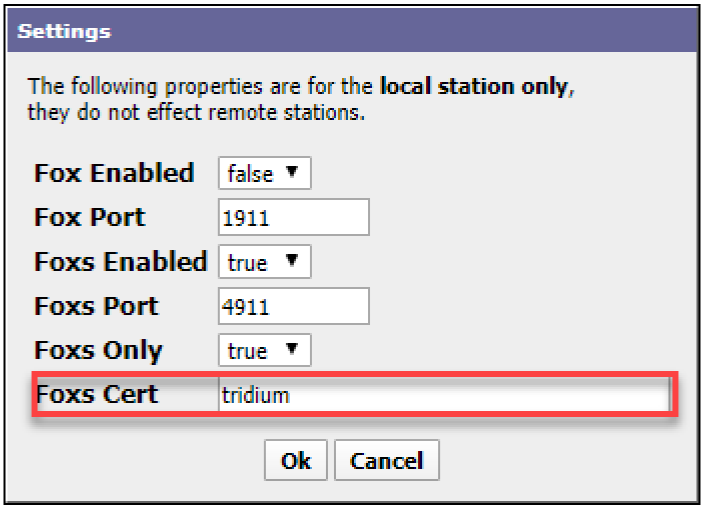
Settings

The following properties are for the **local station only**, they do not effect remote stations.

Fox Enabled	false ▼
Fox Port	1911
Foxs Enabled	true ▼
Foxs Port	4911
Foxs Only	true ▼
Foxs Cert	tridium

Step 4. For `Foxs Cert`, enter the platform/station’s server certificate.

Foxs Cert is the last property in the **Settings** window.



Settings

The following properties are for the **local station only**, they do not effect remote stations.

Fox Enabled: false
Fox Port: 1911
Foxs Enabled: true
Foxs Port: 4911
Foxs Only: true
Foxs Cert: tridium

The `tridium` certificate is the default, self-signed certificate. For maximum security store a unique server certificate in each controller/station's User Key Store that was signed by a root CA certificate in the User Trust Store.

Defining a display name for a controller station

Every station on the network requires a unique IP Address. In addition to this address (a series of numbers), each station can have a unique Display Name and a unique Station Name. The station's Display Name adds an easily-understood text name. Its Station Name can be more technical using industry abbreviations, acronyms, and labels. If the system has a single controller, the default Station Name is sufficient. In a company-wide installation, a best practice is to give each station (controller and Supervisor) meaningful names that conform to a standard naming convention.

Step 1. Click **Controller Setup** > **Miscellaneous** > **Network TCP/IP Settings**.

Step 2. Enter a descriptive **Station Display Name** and a **System Display Name**.
The **System Display Name** refers to the whole installation. Often, this is the company name or system name for the whole company. These names should differentiate controllers from one another and from one or more Supervisor stations.

Step 3. Click the **Apply Changes and Reboot** button. Allow the platform to restart.

Setting the date and time

This procedure configures the platform date and time . Both platforms (Supervisor and controller) require this configuration step.

Prerequisites:
You are working in web UI.

Step 1. Expand **Controller (System) Setup** > **Miscellaneous**, and click **System Date Time**.

Step 2. Click the check-box next to **Change System Time**.
The software warns you that saving time zone changes requires a platform restart. The system requires this restart even if the time differential does not change. For example, changing from America/New York to America/Toronto requires a restart, even though the current time may be the same in both places.

Step 3. To activate the date and time properties, click **Ok**.

Step 4. Configure the properties and click **Save**.
The Supervisor PC or remote controller restarts.

User management

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

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

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

Roles

Roles define a set of permissions or privileges that control the system functions available to specific users. A user may have multiple roles. Every user needs at least one role.

The system provides default roles for which permissions are already configured.

- The *Admin* role has full system privileges and can see all views and administrator-only functions including those involving controller setup, network discovery, and object linking.
- The *Badge Operator* role may handle only badge administration, view reports and create custom reports, but cannot configure properties, view or acknowledge alarms.
- The *Maintenance* role includes the ability to view hardware reports and perform system maintenance tasks, such as configuring remote controllers, creating and updating graphics, as well as adding and editing user-role information.
- The primary task of the *Operator* role is to monitor and acknowledge alarms using the alarm console. The operator can view, but not edit, certain other system and personnel reports.
- The *Personnel Management* role provides access to tenant and personnel views. This user can edit personnel and badge management properties and has read-only access to access right and tenant management properties.

The following tables summarize the features each default role can access.

Table 14. Monitoring

Role: Function:	**Admin**	**Badge Operator**	**Maintenance**	**Operator**	**Personnel Management**
Alarm Console	X	X	X	X	
Activity Monitor	X	X	X	X	
Video Monitoring, Surveillance Viewer	X		X	X	
Video Monitoring, Playback Viewer	X		X	X	

Table 15. Personnel

Role: Function:	**Admin**	**Badge Operator**	**Maintenance**	**Operator**	**Personnel Management**
People	X	X	X	X	X

Role:					
Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Badges	X	X	X	X	X
Access Rights	X	X	X	X	X
Tenants	X	X	X	X	X
Additional Personnel Data	X	X	X	X	

Table 16. Reports

Role:					
Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Access History	X	X	X	X	
Alarm History	X	X	X	X	
Intrusion History	X	X	X	X	
Attendance History	X	X	X	X	
Audit History	X	X	X	X	
Log history	X	X	X	X	
Hardware Reports, Doors	X	X	X		
Hardware Reports, Readers	X	X	X		
Hardware Reports, Inputs	X	X	X		
Hardware Reports, Outputs	X	X	X		
Hardware Reports, Elevators (controller only)	X	X	X		
Hardware Reports, Remote Modules	X	X	X		
Hardware Reports, Intrusion Displays	X	X	X		
Hardware Reports, BACnet Points	X		X		
LDAP Audit History	X	X	X		
Miscellaneous Reports, Person Access Right Report	X	X	X	X	
Miscellaneous Reports, Person Reader Report	X	X	X	X	
Miscellaneous Reports, Access Right Reader Report	X	X	X	X	
Miscellaneous Reports, Personnel Changes	X	X	X	X	

Table 17. Controller (System) Setup

Role:					
Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Schedules, Schedules	X	X	X	X	
Schedules, Calendar Schedules	X	X	X	X	
User Management, Users	X		X	X	
User Management, Roles	X		X	X	
User Management, Change Password	X	X	X	X	X
Backups	X				

Table 18. Controller (System) Setup, Remote Devices

Role:					
Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Remote Drivers	X	X	X		
Remote Modules, Remote Module Setup (controller only)	X	X	X		

Role: Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Remote Modules, Remote Module Identification (controller only)	X	X	X		
Remote Modules, Access Network Setup (controller only)	X	X	X		
Niagara Integration IDs	X	X	X		
BACnet Network (controller only)	X	X	X		
BACnet BDT Manager (controller only)	X	X	X		
Station Manager	X	X	X		
Certificate Manager	X	X	X		

Table 19. Controller (System) Setup, Access Setup

Role: Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Access Zones	X	X	X	X	
Card Formats	X	X	X	X	
Access Control Setup	X	X	X	X	
Additional Personnel Entry	X		X		

Table 20. Controller (System) Setup, Intrusion Setup

Role: Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Intrusion PINs	X	X	X		
Intrusion Zones	X	X	X		
Intrusion Displays (controller only)	X	X	X		

Table 21. Controller (System) Setup, Alarm Setup

Role: Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Alarm Classes	X	X	X	X	
Alarm Instructions	X	X	X	X	
Alarm Count Relays (controller only)	X	X	X		
Email Accounts	X	X	X	X	
Email Recipients	X	X	X	X	
Station Recipients (controller only)	X	X	X		
Power Alarm Setup (controller only)	X	X	X		
Alarm Consoles	X	X	X	X	
Alarm Extensions	X	X	X	X	

Table 22. Controller (System) Setup, Miscellaneous

Role: Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Keypad Configuration	X		X		
PDF Styles	X	X	X		

Role: Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
License Manager	X		X		
Network TCP/IP Settings	X				
Controller Maintenance (controller only)	X	X	X		
Graphics, Graphics Management	X	X	X	X	
Graphics, Images	X	X	X	X	
Graphics, Navigation Groups	X	X	X	X	
Server Maintenance (Supervisor only)	X	X	X		
Configure Database	X	X	X		
Web Service	X		X		
Replication Service (Supervisor only)	X		X		
Jobs	X	X	X		
System Date Time	X		X		
End User License Agreement	X		X		
Third Party Licenses	X		X		
TimeServers Settings	X		X		

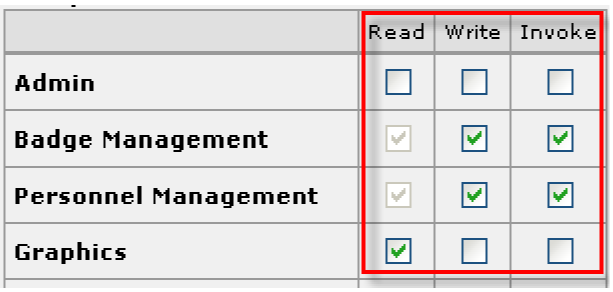
Table 23. Controller (System) Setup, Threat Levels

Role: Function:	Admin	Badge Operator	Maintenance	Operator	Personnel Management
Threat Level Groups	X	X	X	X	
Threat Level Setup	X	X	X	X	

Permissions

Permissions are the properties of role categories that can be configured.

Figure 11. Permissions in Edit Role view



	Read	Write	Invoke
Admin	☐	☐	☐
Badge Management	☑	☑	☑
Personnel Management	☑	☑	☑
Graphics	☑	☐	☐

You can grant or deny permissions for each category that is available to a role by selecting or clearing the appropriate option box for that permission. The following list describes each permission type:

- Read allows the user to view information of this category type. If this permission is denied, the user cannot see information that is assigned to this category.
- Write allows the user to view and modify information of this category type. If this permission is denied, the user may be able to see information that is assigned to this category (if Read permission is granted) but not modify it.
- Invoke relates to calling or activating a command or subroutine. Depending on the context, an invoke is

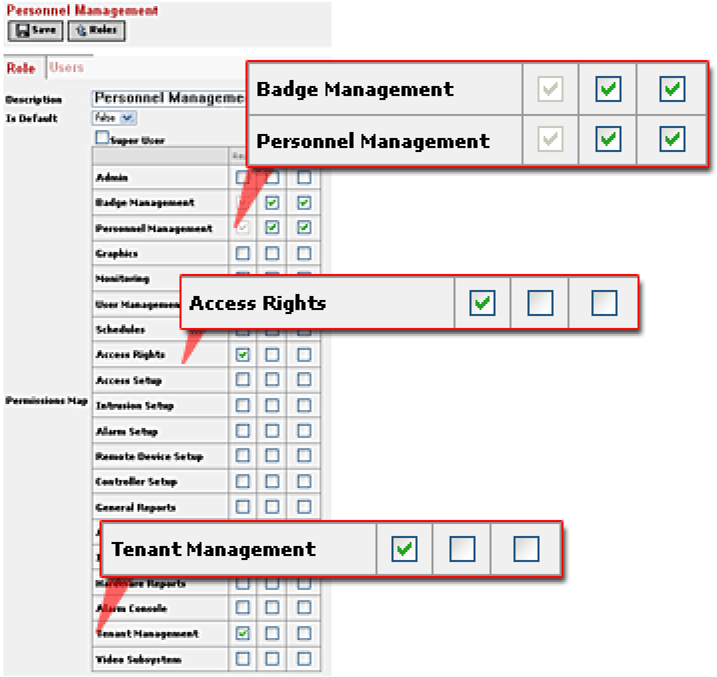
some sort of action, such as a ping, update, override, or door-unlock action. Different actions are available and based on the component, and many have no actions available.

When an invoke permission is granted for a certain category, the user can initiate an available action on the components assigned to the category. If an invoke permission is denied, the user cannot take any action on a component that is assigned to this category.

For example, a user with Alarm Console invoke permission can force clear an alarm. With only read and write permission, a user can acknowledge alarms, view and edit alarm notes and details, but cannot force clear.

For example, a personnel manager requires multiple role permissions.

Figure 12. Permissions granted to a personnel manager



Description: Personnel Manageme

Is Default: false

□ Super User

Permissions Map

Admin	□	□	□
Badge Management	☑	☑	☑
Personnel Management	☑	☑	☑
Graphics	□	□	□
Monitoring	□	□	□
User Management	□	□	□
Schedules	□	□	□
Access Rights	☑	□	□
Access Setup	□	□	□
Intrusion Setup	□	□	□
Alarm Setup	□	□	□
Remote Device Setup	□	□	□
Controller Setup	□	□	□
General Reports	□	□	□
Hardware Reports	□	□	□
Alarm Console	□	□	□
Tenant Management	☑	□	□
Video Subsystem	□	□	□

A Personnel Management role includes the following permissions assignments:

- Badge Management: Read, Write, Invoke
- Personnel Management: Read, Write, Invoke
- Access Rights: Read
- Tenant Management: Read

Creating (editing) a user role

A role assigned to a user (as that user's only role) controls what a user may view, such as personnel, badgeand access rightsviews. Typically, when you assign a role, you also choose the `Personnel Entry Access Profile` for the **`Profile`** property on the User tab. For convenience, you may use a personnel management role to filter views so that only personnel management views are available to a user.

Prerequisites:
You are working in a Supervisor station.

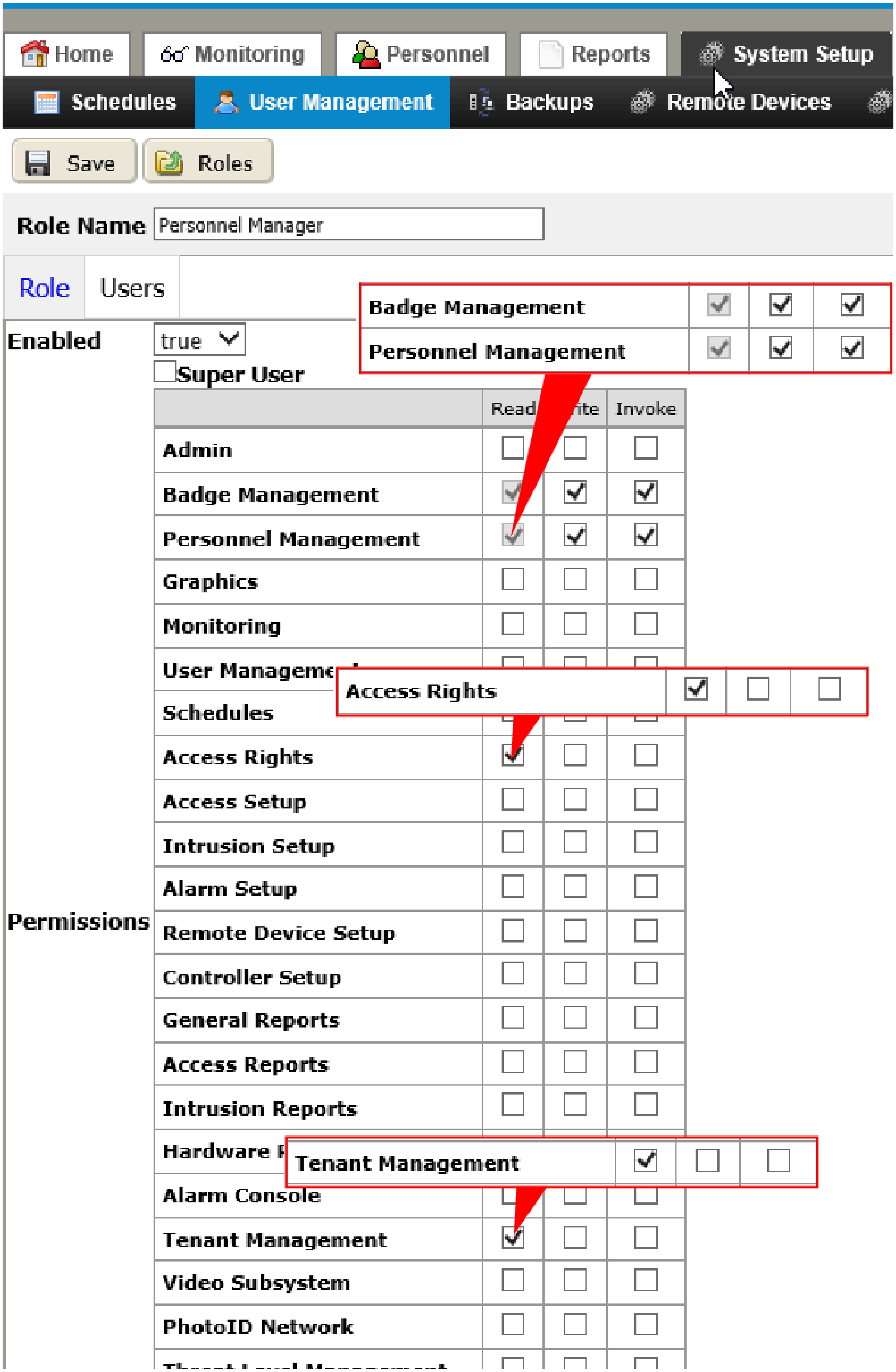
Step 1. From the main menu, click **System Setup** > **User Management** > **Roles**.

Step 2. To open the Add New Role view click the Add button (⊕) at the top of the view.

The add new role view opens. The **Role Name** property appears above the tabbed area.

Step 3. Use the **Role Name** property to assign a unique name to the role.

Step 4. Fill in the **Permissions** boxes to associate with the role and click **Save**.



Role Name: Personnel Manager

Enabled: true

□ Super User

Permissions

	Read	Write	Invoke
Admin	□	□	□
Badge Management	☑	☑	☑
Personnel Management	☑	☑	☑
Graphics	□	□	□
Monitoring	□	□	□
User Management	□	□	□
Schedules	□	□	□
Access Rights	☑	□	□
Access Setup	□	□	□
Intrusion Setup	□	□	□
Alarm Setup	□	□	□
Remote Device Setup	□	□	□
Controller Setup	□	□	□
General Reports	□	□	□
Access Reports	□	□	□
Intrusion Reports	□	□	□
Hardware R	□	□	□
Alarm Console	□	□	□
Tenant Management	☑	□	□
Video Subsystem	□	□	□
PhotoID Network	□	□	□
Threat Level Management	□	□	□

Badge Management	☑	☑	☑
Personnel Management	☑	☑	☑

Access Rights	☑	□	□

Tenant Management	☑	□	□

In this example, a Personnel Management role includes the following permissions assignments:

- Badge Management: Read, Write, Invoke.
- Personnel Management: Read, Write, Invoke.
- Access Rights: Read.
- Tenant Management: Read.

CAUTION: Be careful with selecting `Super User`. A person with this role has access to the entire system.

Creating (editing) a user and assigning a role

The term user refers to someone who is authorized to manage and configure the system. A user is also a person in the system. Other people who use the system to access the building are persons, not users.

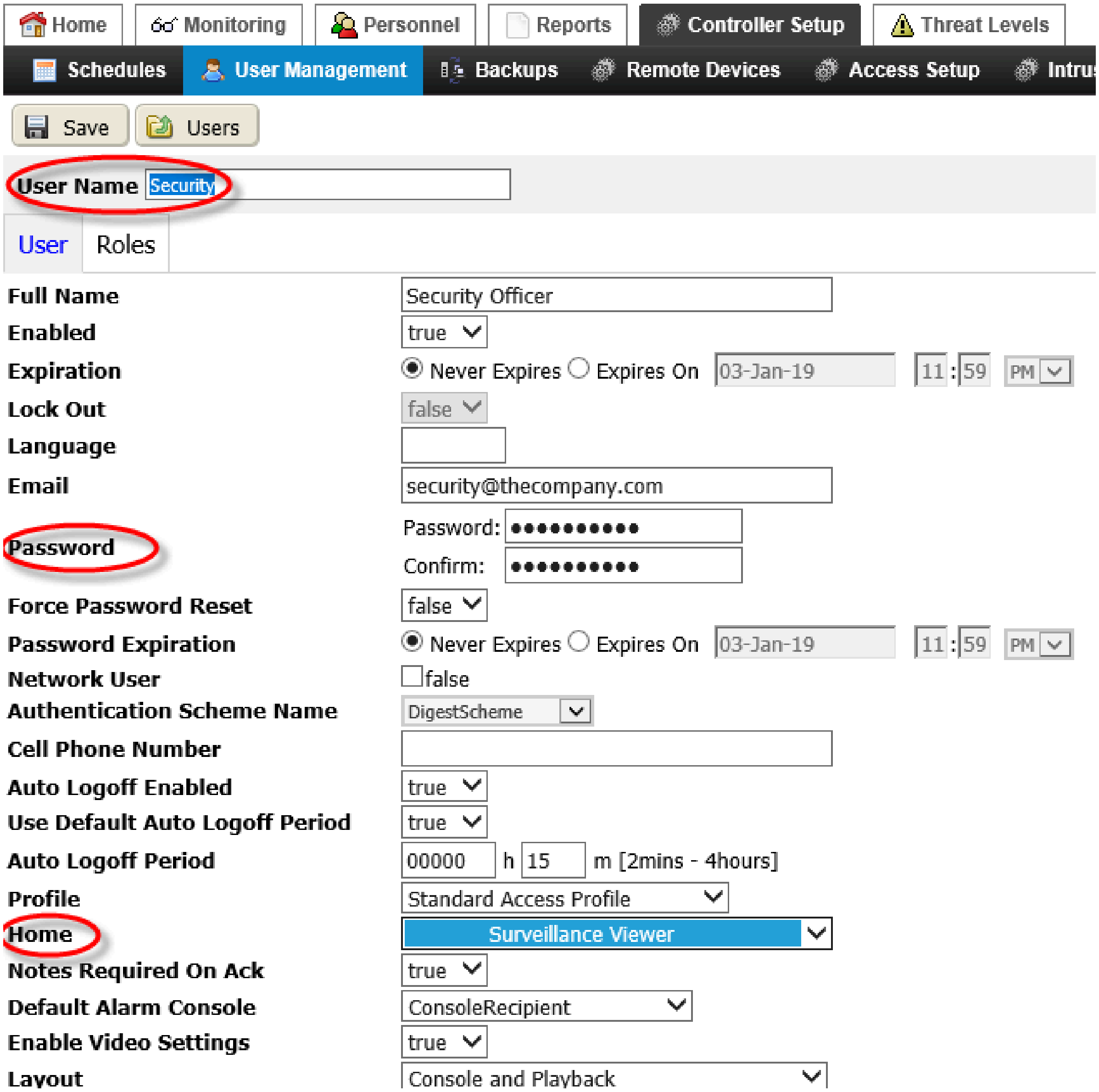
Prerequisites:
Roles have been created. You are using the web UI to create a user in the controller station.

Step 1. From the main menu, click **Controller Setup** > **User Management** > **Users**, and do one of the following.

- To create a new user, click the **Add** button at the top of the view to create a new user type.
- To edit all properties for an existing user, double-click the user row in the table.
- To edit selected properties, right-click the user row in the table and click `Rename` or the Quick Edit button (

  📝

).



User Name	Security
Full Name	Security Officer
Enabled	true
Expiration	● Never Expires ○ Expires On 03-Jan-19 11:59 PM
Lock Out	false
Language	
Email	security@thecompany.com
Password	Password: ●●●●●●●●●● Confirm: ●●●●●●●●●●
Force Password Reset	false
Password Expiration	● Never Expires ○ Expires On 03-Jan-19 11:59 PM
Network User	□ false
Authentication Scheme Name	DigestScheme
Cell Phone Number	
Auto Logoff Enabled	true
Use Default Auto Logoff Period	true
Auto Logoff Period	00000 h 15 m [2mins - 4hours]
Profile	Standard Access Profile
Home	Surveillance Viewer
Notes Required On Ack	true
Default Alarm Console	ConsoleRecipient
Enable Video Settings	true
Layout	Console and Playback

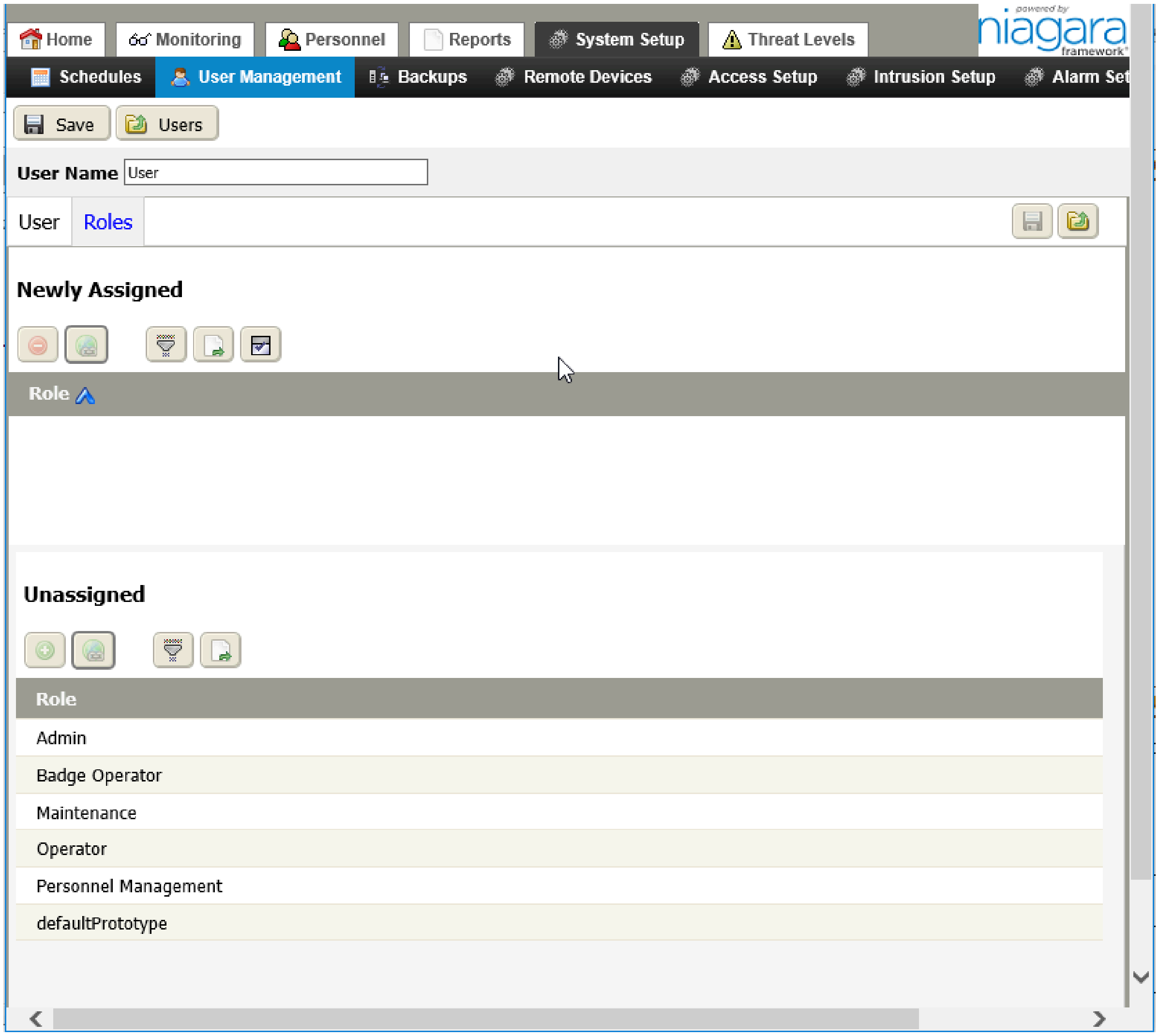
Step 2. Enter the **User Name** at the top of the view above the **Save** button.
This is the **User Name** part of the log-in credential.

Step 3. Enter and confirm the **Password**.
For the Https authentication user, this is the password defined in each respective application. If you need to configure these apps, you may edit their users later to provide credentials. Otherwise, the apps will not connect to the station database.

Step 4. Configure other properties, including **Home**.
Home configures the initial view the user sees after they log in. For example, the UI may open to the Alarm Console for an operator.

Step 5. Click the Roles tab.

The assigned and unassigned roles view opens.



User Name User

Newly Assigned

Role

Unassigned

Role
Admin
Badge Operator
Maintenance
Operator
Personnel Management
defaultPrototype

Step 6. To view the list of Unassigned roles, click the Assign Mode button (☑).

Step 7. Select an unassigned role and click the Assign button (⊕).
The system assigns the role to the user provided that the role assigned to the current user includes adequate permissions. You cannot assign a role to the currently-logged-in user. In other words, a currently-logged-in user cannot change their own role assignments.

Step 8. To edit the permissions associated with the assigned role, double-click the role in the Assigned pane, change permissions and click **Save**.

Step 9. After entering at least a name, password and role you may click **Save**.
At least one assigned role is required to create a user.

Step10. Test each user you add by logging out of the web UI and logging back in with the new user name and password.

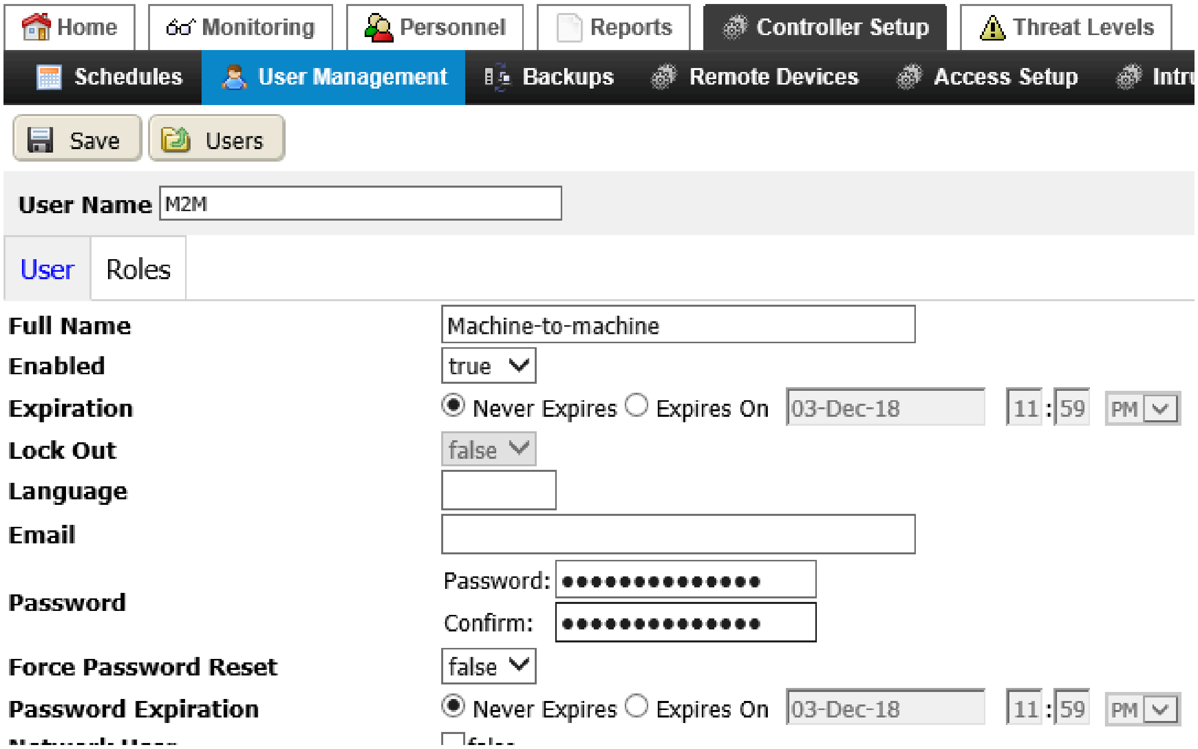
- Verify that the username and password combination works.
- Verify that the UI opens to the correct view.
- For an Alarm Console user, initiate an alarm and acknowledge it. To simulate a door-forced alarm, modify a schedule to force the building into the unoccupied period of the day. Or you could generate a door-held-open alarm.

Creating a controller machine-to-machine user

A machine-to-machine (M2M) user sets up network communication without requiring human intervention.

Prerequisites:
You are working in the web UI connected to a controller station.

Step 1. Navigate to **Controller Setup** > **User Management** > **Users**, and click Add ( ).
The User tab opens.



User Name	M2M
Full Name	Machine-to-machine
Enabled	true
Expiration	● Never Expires ○ Expires On 03-Dec-18 11:59 PM
Lock Out	false
Language	
Email	
Password	Password: •••••••••••••• Confirm: ••••••••••••••
Force Password Reset	false
Password Expiration	● Never Expires ○ Expires On 03-Dec-18 11:59 PM

Step 2. Configure at least the **User Name**, **Password** and confirm that **Enabled** is be set to `true`, **Password Expiration** is set to `Never Expires`, and **Authentication Scheme Name** is set to `DigestScheme`.

Step 3. Click the Roles tab and select the `Admin` role for this user and click **Save**.

Configuring a user's web profile

This procedure edits an existing user. To create a new user, double-click the **User Service**node in the Nav tree and click the **New** button.

Prerequisites:
You are working in Workbench.

Step 1. In the Nav tree, under the **Services** node, expand the **UserService** node and double-click a user.
The selected user property sheet opens.

Step 2. In the User property sheet view, confirm that the **Web Profile** property is set to `Standard`

`Access Profile` or `EntsecWeb Profile`, and that the appropriate Nav file is selected in the **Nav File** property, then click **Save**.

Special user for third party software application

While you can use the default admin superuser to create and configure all system functions, this user does not work with third-party software application.

Third-party application software require a special user to facilitate access to the station database. The reason that the admin user does not work with these third-party apps is that it defaults to DigestScheme authentication. The third-party software require `HTTPBasicScheme` authentication.

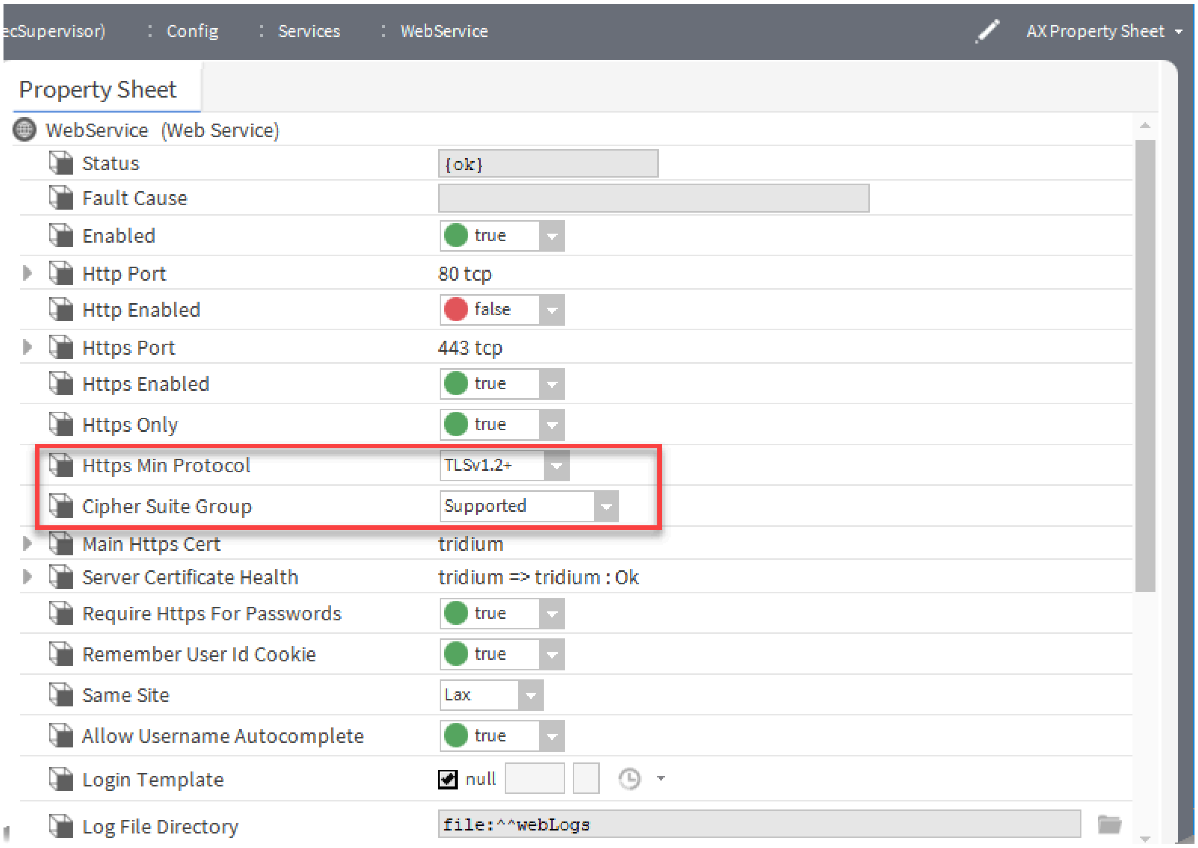
You must create a separate user for each app. You can use Workbench or the web UI to create these users. The credentials you define for each user are those required by third-party software.

Configuring the WebService for Easy Lobby

Easy Lobby requires that two properties in the **WebService** to be configured before you can use it to manage visitors. This procedure requires Workbench to configure these properties, which are not available in the web UI.

Prerequisites:
You are connected to the station that will support Easy Lobby and are using Workbench.

Step 1. Expand **Config** > **Services** and double-click the **WebService**.
The **WebService's AX Property Sheet** opens.



WebService (Web Service)

Status	{ok}
Fault Cause	
Enabled	● true
Http Port	80 tcp
Http Enabled	● false
Https Port	443 tcp
Https Enabled	● true
Https Only	● true
Https Min Protocol	TLSv1.2+
Cipher Suite Group	Supported
Main Https Cert	tridium
Server Certificate Health	tridium => tridium : Ok
Require Https For Passwords	● true
Remember User Id Cookie	● true
Same Site	Lax
Allow Username Autocomplete	● true
Login Template	☑ null
Log File Directory	file:^^webLogs

Step 2. Confirm that **`Https Min Protocol`** is set to `TLSv1.2+`.

NOTE:

TLSv1.0 and TLSv1.1 are still supported for backwards compatibility, but it is recommended to use TLSv1.2 and higher.

Step 3. Change **`Cipher Suite Group`** to `Supported`.

Step 4. To save these changes, click **Save**.

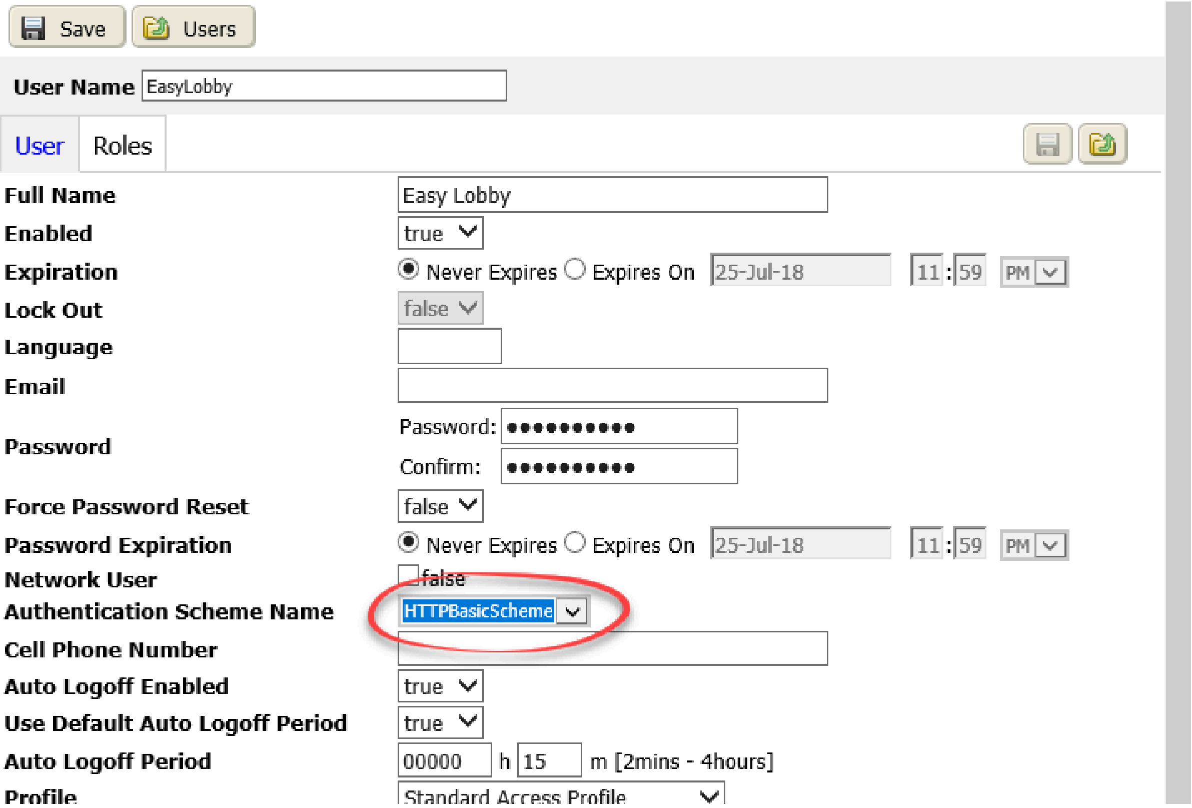
Setting up an Easy Lobby user

For security reasons, a separate user is required to set up Easy Lobby for visitor management. This procedure creates an Easy Lobby user and assigns the Admin role to the Easy Lobby user.

Prerequisites:
Using the web UI, you are connected to the Supervisor station.

Step 1. From the main menu, navigate to **System** > **User Management** > **Users**.

Step 2. To create an Easy Lobby user, click the Add button (⊕).
The New User view opens.



User Name	EasyLobby
Full Name	Easy Lobby
Enabled	true
Expiration	● Never Expires ○ Expires On 25-Jul-18 11:59 PM
Lock Out	false
Language	
Email	
Password	Password: ●●●●●●●●●● Confirm: ●●●●●●●●●●
Force Password Reset	false
Password Expiration	● Never Expires ○ Expires On 25-Jul-18 11:59 PM
Network User	□ false
Authentication Scheme Name	HTTPBasicScheme
Cell Phone Number	
Auto Logoff Enabled	true
Use Default Auto Logoff Period	true
Auto Logoff Period	00000 h 15 m [2mins - 4hours]
Profile	Standard Access Profile

Step 3. Enter at least a password and an **`Authentication Scheme Name`** of `HTTPBasicScheme`.
New users default to the `DigestScheme`, which does not work with the Easy Lobby software.

NOTE: If the `HTTPBasicScheme` is not available, use Workbench to add it to your installation. Refer to "Third-party software application" in the *System Security* chapter of this document.

Step 4. To assign the Admin role to this user, click the Roles tab, click the Assign Mode button (▤), select the `Admin` role in the Unassigned pane, click the Assign button (⊕), and click **Save**.

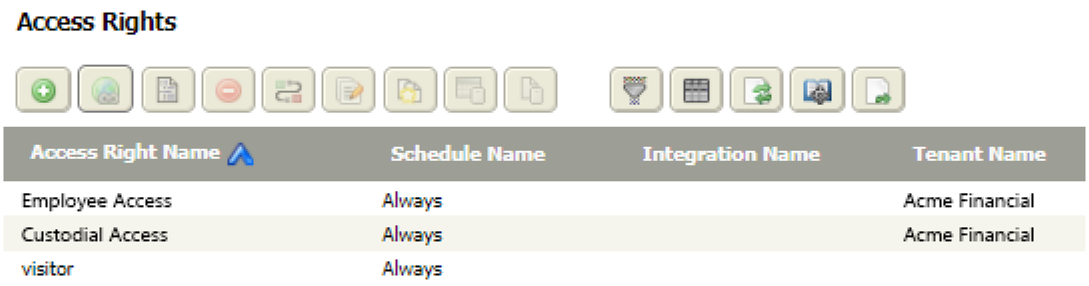
Step 5. Make a note of the User Name and Password so you can enter them into the Easy Lobby software.

Related tasks

- Setting up HTTP Authentication scheme for third party application

Access rights

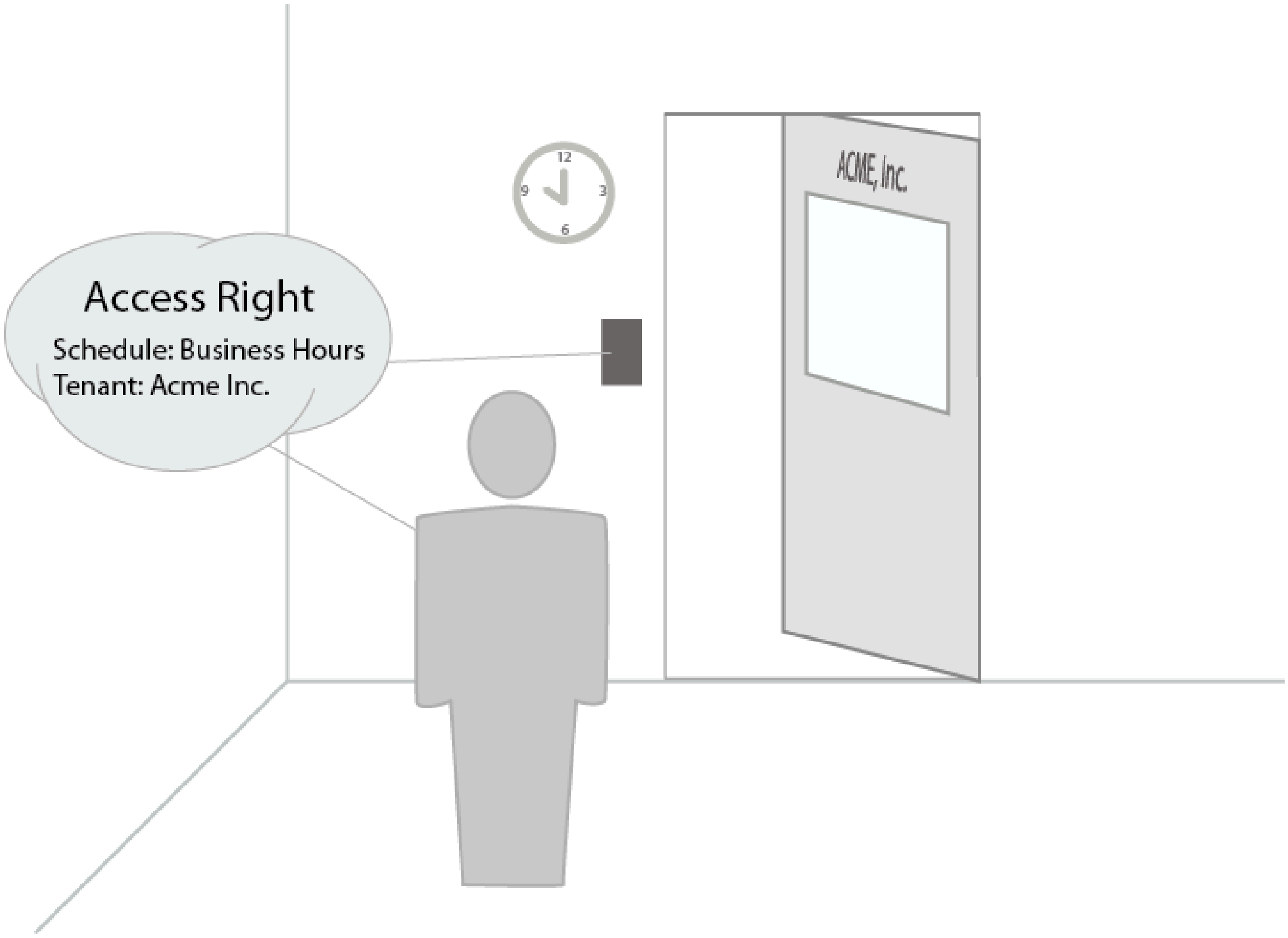
An access right defines a schedule and tenant. You associate access rights with readers and personnel. They allow you to define and schedule what readers a person can use for entry and exit. Access rights provide information about where a person typically resides in a building. In Enterprise Security, an Access Right can have only one tenant, multiple tenants cannot be assigned to one Access Right. However, you can assign more than one Access Right to a single tenant. For example, you can assign the access right named "Employee Access" and the right named "Custodial Access" to a single tenant, as shown in the following image.



Access Right Name	Schedule Name	Integration Name	Tenant Name
Employee Access	Always		Acme Financial
Custodial Access	Always		Acme Financial
visitor	Always		

Access rights control access to a facility while sharing access to some of the same entry and exit locations.

Figure 13. Access right associated with a person and card reader



Assigning an access right to a reader associates the schedule and tenant with the specific reader and door. Assigning the same access right to a person grants that person the right to enter or exit the tenant's building using the reader and door identified by the access right, during the time granted by the schedule.

NOTE: A person may have more than one access right assigned. `Users` do not have access rights – only `Personnel` are assigned access rights.

Access rights control other system functions including threat levels and building controls.

Elevator control

An access right controls the floor(s) that a person can select in an elevator.

The system manages elevator access by providing a relay output for each floor that the elevator serves. 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. This wiring prohibits access to a floor unless the relay is energized, such as by an access right or by a calendar schedule. When the person with the elevator access right swipes their badge, the relays for the floor(s) they can access come on for a few seconds so they can make their selection.

When creating an elevator access right, you choose the card reader that is associated with the elevator, then specify the floors that are accessible by the person with that access right. You can also assign a schedule to individual floors such that during daytime hours, the floor can be enabled automatically.

Creating an access right

Access rights define general information that applies to person types. The schedule associated with an access right defines when the right is valid. Creating an access right includes associating specific card readers, doors, and elevators and people.

Prerequisites:
You are working at the Supervisor station. A schedule to associate with the access right exists.

Step 1. From the main menu, select **Personnel** > **Access Rights**.
The Access Rights view opens.

Step 2. Click Add (⊕).
The Add New Access Right view opens.

Step 3. Fill in the name of the right.
The name might be associated with a building or other location or relate to the type of user.

Step 4. Click the chevron next to the **`Schedule`** property, select a schedule from the **Ref Chooser** and click **Ok**.

Step 5. If the building is configured for multiple tenants, click the chevron next to the **`Tenant`** property, select the tenant from the **Ref Chooser** and click **Ok**.

Step 6. Click the **Save** button.
The access right is saved and the edit existing access right viewopens.

Editing access right effective date and assigned threat level

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

Step 1. From the main menu, select **Personnel** > **Access Rights**.
The Access Rights view opens.

Step 2. To edit the access right, double-click its row in the table.
The edit view opens.

Step 3. Click the People tab and highlight the person whose access right effective date you want to change.

Step 4. In the toolbar menu, click the **Change Assignment Properties** button (⧉).
The **Change Assignment Properties** window opens.

Step 5. Configure the properties: **`Start Date`** and **`End Date`** and **`Assigned Threat Level`**, and click the **Ok** button.
The access right properties are changed.

NOTE: Changing the **`Assigned Threat Level`** in an access right breaks the connection between the access right and the threat level defined by the access right's associated threat level group. Future changes to the threat level as defined in the threat level group will not affect the threat level that has been configured directly on an access right.

Step 6. To update the database, click the **Save** button at the top of the view.

Access control setup

Access is controlled by a complex combination of hardware (card readers and doors), passwords, PINs (Personal Identification Number), access zones, intrusion zones, integration IDs and access rights.

Access zones control occupancy levels and monitor the entry and exit actions of personnel for a defined area. You may use anti-passback controls based on occupancy. This guide provides procedures for setting up access zones.

Access control methods

An access method determines how a person gains access to a building or area.

The system provides these methods to control access:

- Card-only access allows entry or exit using a card at a reader. No PIN is required for this type of access.
- Card plus PIN access requires both a card and a PIN (Personal Identity Number).
- Card or keypad access requires either a card swipe, card number entry, or an intrusion PIN entry using a keypad for access.
- Control access by schedule allows access only at certain times, depending on the schedule parameters. The Installation and Maintenance Guide provides procedures for setting up regular schedules. This guide covers special events.
- Access is available through the graphical user interface, which controls the doors.

Access zones

An access zone is a secured physical area used to control and monitor the entry and exit of personnel to and from the zone. Entry and exit doors, their associated readers, and configuration properties define each access zone. When an access zone is enabled or disabled, a log entry is written and, optionally, an alarm is generated (for disabling the access zone).
The system monitors zone occupancy by counting the number of people who enter and exit, by identifying occupant type (supervisor or other), and by maintaining an occupant threshold (the maximum or minimum number of people allowed in the zone). Access zone-related alarms are configurable in terms of high, medium, low, or off, as defined by their associated alarm classes.

Supervisor requirement

You may designate any person-type as supervisor. When supervisor enforcement is in effect for an access zone, at least one occupant of the access zone must have the supervisor designation.

Occupancy counts and thresholds

Occupancy identifies who is in an access zone at any given time. Occupancy monitoring must be enabled. When enabled and an entry reader grants access, the system increments the occupancy count. When a reader grants an exit, the system decrements the occupancy count. A user with proper authorization may reset occupancy count to zero manually at any time or automatically according to a designated time-schedule.

Occupancy thresholds configure the minimum and maximum number of occupants that are allowed in an access zone. Thresholds may be enforced by denial of access at the entry door or by the generation of an alarm—or a combination of both, using hard or soft enforcement, as described, below.

Anti-passback feature

The return of an occupant to an access zone after leaving the zone is called a passback. The system's anti-passback feature configures when an occupant is allowed to pass back. In addition to tracking who enters and exists (occupancy), the system monitors the time between badge swipes. An occupant must exit through a controlled exit reader door, and the **`Passback Timeout`** must expire for the occupant to be eligible for re-entry into the access zone. A re-entry attempt by an occupant or a second badge swipe that occurs prior to the **`Passback Timeout`** value is an anti-passback violation, which may generate an alarm.

System users whose access zone permission is configured for write enabled may change the **`Reset Occupancy Time`** and **`Passback Timeout`** properties for an access zone.

Access enforcement

Several options exist for enforcing the supervisor requirement, count thresholds, and the anti-passback feature.

- Enforcement may be disabled.
- Hard enforcement may be configured. This type of enforcement results in access denied at a card reader and the generation of an alarm.
- Soft enforcement results in access granted but with the generation of an alarm.

In an environment where enforcement depends on a network connection, hard enforcement results if network communication is lost.

Multiple controller zones

When an access zone spans multiple controllers, one controller serves as the zone master. All other dependent controllers rely on the master to maintain occupancy and configuration data. Dependent controllers query the master to determine the authentication criteria at any given time.

The system maintains configuration data in all remote controllers so that in case there is a loss of communication, a designated form of fall-back enforcement takes effect. When an access zone is configured with supervisor monitoring, threshold monitoring, or anti-passback, fall-back enforcement occurs as follows:

- Hard enforcement denies access, and post an entry to the access report indicating that the denial of access was due to communication failure.
- Soft enforcement grants access, but posts an entry to the access report indicating that the current occupancy criteria are unavailable due to communication failure.

Grouping

You use grouping, in an access zone to include other stations and their readers as part of the access zone. A remote controller that originates (or creates) an access zone is always the access zone master—even if the zone is created from a stand-alone controller that is subsequently added to a Supervisor. As the access zone master, this controller maintains the list of all people who have access to the zone.

NOTE: Do not create access zones from the Supervisor station. Create and maintain the access zone master at a remote host controller so that a network connection to a Supervisor is not critical to keep the access zone functioning. If the Supervisor is the master, and a network connection to the Supervisor is lost, the access zone does not function.

Note the following points about grouping and the Add New Access Zoneor Edit Access Zone views:

- You must be connected to the master controller station.
- The stations (points) to add to the group must be joined in a peer role relationships with the master station.
- The Entry Reader and Exit Reader tabs display only local readers.
- The Occupants tab and the Supervisor tab are always available in the access zone views but the information they display is based on settings from the access zone master station.
- You can only add readers to access zones when you are connected to the reader’s assigned station. Readers are not visible or configurable from remotely-grouped stations.

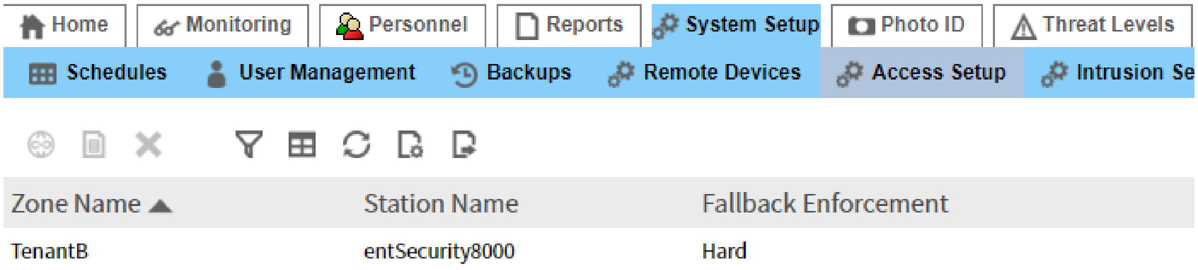
Creating a new master access zone

A master access zone groups related stations and their readers that share physical proximity. The stations within an access zone share access zone naming, status, occupancy, and Supervisor information. The controller that originates (or creates) an access zone is the access zone master — even if the zone is created from a stand-alone controller that is subsequently added to a Supervisor station.

Prerequisites:
Entry and exit readers are required for access zones to track occupancy.

You perform this procedure in a remote controller station. You cannot create an access zone from the Supervisor station. If a Supervisor station served as the master and connection to the Supervisor is lost, the access zone would not function and access might be denied.

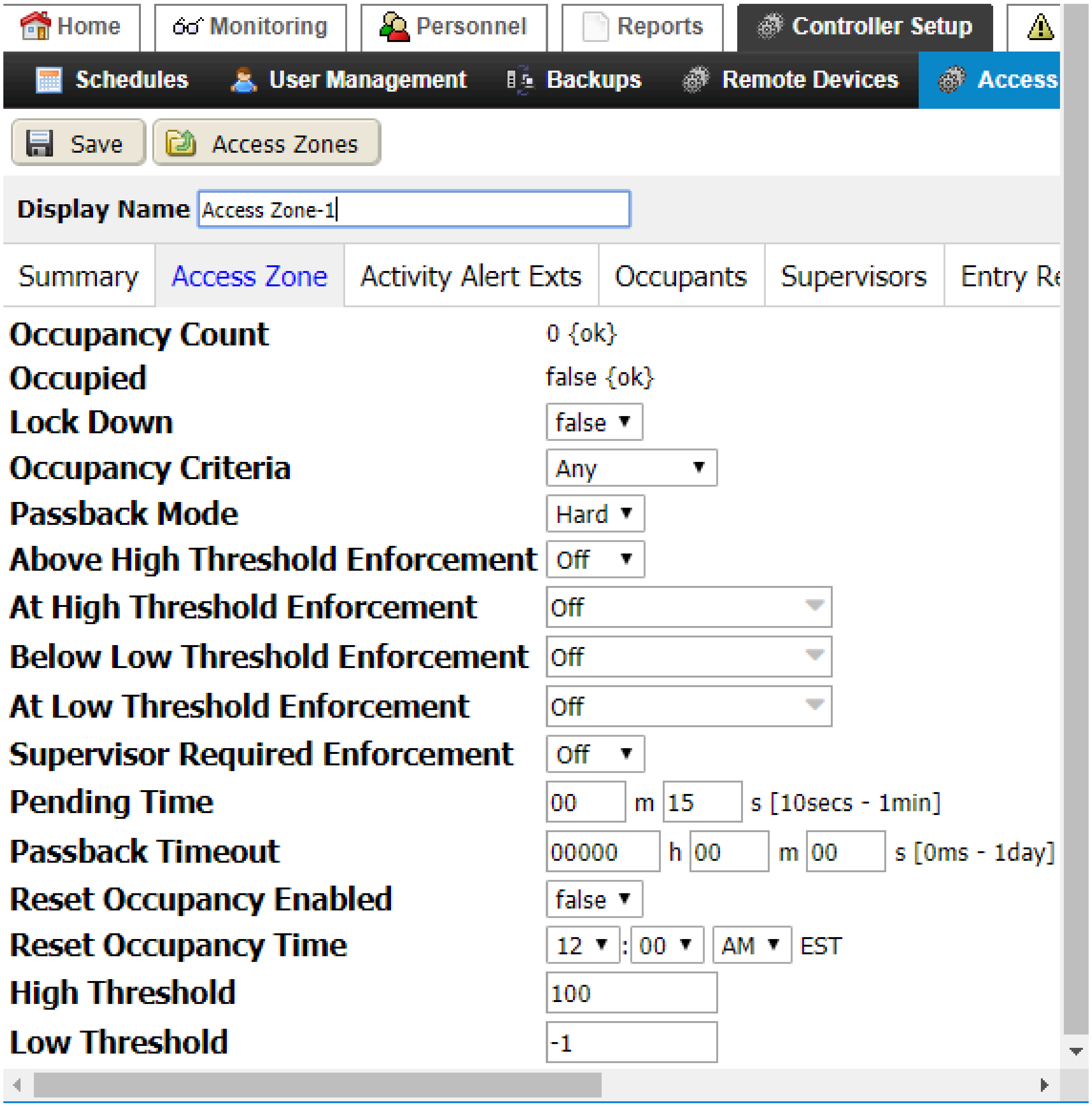
Step 1. From the main menu, select **Controller Setup** > **Access Setup** > **Access Zones**.
The Access Zones view opens.



Zone Name ▲	Station Name	Fallback Enforcement
TenantB	entSecurity8000	Hard

Step 2. Click the **Add** button at the top of the view.

The Add New Access Zone view opens with the Access Zone tab selected.



Display Name Access Zone-1

Occupancy Count	0 {ok}
Occupied	false {ok}
Lock Down	false
Occupancy Criteria	Any
Passback Mode	Hard
Above High Threshold Enforcement	Off
At High Threshold Enforcement	Off
Below Low Threshold Enforcement	Off
At Low Threshold Enforcement	Off
Supervisor Required Enforcement	Off
Pending Time	00 m 15 s [10secs - 1min]
Passback Timeout	00000 h 00 m 00 s [0ms - 1day]
Reset Occupancy Enabled	false
Reset Occupancy Time	12 : 00 AM EST
High Threshold	100
Low Threshold	-1

Step 3. Enter the name of the master zone in the **Display Name** property.

Step 4. Configure zone properties on the Access Zone tab.
Several properties provide soft and hard options. The *Reference* manual explains these properties in detail. Hard means that if the occupant does not meet the requirement, the system denies access and generates an alarm. Soft means that even if the occupant does not meet the requirement, the system allows access, but also generates an alarm.

Step 5. Configure all applicable properties on the other tabs.

Step 6. To create the zone, click the **Save** button.
The editview of the access zone opens, with the Summary tab active.

Adding readers to an access zone

Entry and exit readers keep track of building occupants and supervisors.

Prerequisites:

The access zone exists in the local station.

Step 1. From the main menu, select **Controller Setup** > **Access Setup** > **Access Zones.**
The Access Zones view opens

Step 2. Double-click an access zone row in the table.
The editview for the access zone opens.

Step 3. Click a reader tab (Entry or Exit Readers), and click the Assign Mode button (▤)
A list of the available readers opens in the Unassigned pane.

Step 4. Select the name of a reader from the Unassigned list and click and the Assign button (⊕).
To remove an entry and exit reader from the station's currently-displayed access zone, select the row in a Assigned pane and click the Unassign button (

⊖

).

Extending an access zone to include multiple stations

An access zone that includes multiple stations is a group. In addition to extending the access zone physically, this allows sharing of access zone naming, status, occupancy, and supervisor information.

Step 1. From the main menu, select **Controller Setup** > **Access Setup** > **Access Zones.**
The Access Zones view opens

Step 2. Double-click an access zone row in the table.
The edit view for the access zone opens.

Step 3. Click the Grouping tab, and click the Assign Mode button (▤).
The Assigned pane lists the stations that are part of the group. The Unassigned pane lists the stations that are available to join the group.

Step 4. To assign a station, select its row and click the Assign button (⊕).
The system associates the station with the group.

NOTE: Access zone information is passed to a Supervisor station, as appropriate, but entry and exit readers are not configurable or visible from the Supervisor.

Step 5. To remove a station from the currently-displayed group, select its name in the Assigned pane and click the Unassign button (⊖).

Assigning a supervisor to an access zone

Only people designated as supervisors are eligible to be assigned as a supervisor for a specific access zone. These have the `Supervisor` property configured as `true` on their personnel record.

Prerequisites:
The access zone exists in the local station.

Step 1. From the main menu, select **Controller Setup** > **Access Setup** > **Access Zones.**
The Access Zones view opens

Step 2. Double-click an access zone row in the table.
The edit view for the access zone opens.

Step 3. Click the Supervisors tab, and click the Assign Mode button (▤).
A list of any currently-assigned supervisors opens in the Assigned pane. A list of authorized supervisors opens in the Unassigned pane.

Step 4. To assign a supervisor, select the person row and click the Assign button (⊕).

The system associates the person with the zone as a supervisor. To remove a supervisor from the currently-displayed access zone select the name in the Assigned pane and click the Unassign button (

⊖

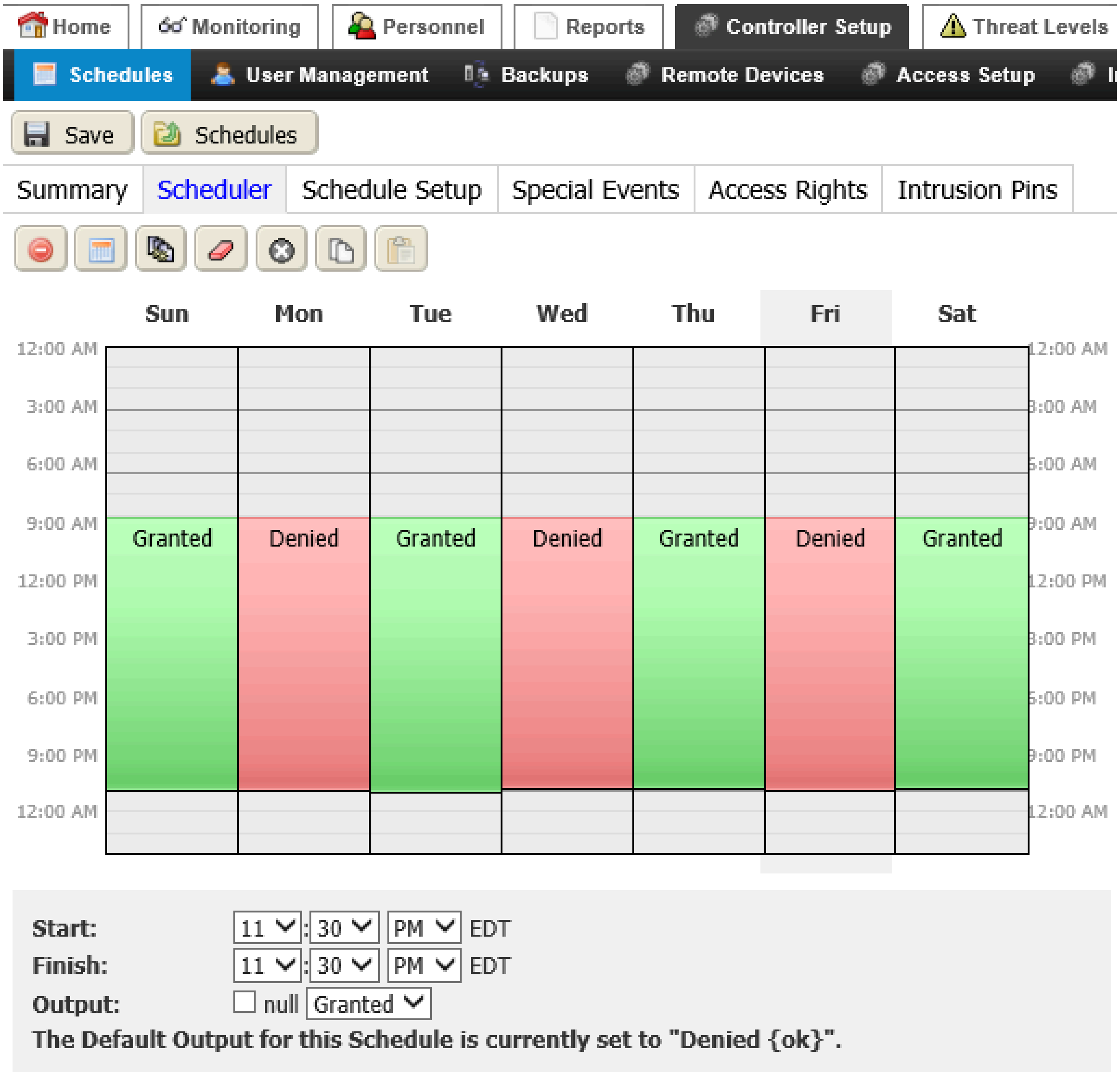
).

Weekly schedule setup

Weekly schedules define when a building is open for business.

A weekly schedule defines normal working days.

Figure 14. Weekly scheduler view



Sun	Mon	Tue	Wed	Thu	Fri	Sat
Granted	Denied	Granted	Denied	Granted	Denied	Granted

Start: 11 : 30 PM EDT
Finish: 11 : 30 PM EDT
Output: □ null Granted

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

The scheduling interface uses a simple calendar view. The screen capture is an example of a schedule used to configure access rights for a daily shift. The procedures in this chapter configure a basic weekly schedule, which you can associate with doors. The *Facility Manager's Guide* explains calendar schedules and how to add special events and holidays.

Adding or editing a schedule (default settings)

This procedure describes how to create a standard schedule that represents normal daily building activity.

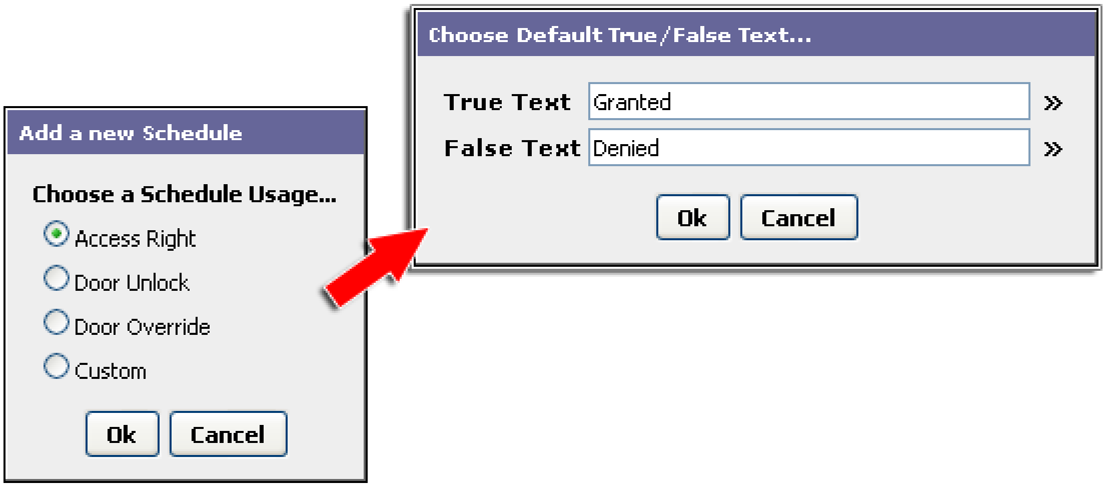
Prerequisites:
You are working in the Supervisor station.

Step 1. Click **System Setup** > **Schedules**.
The Schedules view opens.

Step 2. Do one of the following:

- To start a new schedule, click the Add button (⊕).
- To edit an existing schedule, double-click the schedule row in the table.

If you are adding a new schedule, the **Add a New Schedule** window opens.



Add a new Schedule

Choose a Schedule Usage...

● Access Right
○ Door Unlock
○ Door Override
○ Custom

Ok Cancel

Choose Default True/False Text...

True Text: Granted

False Text: Denied

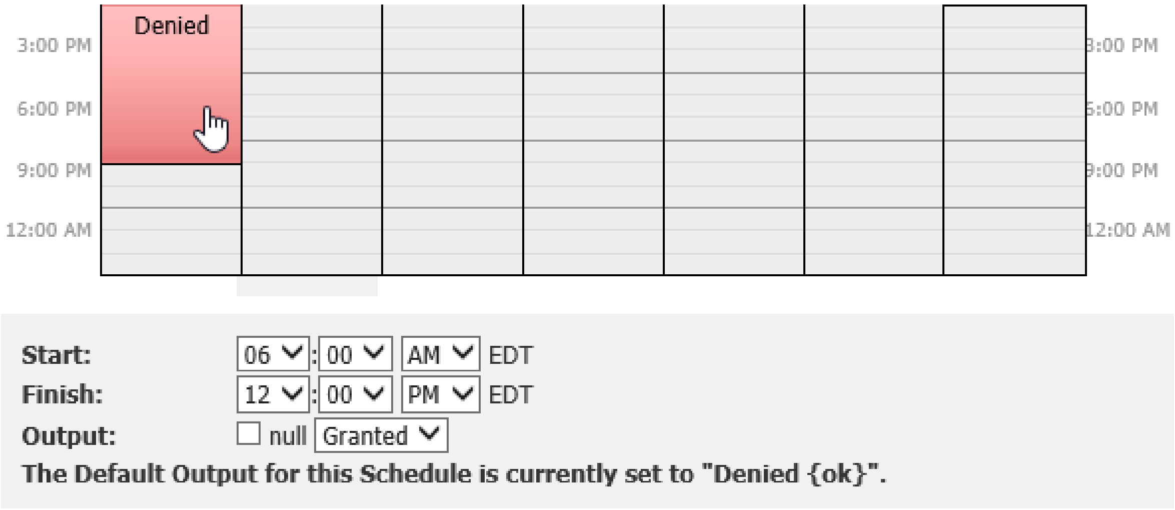
Ok Cancel

The **`Usage`** property in the **`Add a new Schedule`** view identifies the purpose of the schedule making it convenient to identify and assign schedules to appropriate components (access rights, door overrides, door unlock, and others). Selecting the `Custom` option defines a new use. Each use can have its own facets so that the Boolean `true`, and `false` change as appropriate for the schedule's application. For example, for an access right, true can change to "Granted" and false to "Denied."

Step 3. For a new schedule, select the type of schedule and click **Ok**.
After defining the purpose for the schedule, the system opens the Add New Schedule view, Scheduler tab.

Step 4. Enter a name for the calendar schedule in the **`Display Name`** property.

Step 5. To add or edit an event, click in a day at the approximate event start time, and drag down to define the start and finish times.



Start: 06 : 00 AM EDT
Finish: 12 : 00 PM EDT
Output: □ null Granted
The Default Output for this Schedule is currently set to "Denied {ok}".

Once entered, events appear as solid colored blocks, while unscheduled (default output) time appears as light gray. The event remains selected (by default, pink colored) when you release the mouse button.

Step 6. As needed, click again and drag on the event’s top or bottom edge to change its start or finish time (in broad increments).
Right-click on a scheduled block to use the popup menu to copy and paste event times across predefined days of the week, to delete an event or to clear a day or week.

Step 7. Choose an Output option (`true` or `false`) and use the **`Start`** and **`Finish`** properties to specify when the Output option is effective.

NOTE: When you click on the block in the scheduler, you can choose if that block is true or false. For example, when you add the event, the block may be set to "locked" when in fact you want the door to be unlocked during that period. Sometimes you may need to use the start and finish to get the exact time because the dragging function isn't very granular.

Step 8. Use the properties on each tab to define a schedule, and click **Save**.

NOTE: For weekly schedules, it is a good practice to save your changes while working in each tab, even though any save applies to changes made on all tabs.

The system saves the new or edited schedule and displays it in the edit schedule view.

Creating a custom-usage schedule

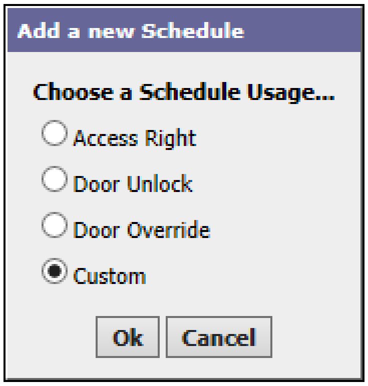
Most schedules control access rights, door unlock and door override. A custom-usage schedule expands the capabilities of the system.

An example of when you may want to use a custom-usage schedule is in the case where you want to set up a schedule that automatically arms and disarms an intrusion zone. You could name the usage “Intrusion.” You may set the true state to `armed` , and the false state to `disarmed` . Make the default state `true`. Now you can easily schedule your intrusion zone to disarm during occupied periods.

Step 1. From the main menu, click **System (Controller) Setup** > **Schedules**.
The Schedules view opens.

Step 2. Start a new schedule by clicking the Add button (⊕).

The **Add A New Schedule** window opens.

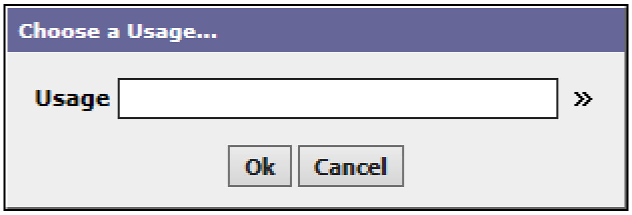


Add a new Schedule

Choose a Schedule Usage...

○ Access Right
○ Door Unlock
○ Door Override
● Custom

Step 3. Click the `Custom` option and click **Ok**.
The **Choose a Usage...** window opens.



Choose a Usage...

Usage

Step 4. Use the string chooser to select the component with which to associate the schedule, and click **Ok**.
The **Choose Default True/False Text...** window opens.

Step 5. Define what you want to appear when the condition is true, and what should appear when it is false and click **Ok**.
The Add New Schedule view opens.

Step 6. Configure the `Start` and `Finish` times and drag the cursor to fill in each day.
Notice that the true and false text you defined appears in the `Output` property drop-down list.

Chapter 7. NAC Driver Controller Setup and Integration

The chapter describes the steps to discover and configure the NAC controller to the existing system.

Prerequisites

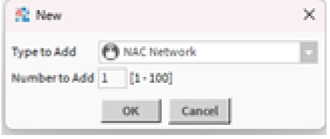
1. Workbench is already licensed with Niagara Access Application for Supervisor.
2. Niagara Access (NAC Server) is already installed and configured.
3. The **Rdbms Network** and the database is configured under **Rdbms Network**.
4. The NAC Controllers have already gone through the initial configuration setup. This step must be completed before the controller can be used and added to Niagara Access and NAC Network.

Add NAC Network

This topic explains to add the NAC network.

Step 1. Navigate to the **Config** > **Drivers** and double-click on the **Drivers** tab.

Step 2. Click the **New** button on the **Driver Manager** view.

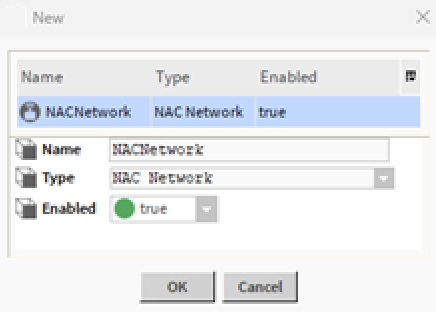


Type to Add: NAC Network

Number to Add: 1 [1 - 100]

A **New** window opens.

Step 3. Select the NAC Network from the drop-down list and click `OK`.



Name	Type	Enabled
NACNetwork	NAC Network	true

Name: NACNetwork

Type: NAC Network

Enabled: true

A second **New** window opens.

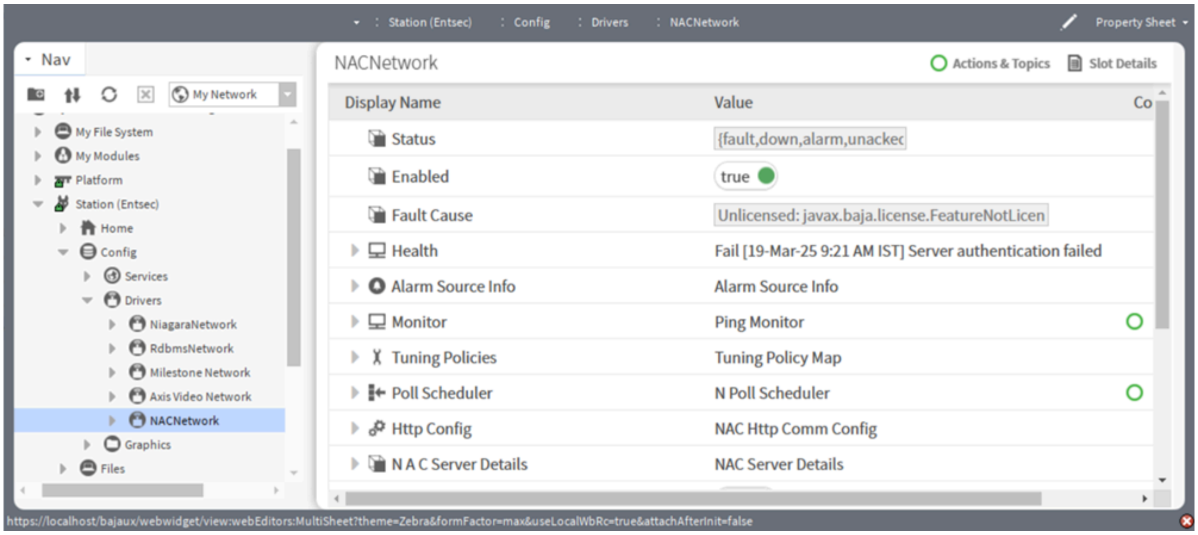
Step 4. Use this window to give the network a unique name and click `OK`.

Configure NAC Network

This section provides instructions for a NAC network configuration.

Prerequisites:
Login to Niagara Access in Web Browser.

Step 1. Right-click the **NAC Network** > **Views** > **Property Sheet**.



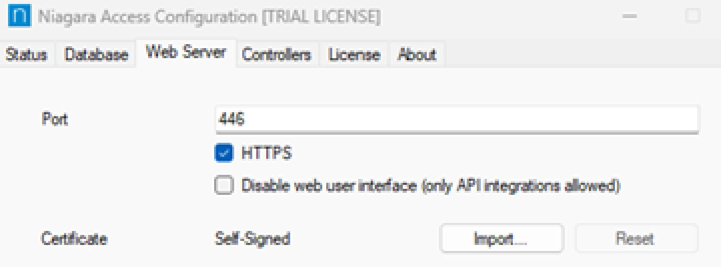
Display Name	Value
Status	{fault,down,alarm,unackec
Enabled	true ●
Fault Cause	Unlicensed: javax.baja.license.FeatureNotLicen
Health	Fail [19-Mar-25 9:21 AM IST] Server authentication failed
Alarm Source Info	Alarm Source Info
Monitor	Ping Monitor
Tuning Policies	Tuning Policy Map
Poll Scheduler	N Poll Scheduler
Http Config	NAC Http Comm Config
N A C Server Details	NAC Server Details

The **Property Sheet** view opens.

Step 2. Configure the following properties for the network

a. Expand **Http Config** > **Address**. Enter the **`IP Address`** as `Localhost` .

b. Enter the **`Port`** number already set for **Niagara Access** (NAC Server) in the Niagara Access Configuration application.



Port: 446

☑ HTTPS

☐ Disable web user interface (only API integrations allowed)

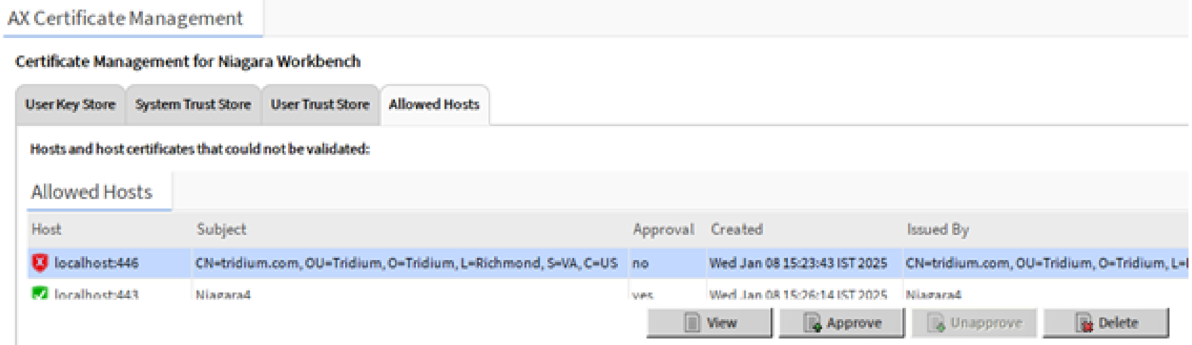
Certificate: Self-Signed

Launch the **Niagara Access Configuration** application via the desktop shortcut on the system hosting the **Niagara Access** (NAC Server) to locate the **`Port`** number. Note that administrator privileges on Windows are required to run this application. Once open, go to the **Web Server** tab and check the **`Port`** field.

c. Expand **`NAC Server Details`** to enter server **`Credentials`**. Ensure the **`Username and Password`** entered match those already configured for the **Niagara Access** (NAC Server), then click `Save` .

Step 3. Right-click on **NAC Network** > **Actions** > **Ping**. Once the ping action is completed, proceed to approve the host certificate.

Step 4. Navigate to **Tools** > **Certificate Management**. Under the **Allowed Hosts** tab, choose the desired certificate and click `Approve` to validate the host certificate.



Hosts and host certificates that could not be validated:

Host	Subject	Approval	Created	Issued By
localhost:446	CN=tridium.com, OU=Tridium, O=Tridium, L=Richmond, S=VA, C=US	no	Wed Jan 08 15:23:43 IST 2025	CN=tridium.com, OU=Tridium, O=Tridium, L=
localhost:443	Niagara4	yes	Wed Jan 08 15:26:14 IST 2025	Niagara4

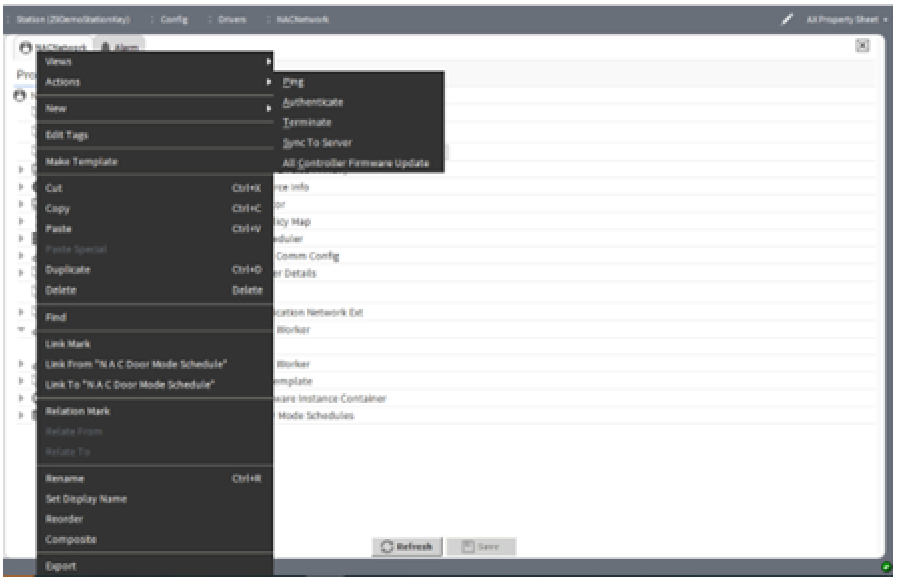
Step 5. To authenticate the connection with the server right-click on **NAC Network** > **Actions** > **Authenticate**. If authentication is successful, the network status will update to `OK`, and the fault cause will be cleared.

Step 6. To synchronize all configurations with the server, click on **NAC Network** > **Actions** > **Sync To Server**.

NAC Network Actions

In addition to the standard operations, the actions supported by the NAC Network component include the following.

Actions



- **Ping** : The Ping action establishes communication with the server to confirm the connection.
- **Authenticate** : You must authenticate to the server before adding any device to the network, using the correct username and password for successful authentication.
- **Terminate**: This action terminates a session initiated through authentication, invalidating the associated session token once triggered.
- **Sync to Server**: Transfer network and device configuration properties to the server whenever **NAC Network** or **NAC Device** properties are modified.
- **All Controller Firmware update**: Update the firmware for all controllers listed under the **NAC Network**.

NAC Device Setup and configuration

This chapter explains about **NAC Device** setup.
Currently, NAC Driver can support two types of controllers.

1. ZKTeco Controller
2. Azure Controller

Adding NAC Controller to Workbench

NAC device Manager view manages the devices (NAC devices) connected or that need to be added to the NAC network. It is available only for configuring NAC Devices.

The NAC Controllers have completed the first configuration setup. For more information, see the "NAC Controllers-Initial Setup.pdf" page.

NAC Controller can be added and configured in two ways

1. Manually add the controller using a new command.
2. Add controller using the discover option.

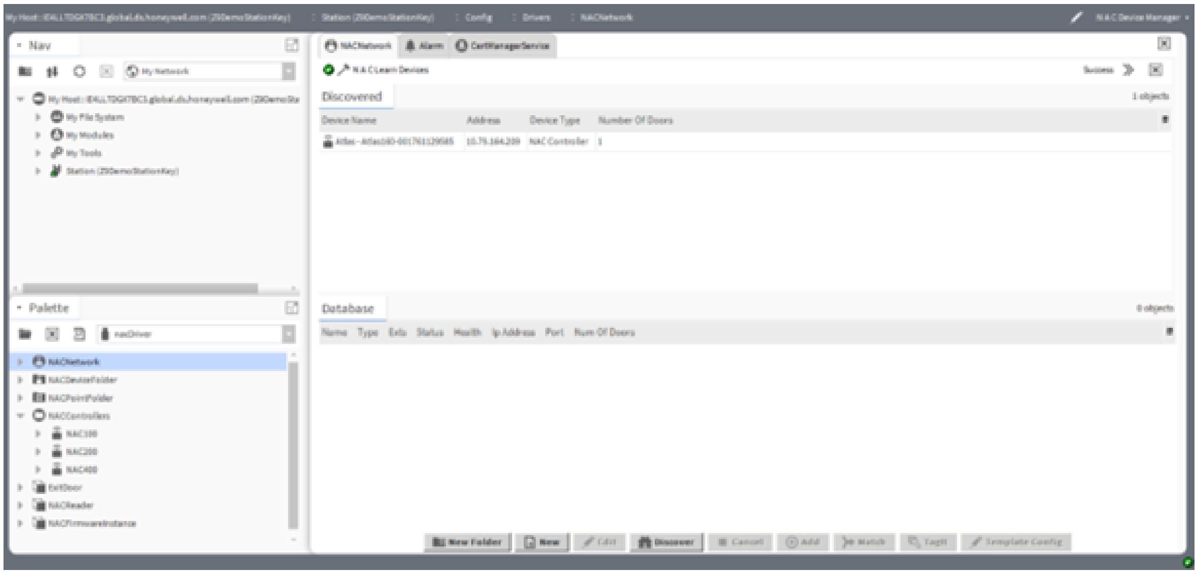
Discovering and Adding NAC Controller

This topic explains how to add an NAC controller to the Workbench.

Prerequisites:
Ensure that the controllers are connected to the same network as the server before attempting to discover them in the Device Manager view.

Step 1. Navigate to the **NAC Device Manager** view within the **NAC Network**.

Step 2. Click on the `Discover` button located at the bottom of the **NAC Device Manager** view.



Device Name	Address	Device Type	Number Of Doors
Atlas--Atlas160-001761129585	10.75.164.209	NAC Controller	1

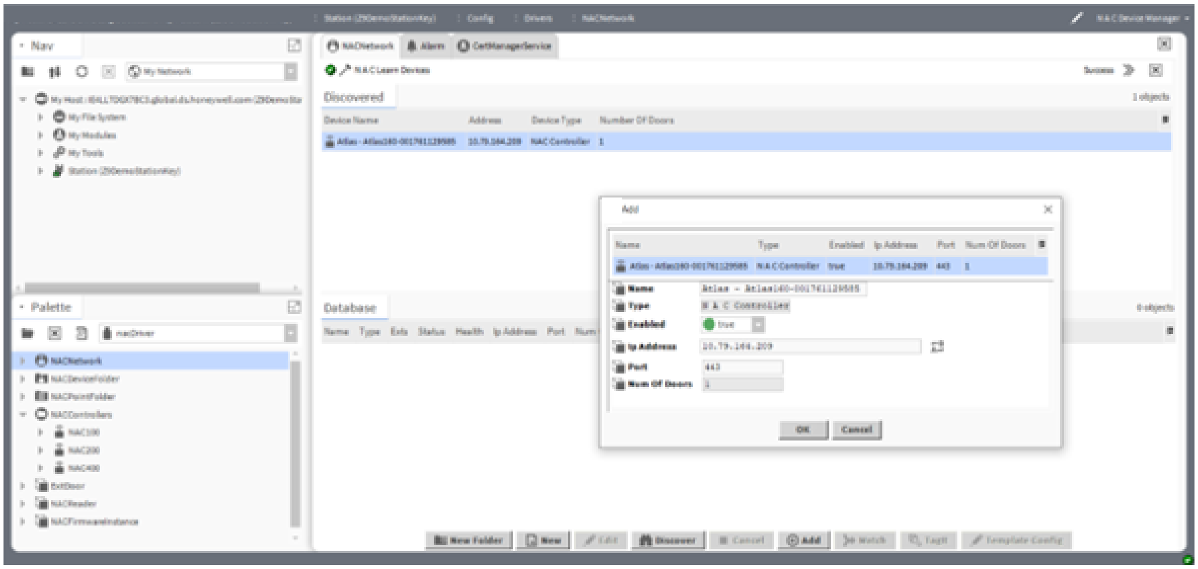
Name	Type	Exts	Status	Health	Ip Address	Port	Num Of Doors

The discovery process will search for controllers in the local network database and display all the controllers found on the network.

Step 3. Right-click on the desired discovered controller and click the `Add` button.

Step 4. In the **Add** window, verify the configuration properties, such as the **`IP Address`** and **`Port`** of the device.

Step 5. Click `OK` to add the controller to the server.



Discovered

Device Name	Address	Device Type	Number Of Doors
Atlas - Atlas160-001761129585	10.79.164.209	NAC Controller	1

Add

Name	Type	Enabled	Ip Address	Port	Num Of Doors
Atlas - Atlas160-001761129585	N A C Controller	true	10.79.164.209	443	1

Name: Atlas - Atlas160-001761129585
Type: N A C Controller
Enabled: true
Ip Address: 10.79.164.209
Port: 443
Num Of Doors: 1

Adding NAC Controller Manually to Workbench

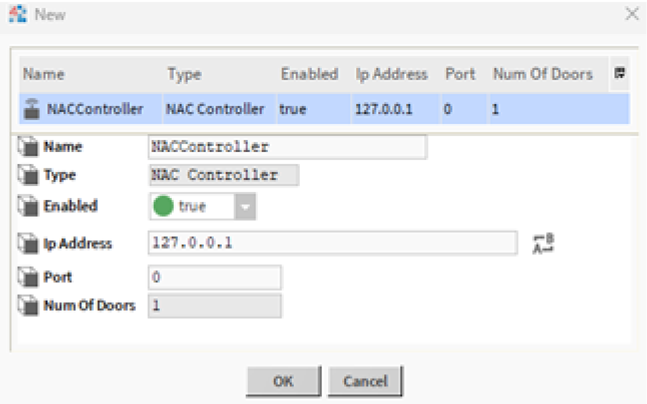
This topic explains the steps to add the NAC controller manually to the Workbench.

NAC Controller can be added and configured in two ways

1. Through Device Manager View.
2. Through Palette.

Step 1. Right-click on **ViewsNAC Network** > **Views** > **NAC Device Manager**.

Step 2. Click the **New** button on the Device Manager view.



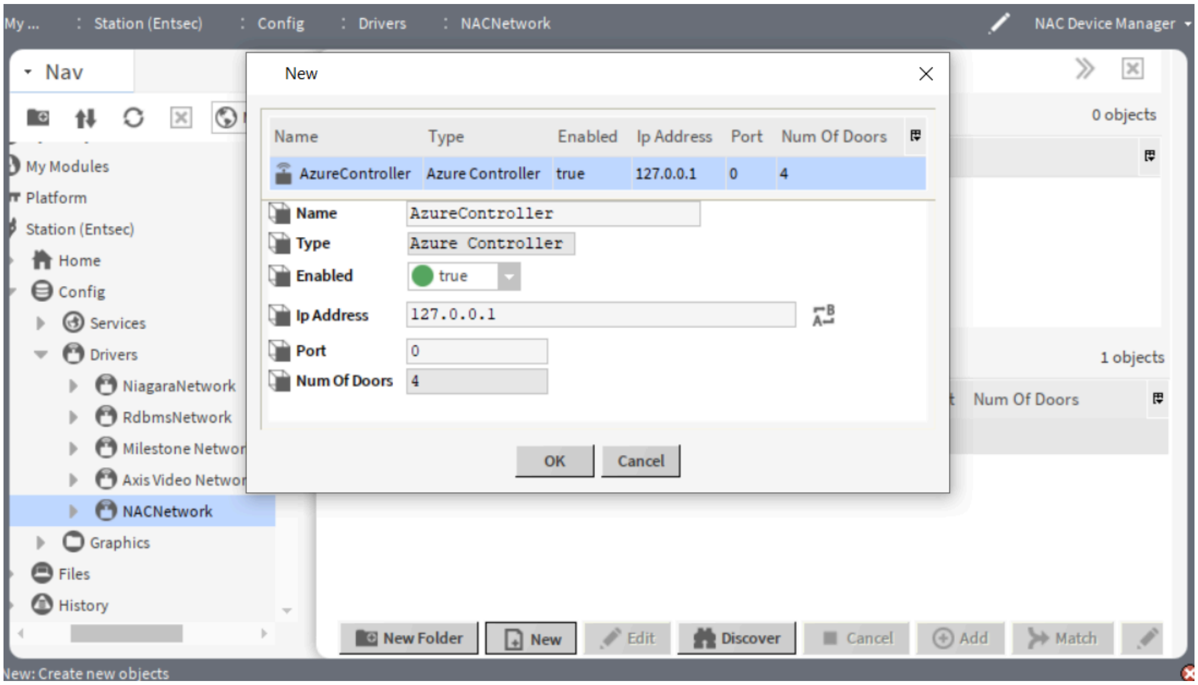
New

Name	Type	Enabled	Ip Address	Port	Num Of Doors
NACController	NAC Controller	true	127.0.0.1	0	1

Name: NACController
Type: NAC Controller
Enabled: true
Ip Address: 127.0.0.1
Port: 0
Num Of Doors: 1

The **New** window opens.

Step 3. Select the required controller from the drop-down list and click OK .



New

Name	Type	Enabled	Ip Address	Port	Num Of Doors
AzureController	Azure Controller	true	127.0.0.1	0	4

Name	AzureController
Type	Azure Controller
Enabled	● true
Ip Address	127.0.0.1
Port	0
Num Of Doors	4

OK Cancel

A second **New** window opens

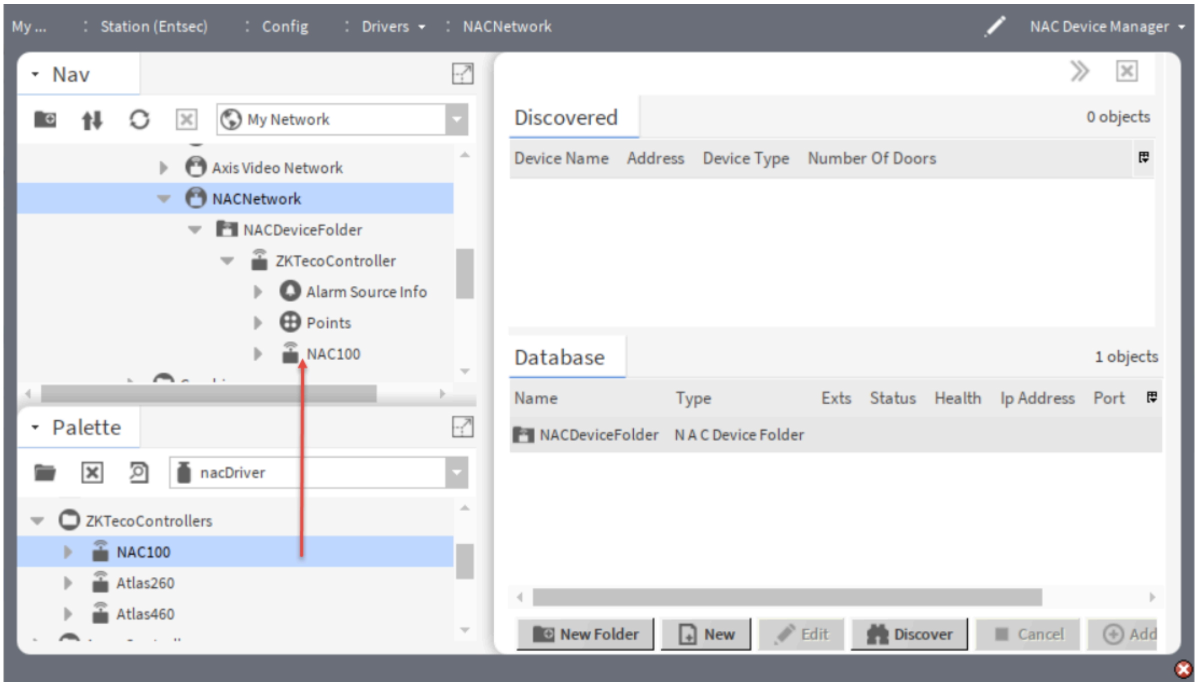
Step 4. Use this window to give the controller a unique name and click `OK` .
Follow the below steps to quickly add the device type directly from the palette.

Step 5. Open Workbench.

Step 6. Click on **Config** > **Drivers** > **NAC Network** under the station to open the Drivers view.

Step 7. Once the Drivers view is open, search for **nacDriver** in the palette's search bar.

Step 8. Drag the required controller type under the **NAC driver** to the Device Manager.



Discovered — 0 objects

Device Name	Address	Device Type	Number Of Doors

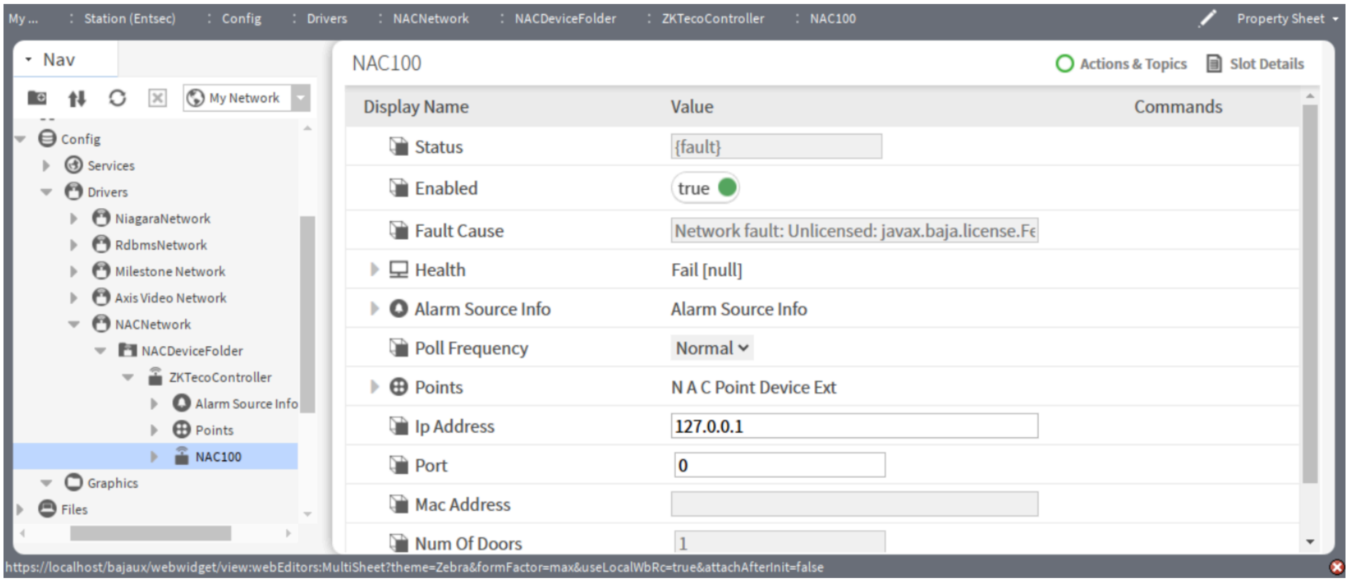
Database — 1 objects

Name	Type	Exts	Status	Health	Ip Address	Port
NACDeviceFolder	N A C Device Folder					

nacDriver-NACController

This component explains how to configure the NAC Controller.

Figure 15. NAC Controller Property Sheet



NAC100

Display Name	Value	Commands
Status	{fault}	
Enabled	true ●	
Fault Cause	Network fault: Unlicensed: javax.baja.license.Fe	
Health	Fail [null]	
Alarm Source Info	Alarm Source Info	
Poll Frequency	Normal	
Points	N A C Point Device Ext	
Ip Address	127.0.0.1	
Port	0	
Mac Address		
Num Of Doors	1	

https://localhost/bajaux/webwidget/view:webEditors:MultiSheet?theme=Zebra&formFactor=max&useLocalWbRc=true&attachAfterInit=false

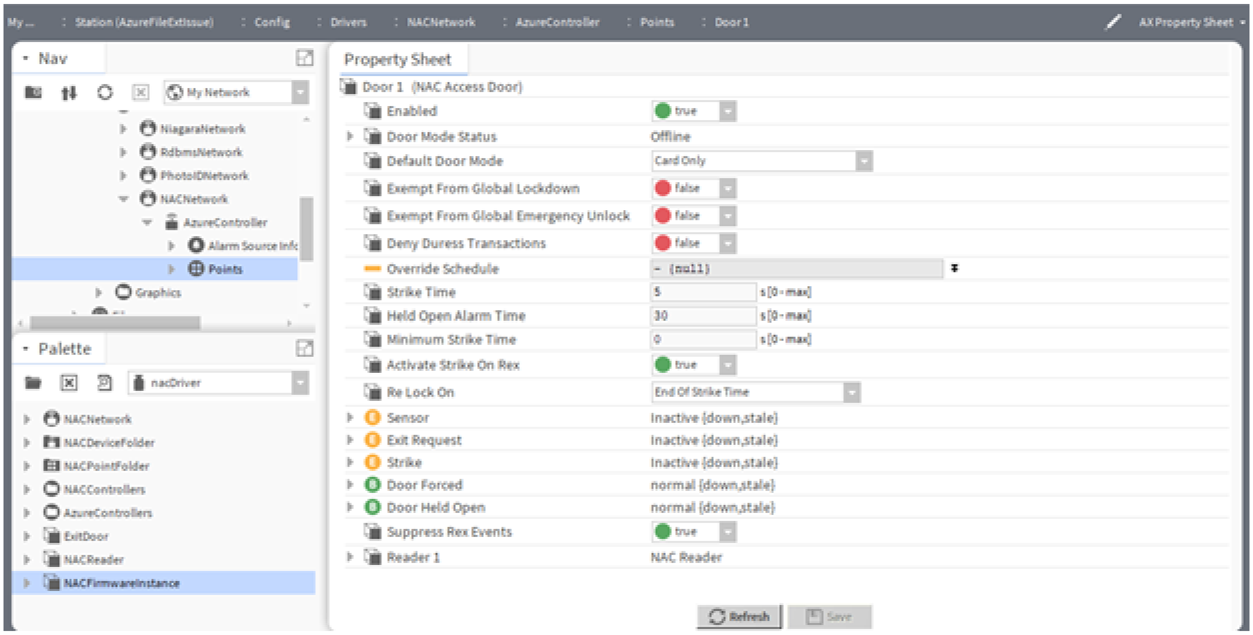
- Component Location:nacDriver Palette
- To access these properties, expand **Config** > **Drivers** > **NAC Network** > **NAC Device** > **NAC Controller** and right click the controller **Views** > **Property sheet.**
- Other than the standard properties (status, enabled, fault cause, health, Alarm Info, and poll frequency) these property supports the controller component.

Property	Value	Description
Points	Door, Reader, and other points of property	The folder space consists of NAC sensor points, NAC Device points and multiple door component based on the controller type (1, 2 ,4 Door Components). Refer Points Section for more details
IP Address	Read-only	Defines the IP address or host and port of the NAC Controller. The location can be on the network or elsewhere available on an intranet or the internet
Port	Read-only	Network port of the controller (all controllers would be updated with 443 by default)
Mac Address	Read-only	Corresponds to the MAC Address of the controller
Number of Doors	Read-only	Reports the Controller type like 1 Door, 2 Door or 4 Door and the maximum number of doors supported by the controller
Firmware version	Read-only	Represents standard controller firmware version

NAC Door Setup and Configuration

With the controller, the default access mode for the door is Card Only. But there are other modes also available like Card and Pin, Facility Code Only, Card and Bio, Card and Bio and Pin, Bio and Pin, Bio Only etc By default the Controller component consists of one Door component with **nacReader** component along with **NACDevicePoint** , **NACStrikePoint** and **NACSensorPoint**.

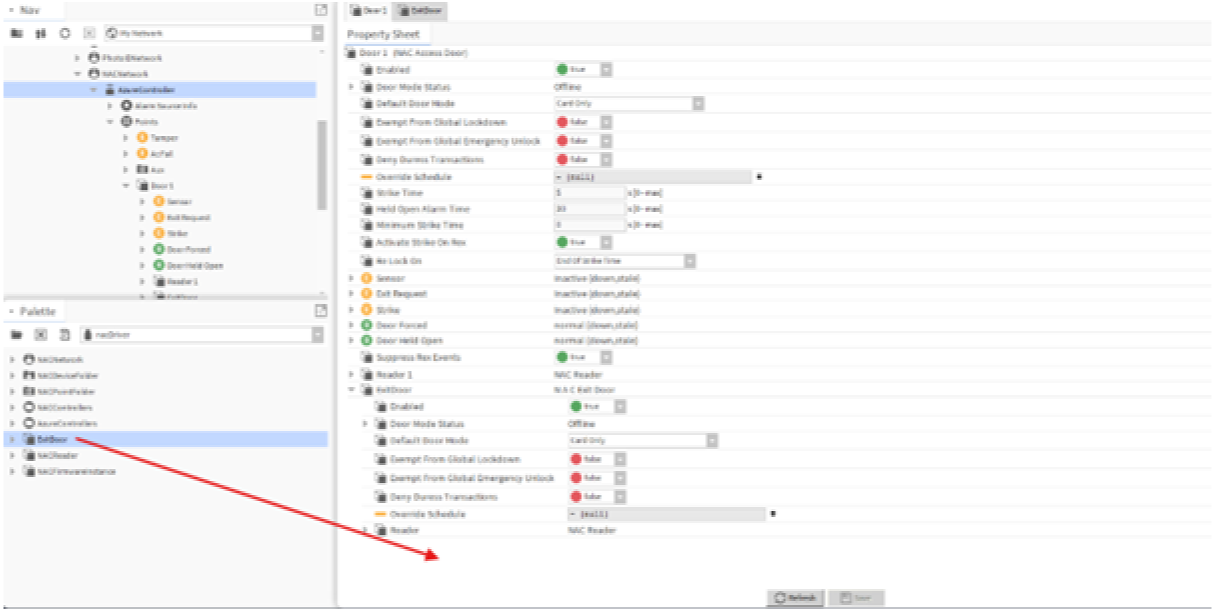
Figure 16. NAC Door



Door 1 (NAC Access Door)

Enabled	true
Door Mode Status	Offline
Default Door Mode	Card Only
Exempt From Global Lockdown	false
Exempt From Global Emergency Unlock	false
Deny Duress Transactions	false
Override Schedule	- {null}
Strike Time	5 s [0 - max]
Held Open Alarm Time	30 s [0 - max]
Minimum Strike Time	0 s [0 - max]
Activate Strike On Rex	true
Re Lock On	End Of Strike Time
Sensor	Inactive {down,stale}
Exit Request	Inactive {down,stale}
Strike	Inactive {down,stale}
Door Forced	normal {down,stale}
Door Held Open	normal {down,stale}
Suppress Rex Events	true
Reader 1	NAC Reader

If a door needs to be designated as an Exit Door, the Exit Door Extension must be added from the Palette.To add it, simply drag the **ExitDoor** Extension from the palette into the **NAC Door** View.



Door 1 (NAC Access Door)

Enabled	true
Door Mode Status	Offline
Default Door Mode	Card Only
Exempt From Global Lockdown	false
Exempt From Global Emergency Unlock	false
Deny Duress Transactions	false
Override Schedule	- {null}
Strike Time	1 s [0 - max]
Held Open Alarm Time	30 s [0 - max]
Minimum Strike Time	0 s [0 - max]
Activate Strike On Rex	true
Re Lock On	End Of Strike Time
Sensor	Inactive {down,stale}
Exit Request	Inactive {down,stale}
Strike	Inactive {down,stale}
Door Forced	normal {down,stale}
Door Held Open	normal {down,stale}
Suppress Rex Events	true
Reader 1	NAC Reader
ExitDoor	N A C Exit Door
Enabled	true
Door Mode Status	Offline
Default Door Mode	Card Only
Exempt From Global Lockdown	false
Exempt From Global Emergency Unlock	false
Deny Duress Transactions	false
Override Schedule	- {null}
Reader	NAC Reader

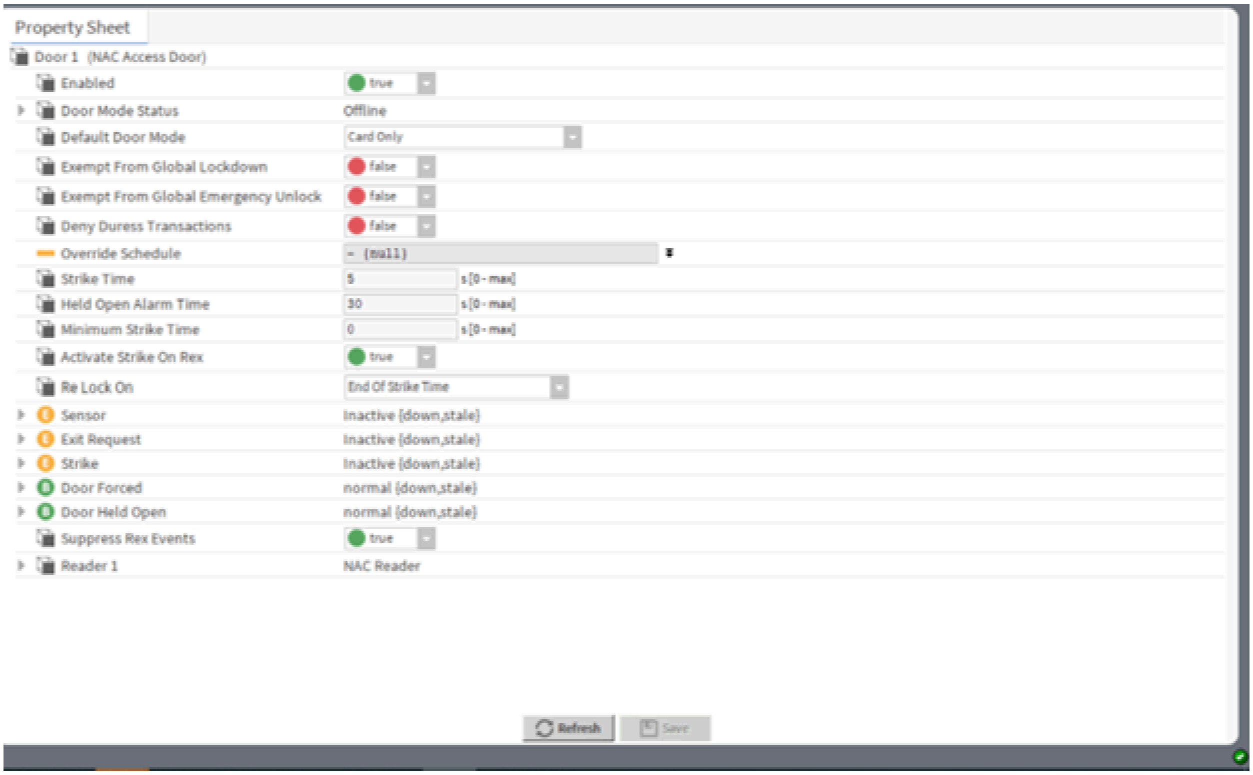
Exit Door can be configured as same as another door.

NOTE: Each Door component may include up to one Exit Door along with Readers. However, the Access Points associated with the Door component are shared between both the Access Door and Exit Door elements.

nacDriver nacDoor

The component provides the door configuration property for the **NAC Driver**. By default, the Controller component includes a single Door component, which is equipped with a **nacReader** component, as well as **NACDevicePoint**, **NACStrikePoint**, and **NACSensorPoint** elements.

Figure 17. NAC Door Property Sheet



Property Sheet

Door 1 (NAC Access Door)

Enabled	● true
Door Mode Status	Offline
Default Door Mode	Card Only
Exempt From Global Lockdown	● false
Exempt From Global Emergency Unlock	● false
Deny Duress Transactions	● false
Override Schedule	- {null}
Strike Time	5 s [0 - max]
Held Open Alarm Time	30 s [0 - max]
Minimum Strike Time	0 s [0 - max]
Activate Strike On Rex	● true
Re Lock On	End Of Strike Time
Sensor	Inactive {down,stale}
Exit Request	Inactive {down,stale}
Strike	Inactive {down,stale}
Door Forced	normal {down,stale}
Door Held Open	normal {down,stale}
Suppress Rex Events	● true
Reader 1	NAC Reader

- Component Location:nacDriver Palette
- To access these properties, expand **Config** > **Drivers** > **NAC Network** and right-click the Controller **Door** > **Views** > **Property sheet**.
- Other than the standard properties (Enabled and Door Mode Status) these property supports the controller component.
- If a door needs to be configured as an Exit Door, the Exit Door Extension must be added from the Palette.

Property	Value	Description
Default Door Mode	drop-down list	Contains door modes to access the door like Card and Pin, Facility Code Only, Card and Bio, Card and Bio and Pin, Bio and Pin, Bio Only, etc.
Exempt From Global Lockdown	true or false (default)	Specifies a particular door that is excluded from auto-locking after it is opened.
Exempt From Global Emergency Unlock	true or false (default)	Specifies a particular door to exclude from the emergency unlock doors.

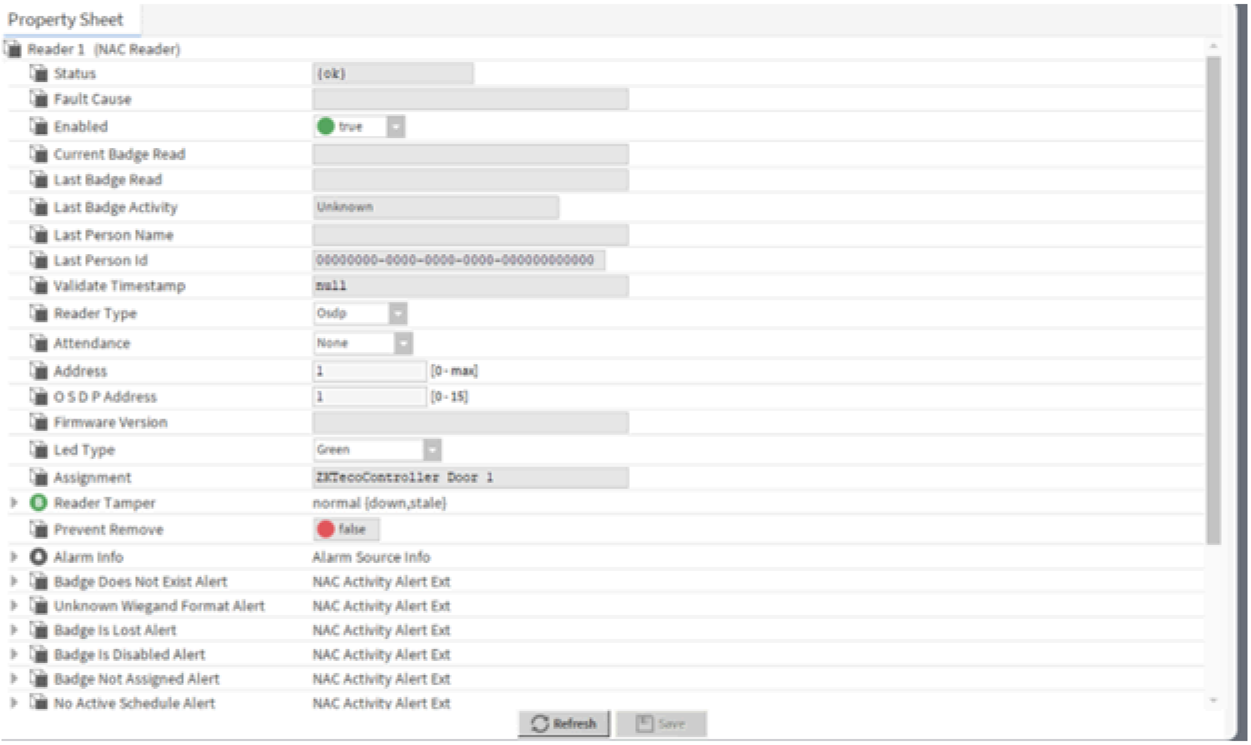
Property	Value	Description
Deny Duress Transactions	true or false (default)	Allows to open the door if more pressure applied.
Override Schedule	null (default), true or false	When null is enabled, reports the incoming value from the device. You cannot change this value. To change this value, click the double-arrow to the right and remove the null check mark.
Strike Time	hours minutes seconds (defaults to 5 seconds)	Sets the duration for the card swipe, ensuring it is maintained for the specified amount of time.
Held Open Alarm Time	hours minutes seconds (defaults to 30 seconds)	Configures how long the door may be held open before an alarm condition manifests.
Minimum Strike Time	hours minutes seconds (defaults to 0 seconds)	The card swipe must be maintained for at least the minimum specified duration
Activate Strike on Rex	true (default) or false	The strike is activated when a Request to Exit is initiated.
Re Lock On	drop-down list	Defines what should happen with a door that has just been unlocked. Relock on the End of Strike Time, and locks the door as soon as strike time ends. Relock on Door Open, lock the door as soon as it unlocks. Relock on Door Close, lock the door either after the Access Unlock Time expires (if the door has been unlocked but not opened) or when the door closes.
Sensor	Additional properties	Sensors are contact devices that monitor the state of a door
Exit Request	Additional properties	Normal exit from an access zone. Exit requests are devices that provide access to leave through a door without having to present a badge/card.
Strike	Additional properties	Defines the state of the door like lock is released or not

Property	Value	Description
Door Forced	Additional properties	Configures the Door Forced Extension to set the alarm-related properties.
Door Held Open	Additional properties	Configures the Door Held Open Extension to set the alarm-related properties.
Suppress Rex Event	true (default) or false	Suppresses the Exit Request events.
Reader	additional properties	This component is documented in a separate topic.

NAC Reader Setup and Configuration

The section addresses a way to configure the **NAC Reader** that is present under the **NAC Access Door**.

Figure 18. NAC Reader



Reader 1 (NAC Reader)

Status	{ok}
Fault Cause	
Enabled	● true
Current Badge Read	
Last Badge Read	
Last Badge Activity	Unknown
Last Person Name	
Last Person Id	00000000-0000-0000-0000-000000000000
Validate Timestamp	null
Reader Type	Osdp
Attendance	None
Address	1 [0 - max]
O S D P Address	1 [0 - 15]
Firmware Version	
Led Type	Green
Assignment	ZKTecoController Door 1
Reader Tamper	normal {down,stale}
Prevent Remove	● false
Alarm Info	Alarm Source Info
Badge Does Not Exist Alert	NAC Activity Alert Ext
Unknown Wiegand Format Alert	NAC Activity Alert Ext
Badge Is Lost Alert	NAC Activity Alert Ext
Badge Is Disabled Alert	NAC Activity Alert Ext
Badge Not Assigned Alert	NAC Activity Alert Ext
No Active Schedule Alert	NAC Activity Alert Ext

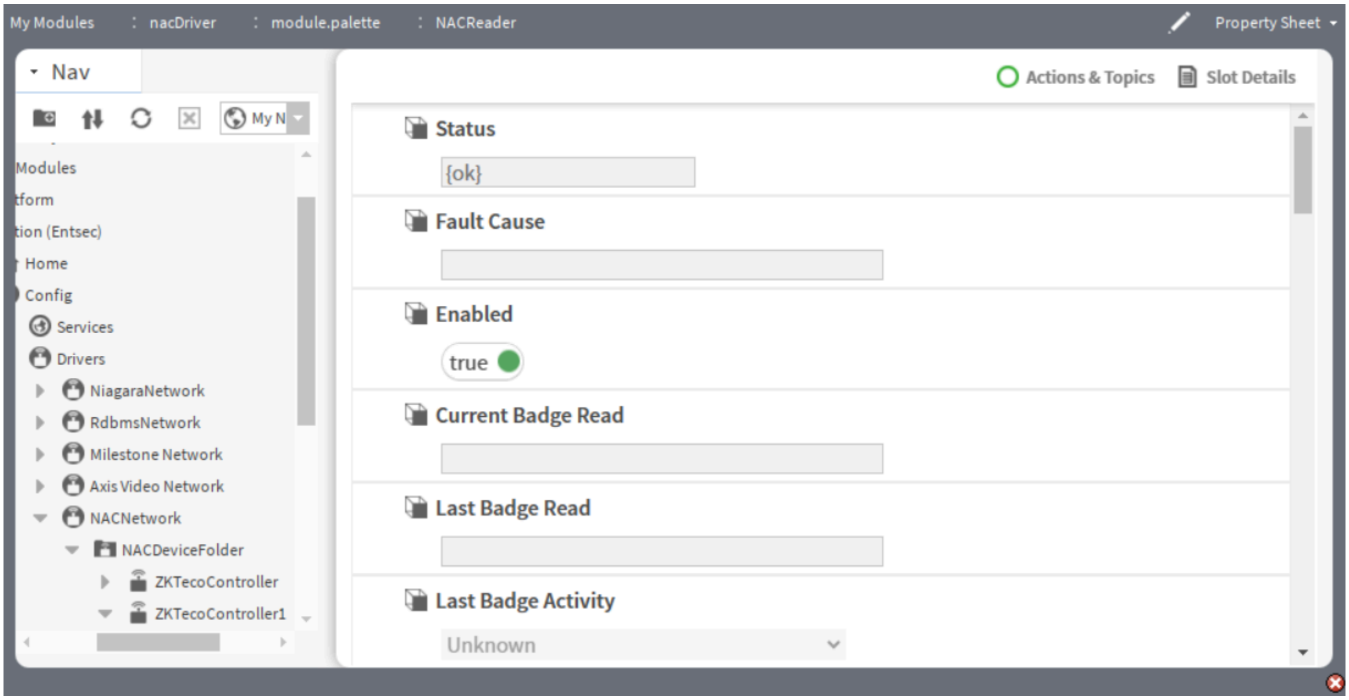
Configure the NAC Reader properties

1. Double-click on the Reader to open the Edit window.
2. Edit the reader configurations, including Name, Enable, Reader Type, Address, and OSDP Address.
3. Click `OK` to save the changes.

nacDriver-nacReader

The component provides the reader configuration property for the **NAC Driver**.

Figure 19. Nac Reader Property Sheet



Status: {ok}

Fault Cause:

Enabled: true ●

Current Badge Read:

Last Badge Read:

Last Badge Activity: Unknown

- Component Location:nacDriver Palette
- To access these properties, expand **Config** > **Drivers** > **NAC Network** and right-click the controller **Door** > **Views** > **Property sheet.**
- Other than the standard properties (status, enabled, fault cause) these property supports the controller component.

Property	Value	Description
Current Badge Read	read-only	Reports the number of the badge being processed now.
Last Badge Read	read-only	Reports the number of the last-read badge.
Last Badge Activity	read-only	Reports the last read or write using a badge.
Last Person Name	read-only	Reports the owner of the last badge read.
Last Person Id	read-only	Reports the ID of the owner of the last badge read.
Validate Timestamp	read-only	Reports when the system validated the badge.
Reader Type	drop-down	Allows to choose protocol as per controllers between O S D P and Wiegand format to read card data.
Attendance	drop-down	Allows selection of options: `None`,

Property	Value	Description
		`Check In`, and `Check Out` for recording attendance.
Address	number	Address for specific reader.
O S D P Address	number	Address of OSDP, if the reader is O S D P type.
Firmware Version	read-only	Displays current firmware version installed on controller.
Led Type	drop-down	The LED activates upon a card swipe, displaying either Green or a combination of Red and Green.
Assignment	read-only	Shows which door is assigned to the reader.
Reader Tamper	additional properties	Sets up the Reader Tamper Extension to define alarm-related properties in case the reader is tampered with.
Prevent Remove	false (default)	If the remove action is executed on a controller with an encrypted connection, a window appears to confirm whether or not to proceed with the removal.
Alarm Info	additional properties	Standard alarm-AlarmSourceInfo component.
Activity alert extensions	additional properties	Standard accessDriver-ActivityAlertExt. Each has the same set of alarm source info.

Chapter 8. Device configuration

Devices include doors, readers, and sensors and any other components that can be controlled by the Niagara Framework.

Discovering and adding access control modules

This procedure documents how to discover and add to the station database access control modules that are connected to an RS-485 serial bus.

Prerequisites:
You are working in a controller’s web UI.

Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Remote Modules** > **Remote Module Setup**.

Step 2. Click Discover ( ).
The discovery process displays the discovered modules in the lower Discovered pane.

Step 3. Select each individual module and click Add ( ).
The system adds the device to the station database.

Step 4. You can rename the module as you add it to the database and click **OK**.

Step 5. To verify that the device is online, right-click it in the Database pane and click `Wink Device` or select it and click Wink ( ).
The device responds.

Step 6. Instead of discovering modules, you can add each one individually by clicking Manage Devices ( ), selecting `Add` and clicking **OK**, selecting the type of device to add and clicking **OK**, giving the device a name and clicking **OK**,

Step 7. For each module, compare its firmware Installed Version and Available Version columns in the table.

Step 8. If a more recent firmware version is available, select the module, click Upgrade Firmware ( ), verify that the version successfully updated, and click **OK**.

Step 9. To save the station, click **Controller Setup** > **Miscellaneous** > **Controller Maintenance** > **Save Station**

Door configuration

Large companies may have thousands of doors. The procedures in this chapter configure single doors. You can use replication to automatically configure additional remote doors.

Doors are connected to modules, which are hardware components that connect to a controller to provide specialized functions. The devices that secure access doors and elevators connect to these modules.

Best Practice: During door configuration it is a good idea to save a station frequently. To save the current station, click **Miscellaneous** > **Controller Maintenance**, and click **Save Station**.

Configuring a door with an electric strike mechanism

This procedure configures a typical door mechanism that locks upon a loss of power.

Prerequisites:
The door to configure has a card reader with no keypad, a fail-secure electric door strike, a door sensor with alarm notification and a request to exit for shunt alarms only; it does not unlock. A schedule indicating when

the door is unlocked (for normal business hours) exists.

Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Remote Modules** > **Remote Module Setup**.

Step 2. Double-click the module to which the door and its reader are connected.
The Remote Reader Module tab opens.

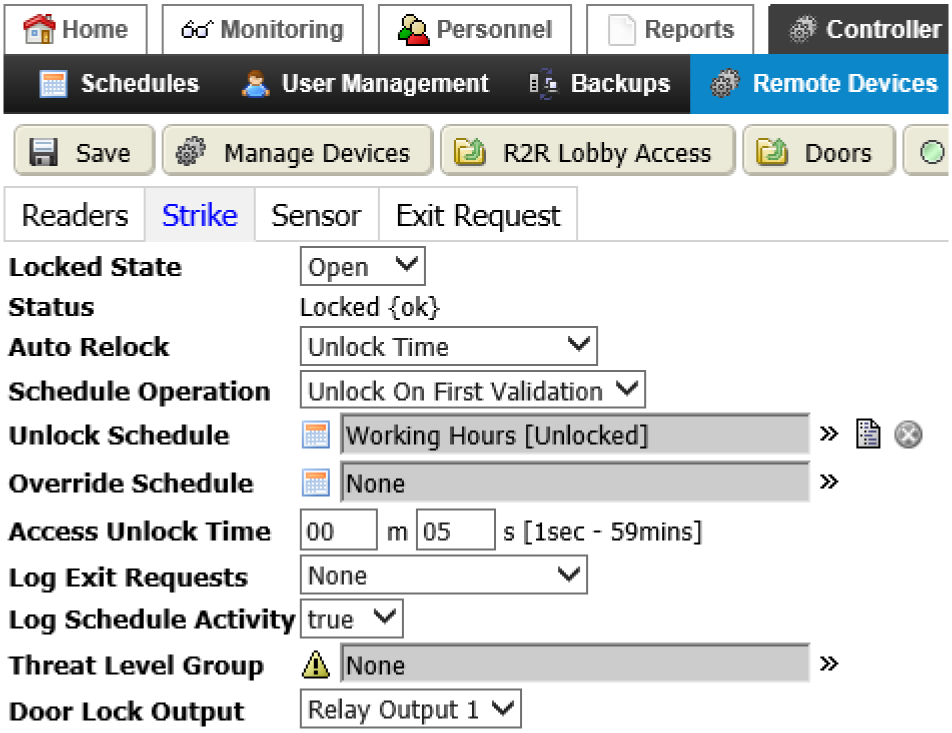
Step 3. To associate the reader with the door, set **`Enabled`** to `true` and click the Doors tab.
The Doors tab opens.

Step 4. To give the door(s) more descriptive names, click **Manage Devices**, select `Rename` and click **Ok**, select the door and click **Ok**, type in a name and click **Ok**.

Step 5. Click the hyperlink to the door view.
The Readers tab opens.

Step 6. To give the reader a more descriptive name, click **Manage Devices**, select `Rename` and click **Ok**, select the reader and click **Ok**, type in a name and click **Ok**.

Step 7. Click the Strike tab and configure its properties according to the screen capture using the company's Unlock Schedule.

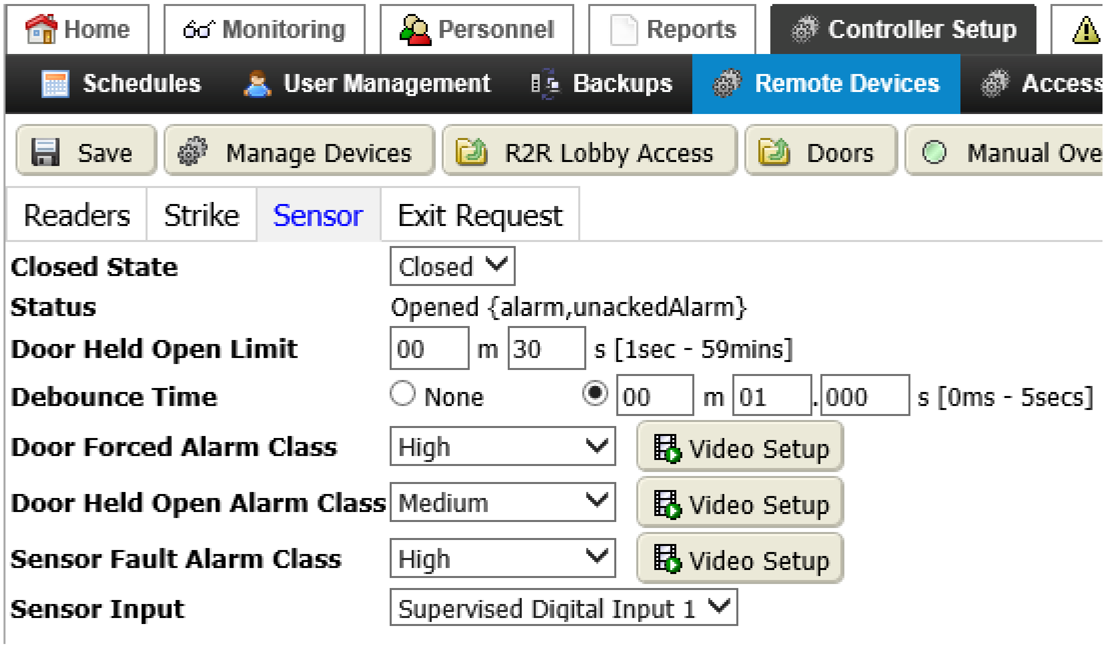


Locked State: Open
Status: Locked {ok}
Auto Relock: Unlock Time
Schedule Operation: Unlock On First Validation
Unlock Schedule: Working Hours [Unlocked]
Override Schedule: None
Access Unlock Time: 00 m 05 s [1sec - 59mins]
Log Exit Requests: None
Log Schedule Activity: true
Threat Level Group: None
Door Lock Output: Relay Output 1

`Schedule Operation` requires a schedule so that the system can identify the first validation, which triggers unlocking the door.

The **`Door Lock Output`** value depends on the hardware configuration.

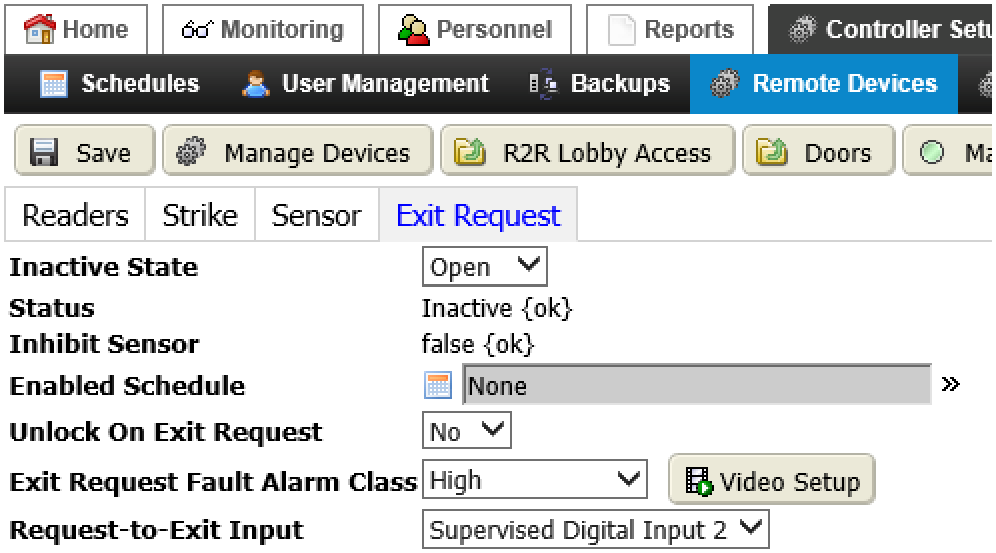
Step 8. Click the Sensor tab and configure the properties according to the screen capture.



Closed State	Closed
Status	Opened {alarm,unackedAlarm}
Door Held Open Limit	00 m 30 s [1sec - 59mins]
Debounce Time	○ None ● 00 m 01 .000 s [0ms - 5secs]
Door Forced Alarm Class	High
Door Held Open Alarm Class	Medium
Sensor Fault Alarm Class	High
Sensor Input	Supervised Digital Input 1

The **`Sensor Input`** value depends on the hardware configuration.

Step 9. Click the Exit Request tab and configure the properties according to the screen capture.



Inactive State	Open
Status	Inactive {ok}
Inhibit Sensor	false {ok}
Enabled Schedule	None »
Unlock On Exit Request	No
Exit Request Fault Alarm Class	High
Request-to-Exit Input	Supervised Digital Input 2

The **`Request-to-Exit`** value depends on the hardware configuration.

Step10. To save the configuration, click **Save** and test the door.

Configuring a door with a mag lock

This procedure configures a door equipped with a mag lock. The contact closes to lock the door.

Prerequisites:
The door has a card reader with no keypad, a magnetic door lock (fail safe), a door sensor with alarm

notification and a request to exit for shunt alarms only (it does not unlock). A schedule exists, which indicates when the door is unlocked (for normal business hours).

Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Remote Modules** > **Remote Module Setup**.

Step 2. Double-click the module to which the door and its reader are connected.
The Remote Reader Module tab opens.

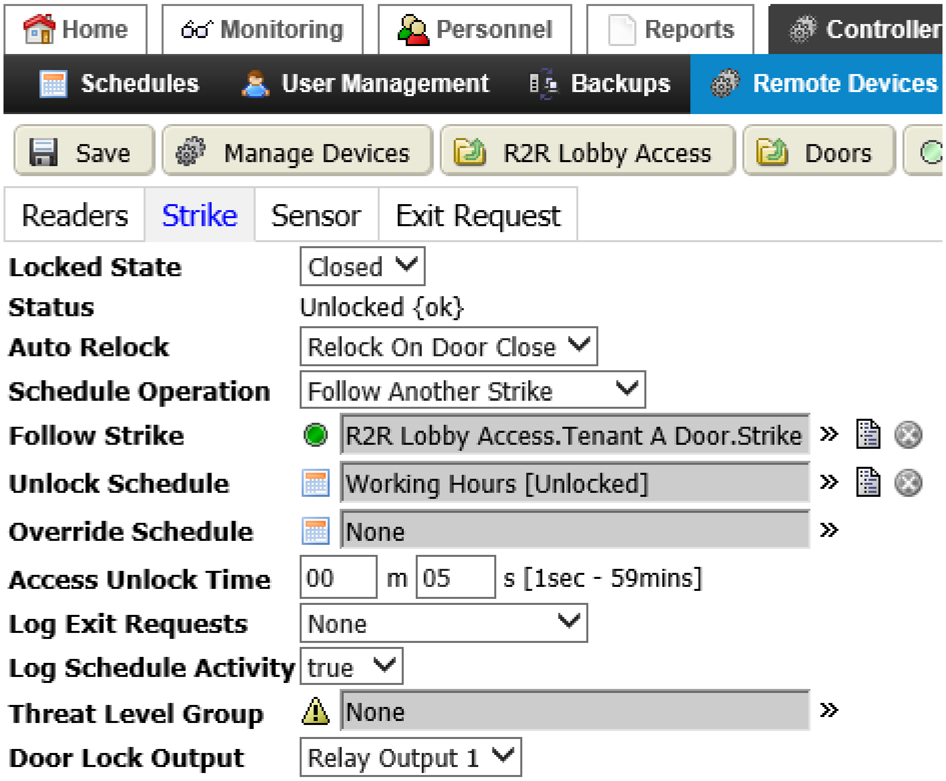
Step 3. To associate the reader with the door, set **`Enabled`** to `true` and click the Doors tab.
The Doors tab opens.

Step 4. To give the door a more descriptive name, click **Manage Devices**, select `Rename` and click **Ok**, select the door and click **Ok**, type in a name and click **Ok**.

Step 5. Click the hyperlink to the door view.
The Readers tab opens.

Step 6. To give the reader a more descriptive name, click **Manage Devices**, select `Rename` and click **Ok**, select the reader and click **Ok**, type in a name and click **Ok**.

Step 7. Click the Strike tab and configure its properties according to the screen capture.

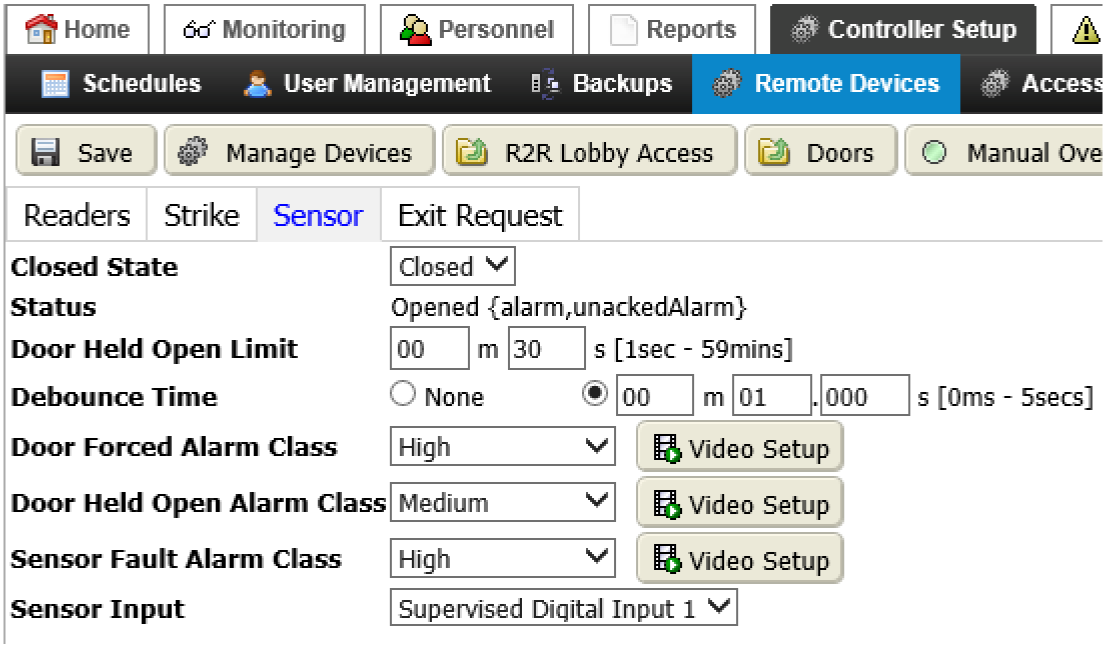


Locked State	Closed
Status	Unlocked {ok}
Auto Relock	Relock On Door Close
Schedule Operation	Follow Another Strike
Follow Strike	R2R Lobby Access.Tenant A Door.Strike
Unlock Schedule	Working Hours [Unlocked]
Override Schedule	None
Access Unlock Time	00 m 05 s [1sec - 59mins]
Log Exit Requests	None
Log Schedule Activity	true
Threat Level Group	None
Door Lock Output	Relay Output 1

A **`Schedule Operation`** of Follow Another Strike requires you to identify the door whose strike this door follows (**`Follow Strike`**). The **`Door Lock Output`** relay depends on the hardware configuration.

The **`Door Lock Output`** value depends on the hardware configuration.

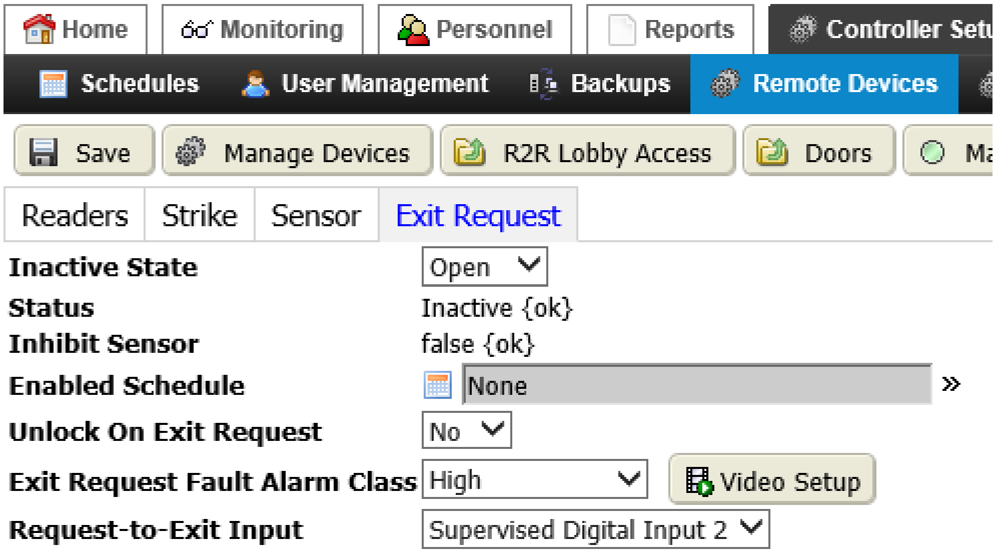
Step 8. Click the Sensor tab and configure the properties according to the screen capture.



Closed State	Closed
Status	Opened {alarm,unackedAlarm}
Door Held Open Limit	00 m 30 s [1sec - 59mins]
Debounce Time	○ None ● 00 m 01 .000 s [0ms - 5secs]
Door Forced Alarm Class	High
Door Held Open Alarm Class	Medium
Sensor Fault Alarm Class	High
Sensor Input	Supervised Digital Input 1

The **Sensor Input** value depends on the hardware configuration.

Step 9. Click the Exit Request tab and configure the properties according to the screen capture.



Inactive State	Open
Status	Inactive {ok}
Inhibit Sensor	false {ok}
Enabled Schedule	None »
Unlock On Exit Request	No
Exit Request Fault Alarm Class	High
Request-to-Exit Input	Supervised Digital Input 2

The **Request-to-Exit** value depends on the hardware configuration.

Step10. To save the configuration, click **Save** and test the door.

Configuring a monitored exit door

The system can monitor doors and lock them in case of a loss of power. A sensor (balanced magnetic switch) monitors this door, but its lock is purely mechanical.

Prerequisites:

The door has no card reader, no door strike, no ability to receive an exit request, but it has a sensor with alarm notification.

Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Remote Modules** > **Remote Module Setup**.

Step 2. Double-click the module to which the door is connected.
The Module tab opens.

Step 3. Click the Doors tab.

Step 4. Click **Manage Devices**, select `Rename` and click **Ok**, select the door and click **Ok**, give the door a descriptive name, and click **Ok**.

Step 5. Click the hyperlink for the door.
Reader, strike and request-to-exit functions are not needed for this door. The various inputs and outputs that are normally reserved for those functions are available for use elsewhere.

Step 6. Click **Manage Devices**, select `Delete` and click **Ok**, select the reader associated with this door, and click **Ok**.

Step 7. Confirm that the Readers tab is no longer available.
If you need another relay output somewhere else in the configuration, you can delete the strike for this door. RO2 will then be available on theAdditional Points tab for the module. There is no harm in allowing the Strike tab to remain with everything set to the defaults.

If you need another supervised digital input somewhere else in the configuration, you can delete the request to exit for this door. SDIn will then be available on the Additional Points tab for the module.

Step 8. If you choose not to delete the request to exit, set the **`Exit Request Fault Alarm Class`** on the Exit Request tab to `Off Alarm Class` to prevent nuisance alarms.

Testing a door

This procedure tests the configuration to ensure it is working as expected.

Step 1. While viewing the Strike tab, click **Manual Override**, select an **`Override Type`** and confirm that the **`Status`** changes to `Unlocked` as expected:

- For a door with an electric strike mechanism, the mechanism energizes the strike magnet to lock the door after the override **`Time`**.
- For a door with mag lock, the contact closes to lock the door after the override **`Time`**.

Step 2. While viewing the Sensor tab, open and close the door to verify that the sensor reports when the door is open.

Step 3. Assign a schedule on the Strike tab that sets up the door to be currently locked, then open the door.

Step 4. On the Sensor tab, verify that the sensor generates a door forced alarm.

Step 5. Open the alarm console and acknowledge the alarm.

Step 6. While viewing the Exit Request tab, issue a request to exit through the door and verify that **`Status`** changes to `Active` and that, even though the schedule indicates the door should be locked, the sensor does not generate an alarm.

Result

Best practice: All doors should be configured to function the same way regardless of the locking mechanism.

Reader configuration

Readers are associated with doors.

Best Practice: During reader configuration it is a good idea to save a station frequently. To save the current station, click **Miscellaneous** > **Controller Maintenance**, and click **Save Station**.

Adding a reader

This procedure adds an existing reader to the station database.

Prerequisites:
You are using the web UI. The reader has been installed next to the door.

Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Remote Modules** > **Remote Module Setup**.

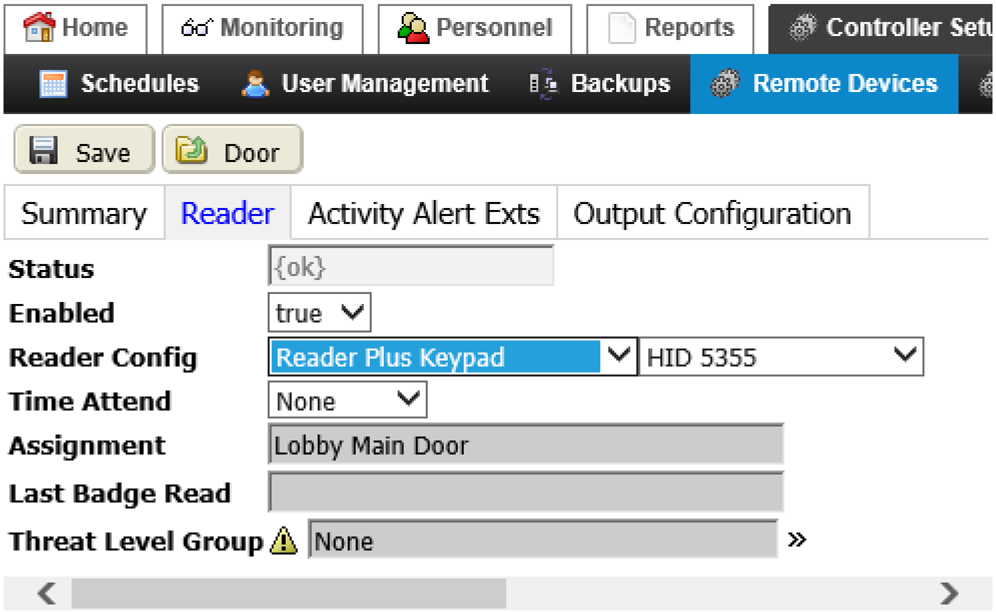
Step 2. Double-click the module to which the door and its reader are connected.
The Remote Reader Module tab opens.

Step 3. To associate the reader with the door, set **`Enabled`** to `true` and click the Doors tab.
The Doors tab opens.

Step 4. Click Manage Devices (⚙), and, select **Add**, and click **Ok**.

Step 5. Select the reader, click **Ok**, name the reader and click **Ok**.
The software creates the reader.

Step 6. Click the reader hyperlink, followed by clicking the Reader tab.
The Reader view opens.



Status	{ok}	
Enabled	true	
Reader Config	Reader Plus Keypad	HID 5355
Time Attend	None	
Assignment	Lobby Main Door	
Last Badge Read		
Threat Level Group ⚠	None	

Step 7. After configuring reader properties, configure the Activity Alert Exts and Output Configuration tabs, then click **Save**.

Assigning a reader and floor to an access right

Each access right supports readers and floors. The association between an access right and its reader(s) tells a Supervisor which of its subordinate stations needs the Orion data. A controller that is wired to a reader and affiliated with a particular access right stores the data required to grant access to personnel who have the right to swipe their badges at its readers.

Prerequisites:
You are working in the web UI. You have already created one or more access rights. You have set up doors,

readers and floors.

Step 1. Click **Personnel** > **Access Rights**.
The Access rights view opens with the list of access rights.

Step 2. Double-click an access right and click the Readers tab.
The assignment view opens.

Step 3. Click the Assign Mode button (▤)
The Unassigned pane opens and populates it with reader records.

Step 4. Select the reader to associate with the access right, and click the Assign button (⊕).
The reader record moves from the Unassigned to the Newly Assigned pane.

Step 5. If the access right applies to a specific floor, click the Floors tab.
The Floors discovery view opens.

Step 6. Click the Assign Mode button (▤)
The system opens the Unassigned pane and populates it with floor records.

Step 7. Select the floor to associate with the access right, and click the Assign button (⊕).
The floor record moves from the Unassigned to the Newly Assigned pane.

Step 8. Click the **Save** button.
The access right is saved and the Summary tab opens.

Step 9. Verify that the correct readers and floors (at the bottom of the view) are assigned to the access right.

Configuring entry and exit readers for attendance tracking

Readers cause doors to open or remain closed based on scanning the information presented to the reader on a badge. They provide the information the Personnel department needs to tract attendance.

Prerequisites:
A door has an electric door strike, a sensor with alarm notification, and entry and exit readers with no keypads. The door's request to exit shunts alarms only. It does not unlock.

Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Remote Modules** > **Remote Module Setup**.

Step 2. Double-click the module to which the door and its reader are connected.
The Remote Reader Module tab opens.

Step 3. Click the Doors tab and click the door's hyperlink.
The Doors tab opens.

Step 4. Configure the Strike, Sensor, and Exit Request tabs as follows and click **Save**.

Tab	Property	Value
Strike	**Locked State**	Open
	Auto Relock	Relock On Door Open
	Schedule Operation	Normal
	Unlock Schedule	None
	Override Schedule	None
	Door Lock Output	Relay Output 1 (depends on your configuration)
Sensor	**Closed State**	Closed
	Door Held Open Limit	30 Sec
	Door Forced Alarm Class	High
	Door Held Open Alarm Class	Medium
	Sensor Fault Alarm Class	High
	Sensor Input	Supervised Digital Input 1 (depends on your configuration)
Exit Request	**Inactive State**	Open
	Enabled Schedule	None When no schedule is assigned, the system enables a request-to-edit by default.
	Unlock On Exit Request	No
	Exit Request Fault Alarm Class	High
	Request-to-Exit Input	Supervised digital Input 2 (depends on your configuration)

Step 5. To give an existing reader a more descriptive name, click **Manage Devices**, select Rename and click **Ok**, select the reader and click **Ok**, type in a name and click **Ok**.

Step 6. To add a reader, click **Manage Devices**, select Add and click **Ok**, select a reader and click **Ok**, type in a name and click **Ok**.
To add a reader, you must have already installed the hardware.

Step 7. Click the entry reader's hyperlink, configure its properties, then click the exit reader's hyperlink and configure its properties. Click **Save** after configuring each set of properties.

Tab	Property	Value
Reader	**Enabled**	true
	Reader Config	Reader Only
	Time Attend	Clock In for the entry reader and Clock Out for the exit reader
	Assignment	(defaults to name of the door)
Activity Alerts Exts	for all alarms: **Alarm Class**	Medium
	for all alarms: **Enable Logging**	(selected)
Output Configuration	**Valid Green**	Follow Strike State
	Green Inactive State	Open
	Red Inactive State	Closed
	Valid Beeper	Custom Time, On 1 Sec
	Invalid Beeper	Custom time, On 2 Sec
	Beeper Inactive State	Open
	Beeper on Door Held Open Alarm	Warning Only with warning time: 15 seconds before the door-held-open alarm sounds. Activating the beeper-on-door-held-open alarm reminds employees to shut the door, saving energy and preventing anything else from entering the building.

Input/output: configuring a roof hatch sensor

In addition to door-monitoring sensors, the system supports other sensors, including roof hatch sensor, motion detector, glass break sensor and auxiliary door sensor using input and output points. A roof hatch sensor provides an example of how to configure these types of sensors.

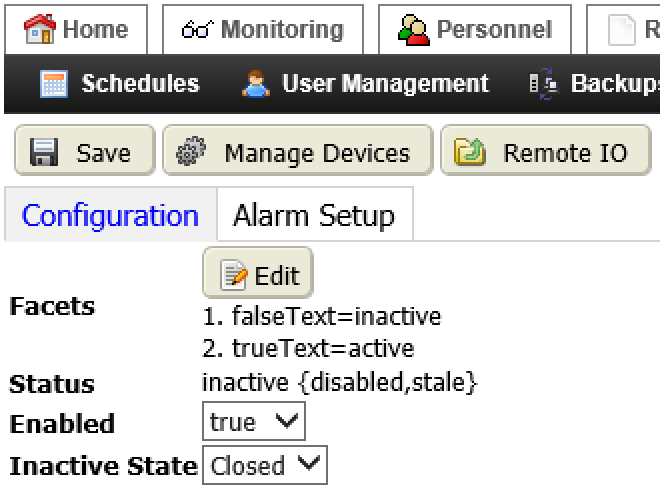
Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Remote Modules** > **Remote Module Setup**.

Step 2. Double-click the remote I/O module to which the sensor is connected.
The tab opens.

Step 3. Click the Additional Points tab.

Step 4. Identify the input point to use and give it a more descriptive name by clicking **Manage Devices**, selecting `Rename` and clicking **Ok**, selecting the input name and clicking **Ok**, typing in a name and clicking **Ok**.

Step 5. Click the input point’s hyperlink.
The tab opens.



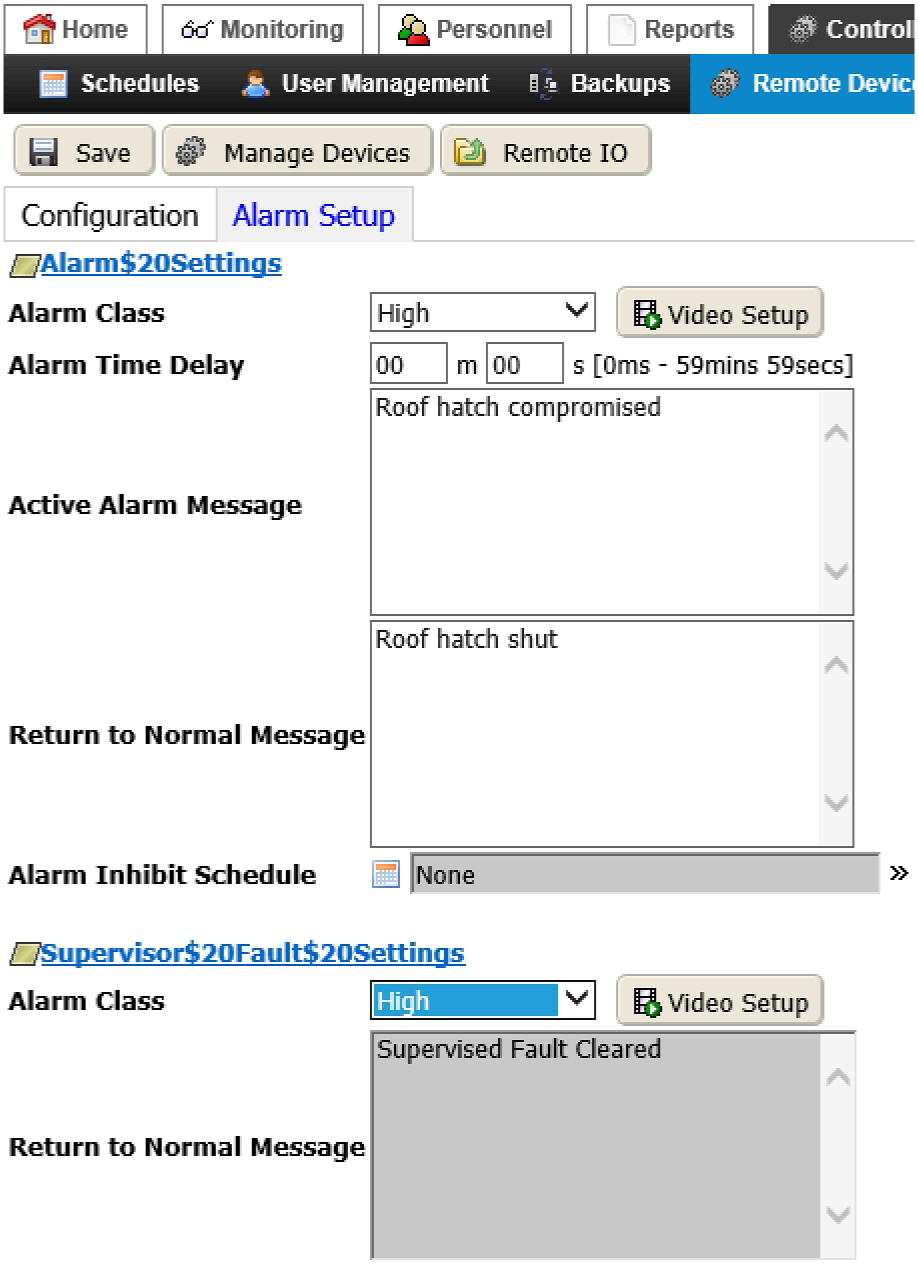
Facets 1. falseText=inactive
2. trueText=active
Status inactive {disabled,stale}
Enabled true
Inactive State Closed

Step 6. Verify the facets: `falseText=inactive`, `trueText=active`

Step 7. Set **`Inactive State`** to `closed`.

Step 8. Set **`Enabled`** to `true` .

Step 9. Click the Alarm Setup tab and configure the roof hatch alarm.



Alarm$20Settings

Alarm Class: High

Alarm Time Delay: 00 m 00 s [0ms - 59mins 59secs]

Active Alarm Message: Roof hatch compromised

Return to Normal Message: Roof hatch shut

Alarm Inhibit Schedule: None

Supervisor$20Fault$20Settings

Alarm Class: High

Return to Normal Message: Supervised Fault Cleared

Step10. Save the configuration.

Motion, glass break, and auxiliary door sensors

The following properties provide examples of how to configure individual sensors.

Motion detector

Tab	Property	Value
Configuration	**Facets**	trueText=active, falseText=inactive
	Enabled	true
	Inactive State	Closed
Alarm Setup	**Alarm Settings Alarm Class**	High Priority

Tab	Property	Value
	Active Alarm Message	Motion detected office
	Return to Normal Message	No motion
	Alarm Inhibit Schedule	Business Hours (or the equivalent)
	Supervisor Fault Alarm Class	High Priority

Glass break sensor

Tab	Property	Value
Configuration	**Facets**	trueText=active, falseText=inactive
	Enabled	true
	Inactive State	Closed
Alarm Setup	**Alarm Settings Alarm Class**	High Priority
	Active Alarm Message	Broken window office
	Return to Normal Message	none
	Alarm Inhibit Schedule	none
	Supervisor Fault Alarm Class	High Priority

Auxiliary door sensor

Tab	Property	Value
Configuration	**Facets**	trueText=active, falseText=inactive
	Enabled	true
	Inactive State	Closed
Alarm Setup	**Alarm Settings Alarm Class**	High Priority
	Active Alarm Message	Auxiliary door open
	Return to Normal Message	Auxiliary door shut
	Alarm Inhibit Schedule	none
	Supervisor Fault Alarm Class	High Priority

Converting a BA station into a Enterprise Security station

A BA (Building Automation) station manages analog and digital inputs from automation devices and components. A Enterprise Security station manages a limited set of access-control components. Converting Supervisor and controller stations to Enterprise Security stations involves installing services and setting up users.

Prerequisites:
You are working in Workbench on a PC that is connected to the network.

Step 1. Open a platform connection to the platform (PC or controller).
A controller platform may be named for its IP address or domain.

Step 2. Connect to the station (PC or controller) you wish to convert.

Step 3. Expand the **Config** > **Services** folders in the Nav tree.

Step 4. If needed, open the Palette (click **Window** > **Side Bars** > **Palette**).

Step 5. Drag the following services from the appropriate palettes to the **Services** folder in the Nav tree.

Palette	Service component
orion	OrionService
entsec	Enterprise Security Service
entsec	AccessControlService
entsec	ReplicationService
entsec	Intrusion Service
entsec	Intrusion SmartKeyService (controller only)

Step 6. Set up an admin user with specific properties.

Property	Value
Nav file	module://entsec/rc/entsecHome.nav
Role	admin
Default Web Profile	Standard Access Profile
Hx Theme	Lucid

Building control integration

Building logic manages a facility's mechanical and electrical systems, such as its HVAC and lighting.

By associating an integration ID with the access right exercised by a person when they enter an access zone, the system can automatically turn on lights and the building's HVAC system.

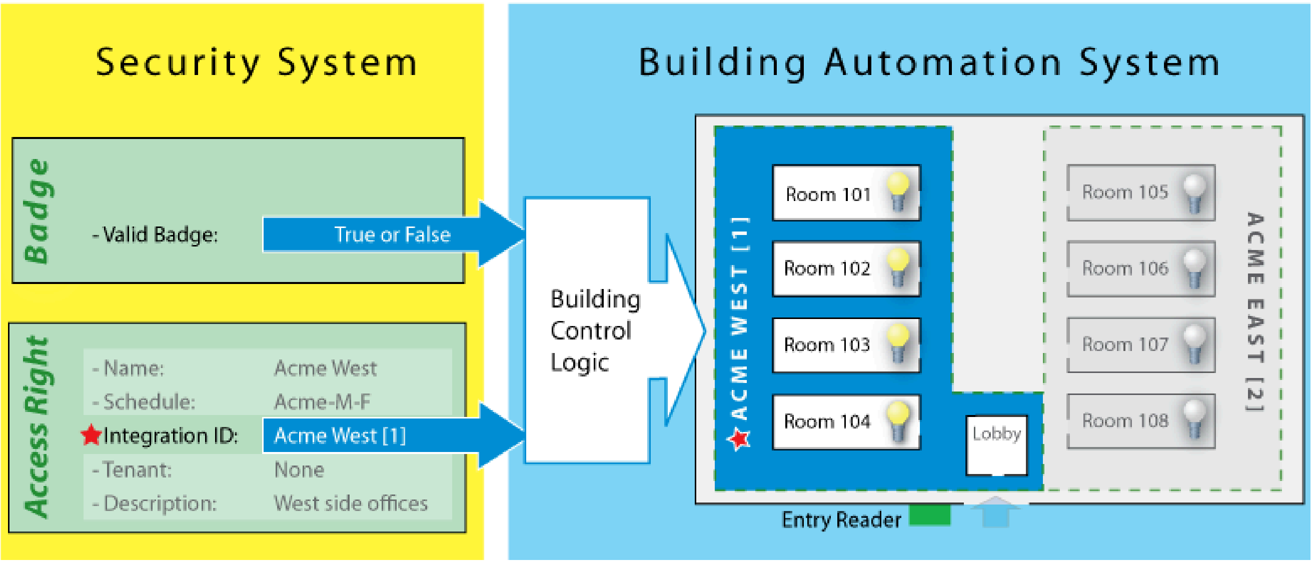
Integration IDs link an access right to the building's control logic. As an option for any access right, an administrator creates a unique integration ID (name and integer value) and assigns it to an access right. When a person exercises the access right to enter the building, the integration ID integer value is available to the building control logic. The integration ID value may be used, along with a valid badge value to initiate HVAC and lighting controls for the areas appropriate to the person or group that is represented by the integration ID.

NOTE: The valid badge property has a `true` or `false` state that defaults to `false` until an authorized, active badge is swiped at an appropriate reader. When this occurs, the property status changes to `true` momentarily (2 seconds by default). This property is only available in Workbench under the reader. You use it in wiresheet logic to determine when a person with valid access has used a reader

An access right may contain only one integration ID. Since many persons may share an access right, they also share the access right integration ID. Therefore, access rights with integration IDs are typically defined and named in terms of the common physical location that persons occupy.

For example, two access rights: Acme West and Acme East might relate to two sides of a single floor in the Acme building. Persons with different access rights may enter the building through a common door and actually have the same overall access to the building. However, if the different access rights contain unique integration IDs, they can trigger building controls to turn on lighting in the west side offices for the west side occupants and the east offices for east side occupants, as appropriate.

Figure 20. Niagara Integration ID



The graphic illustrates a person whose access right identifies an integration ID value of Acme West [1]. The person enters the Acme building using a valid badge. The Building Automation System picks up the ValidBadge=True and IntegrationID=AcmeWest[1] property values from the system (possibly over a BACnet network) and the building control logic triggers a boolean control to turn on the west-side office lights.

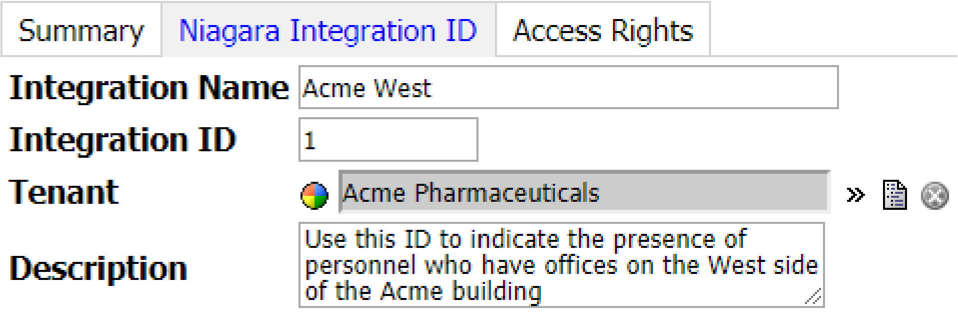
Creating access rights with integration IDs

The following example can be performed from the system's browser interface by an administrator with proper credentials.

Prerequisites:
You are working in a controller station and using the web UI. You have people and one or more schedules in the database.

Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Niagara Integration IDs.**

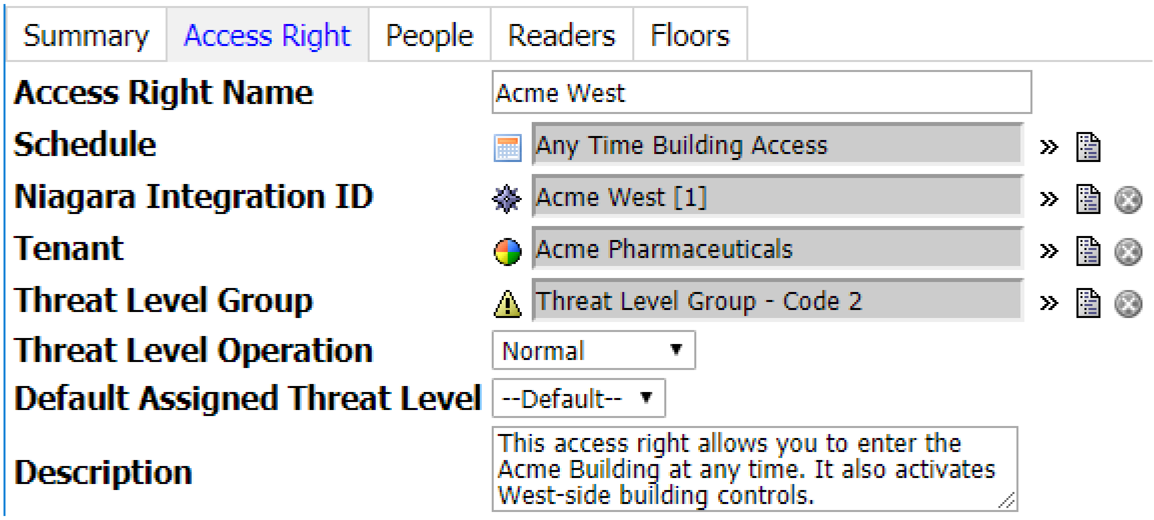
Step 2. To create an integration ID, click Add (⊕).
The Niagara Integration ID tab opens.



Integration Name	Acme West
Integration ID	1
Tenant	Acme Pharmaceuticals
Description	Use this ID to indicate the presence of personnel who have offices on the West side of the Acme building

Step 3. To create an access right, click **Personnel** > **Access Rights**, click Add (⊕).

A blank Access Right tab opens.



Access Right Name	Acme West
Schedule	Any Time Building Access
Niagara Integration ID	Acme West [1]
Tenant	Acme Pharmaceuticals
Threat Level Group	Threat Level Group - Code 2
Threat Level Operation	Normal
Default Assigned Threat Level	--Default--
Description	This access right allows you to enter the Acme Building at any time. It also activates West-side building controls.

NOTE: For convenience, name the access right the same name as the integration ID. Access right and integration ID names do not have to match.

Step 4. Fill in the blanks. Assign the Niagara Integration ID you created to this access right.

Step 5. Click the Readers tab, click the Assign Mode button ( ), select the desired reader from the Unassigned list and click the Add button ( ), and click **Save**.

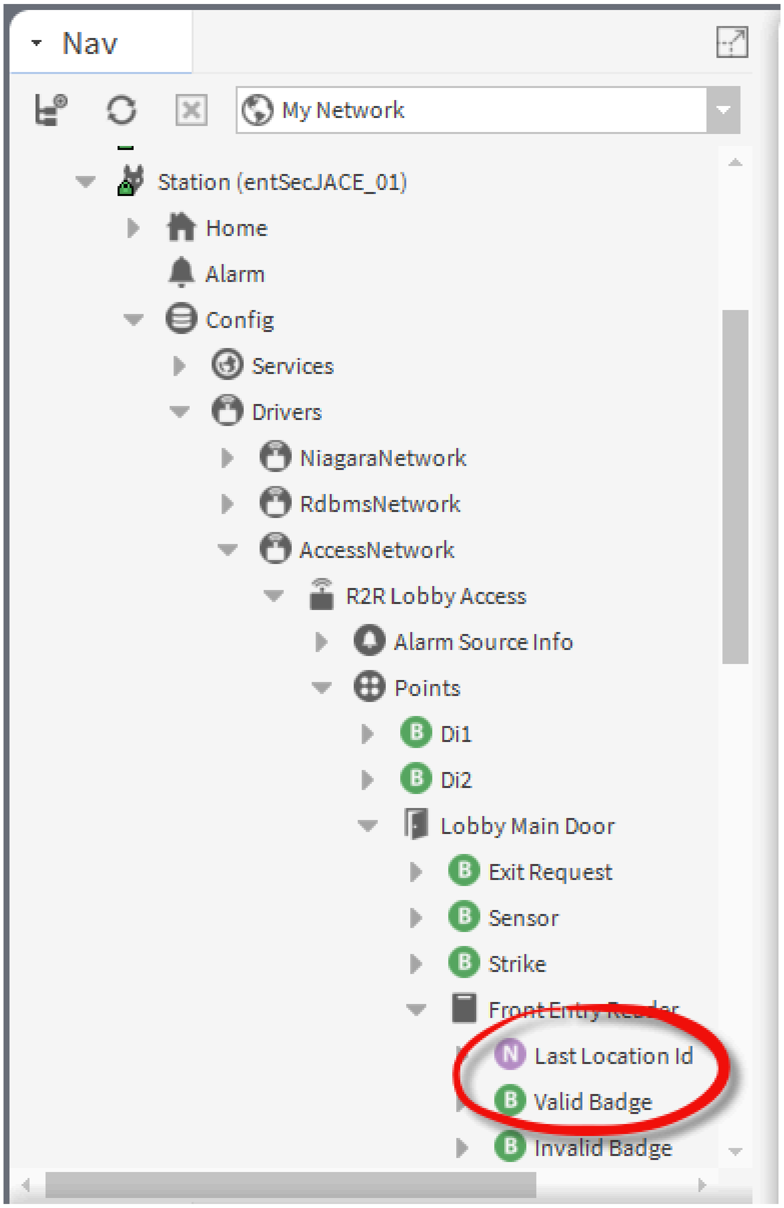
Step 6. To assign an access right to a person, click the People tab, double-click a person or select the person and click Hyperlink ( ), click the Access Rights tab, click the Assign Mode button ( ), select the access right assigned to the integration ID, and then click **Save**.

Setting up building control logic to use integration IDs

The following example is provided for system integrators using Workbench.

Prerequisites:
Workbench is open with network access to both the Enterprise Security system and the building control stations.

Step 1. In the station, navigate to **Config** > **Drivers** > **AccessNetwork** and expand the module, points, door and reader that you are using for access integration (from a Supervisor station, perform point discovery, if necessary).

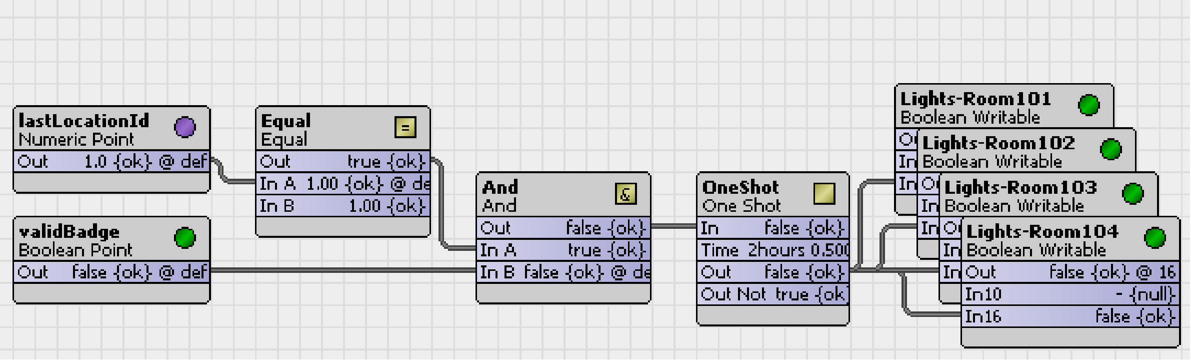


- **Last Location Id** contains the integration ID value of the last badge that was presented at the reader.
- **Valid Badge** has a Boolean value output that provides a two-second (default) pulse when a valid badge is presented.

Step 2. Using the **Last Location Id** and **Valid Badge** points as inputs, create logic on a Workbench wire sheet that requires both of the following to be `true`:

- **Last Location Id** (lastLocationId) value must equal the value of the targeted location. Multiple locations can be defined as a group with a single value. This is the value that the integration ID from the access right must match.
- **Valid Badge** (validBadge) value must be set to `true`. The badge-holder must be authorized as having access at the targeted building door.

The combination of these two pieces of information indicate that an authorized person entered the space and the occupation area associated with the person. The following simple wiresheet illustration provides an example of logic that could be used to turn on lighting when an authorized person gains access to an area.



Chapter 9. Supervisor/controller connections

Once a controller has been configured, and users, schedules and access rights have been set up, it is time to establish communication between a controller and Supervisor stations, and synchronize the Orion database (HSQL) in the controller with the Orion data (MySQL or MS SQL) in the Supervisor PC. This chapter is not necessary for small companies with a single access controller.

The system's discovery feature (learn mode), initiated from a Supervisor station, finds controllers on the local subnet. Discovery is not possible when controller stations are on the other side of a router. Since an Ethernet cable is limited to 300 ft (90 m) and large systems may have multiple routers, it is almost certain that the system cannot discover all the stations in a large network. In addition to discovering remote stations, you may need to manually add stations to the Supervisor.

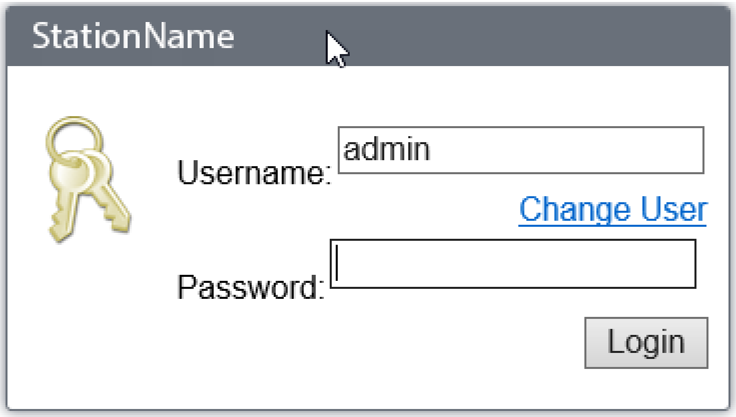
The device management features are not available in a Supervisor station where configuration is called System Setup as opposed to Controller Setup.

Logging in to the Supervisor station using the web UI

The first time you log in the Supervisor station using the web UI (browser), a setup wizard can prompt configuration options.

Prerequisites:
You have opened one of the supported browsers. Your database exists and is ready to use. You have admin rights.

Step 1. In the browser address bar, type the address of the Supervisor station (`localhost` , if using your PC) and press **Enter**.
The login window opens.



StationName

Username: admin

Password:

`Username` defaults to `admin` .

Step 2. Enter your credentials (**`Username`** and **`Password`**), and click **Login**.
You set up the password when you created the Supervisor station.

Step 3. If the station's **Enterprise Security Service** component's **`Init Required`** property is set to `true`, the wizard asks you to confirm the station and system display name, and the network settings before proceeding.
Any change to platform settings requires a reboot.

Step 4. Click each of the wizard buttons in order.
For each button, the wizard opens the appropriate station view for configuring the password, database, and other properties.

Creating a Supervisor machine-to-machine user

A machine-to-machine (M2M) user in the Supervisor station sets up network communication without requiring human intervention.

Prerequisites:
You are working in the Supervisor station using the web UI.

Step 1. Navigate to **System Setup** > **User Management** > **Users**, and click Add (⊕).
The User tab opens.

Step 2. Configure at least the **User Name**, **Password** and confirm that **Enabled** is be set to `true`, **Password Expiration** is set to `Never Expires`, and **Authentication Scheme Name** is set to `DigestScheme`.

Step 3. Click the Roles tab and select the `Admin` role for this user and click **Save**.

Defining a display name for a Supervisor station

A **Station Display Name** adds an easily-understood text name for the station that conforms to the building owner's technical jargon. The **Station Name**, which you entered when you created the Supervisor station from a template conforms to a more cryptic technical convention with industry abbreviations, acronyms and labels.

Prerequisites:
You are connected to the Supervisor station and working in the web UI.

Step 1. Click **System Setup** > **Miscellaneous** > **Network TCP/IP Settings**.

Step 2. Enter a descriptive **Station Display Name** and a **System Display Name**.
The **System Display Name** refers to the whole installation. Often, this is the company name or system name for the whole company. These names should differentiate the Supervisor station from all controller station in the network.

Step 3. Click the **Update Display Names** button.

Editing station information

This procedure configures login credentials and other properties in the Supervisor station's database.

Prerequisites:
This procedure requires the Supervisor station.

Step 1. Expand **System Setup** > **Remote Devices** > **Station Manager**.

Step 2. Select the station in the Database pane and click the Edit button (✎).

Step 3. Configure these properties: Login credentials and other properties for replicating a configuration to one or more remote hosts, or for configuring the joining of a remote station to the Supervisor.

Configuring network settings

Check with your network administrator before setting up or changing network properties.

Prerequisites:

NOTE: If you are changing network properties, write down any changes you make so that you can reach the changed remote controller after rebooting.

Step 1. Navigate to **Controller (System) Setup** > **Miscellaneous** > **Network TCP/IP Settings.**
The Display Names and Network Settings view opens. These names specify two separate titles that appear in the top right area of the browser. The **Station Display Name** precedes the **System Display** name, which also serves as a link to the Home view.

Step 2. Type names and click the **Update Display Names** button.
The names appear in the top right corner of the title bar. The **Interfaces** properties are displayed under the Network Settings heading in the lower part of the view. The following steps are for the TCP/IP settings located directly under the DHCPv4 option list. On initial setup, these properties contain the temporary factory-shipped IP Address.

CAUTION: Do not enable DHCP unless you are certain that the network has DHCP servers! Otherwise, the controller may become unreachable over the network. In general (for stability), it is better to use static IP addressing instead of DHCP, if possible.

Step 3. For **IPv4 Address**, assign an IP address to the controller that is unique for the network you are installing it on.
No other device on the network should use the same IP address.

Step 4. For **IPv4 Subnet Mask**, assign the appropriate subnet mask used by the LAN.

Step 5. Review, and if needed, adjust other TCP/IP settings.

Step 6. To save your changes, click the **Apply Changes and Reboot** button.
The controller reboots to complete the network changes. During a reboot, the controller station's display name (top right corner of the user interface) dims while the station is unavailable. The display name returns to the normal color when the station is restarted.

Configuring the database in the Supervisor station

The Supervisor station must be connected to a running database. If you connected the system database using the Guided Setup Wizard, your database may not require additional configuration. This separate procedure documents how to configure the database, which may be running on the same computer as the Supervisor, or it may be running on a remote computer.

Prerequisites:
You are logged in to the Supervisor station using the web UI with admin privileges. A database of the appropriate type exists. You have configured the RDBMS network for secure communication.

CAUTION: Communication between the database and the Supervisor station must always be available, otherwise the software will not work. Communication must also be secure.

Step 1. From the Supervisor Home, click **System Setup** > **Miscellaneous** > **Configure Database.**
The Configure Database view opens with a Database Services tab, and a MySQLDatabase (the default) tab. No database tab displays if no database driver is installed.

Step 2. Configure the important database services properties at the bottom of the Database Services tab: **Replication Failure Alarm**, **Replication Overrun Alarm**, and **Replication Overrun Limit**.
These properties apply to all databases installed on this Supervisor's network.

Step 3. To add or delete a database, click **Manage Databases.**
The **Manage Databases** window opens.

Step 4. Select the `Delete` or `Add` option and click **Ok.**
The system lists the existing database tabs.

Step 5. Select the database to add or delete and click **Ok.**
Only one database can be enabled at any one time. To use a database other than MySQL, such as the MSSQL database, delete the MySQL database.

Step 6. Enter the database name and click **Ok.**

The software adds the database as a tab to the view. This is the name of the MySQL or MS SQL database you configured before installing the software.

Step 7. Select the database tab, enable the database and configure at least these properties: **`Host Address`**, **`User Name`**, **`Password`**, and **`Database Name`**.

- Host Address identifies the location of the database, which may be on the same computer as the system software or in another location on the network.
- User Name and Password are the credentials you set up when you created the database schema using MySQL or MS SQL. For MySQL, User Name should be a unique name other than “root.”
- Database Name is the unique name you created using MySQL or MS SQL.

The database services are configured and you should now have a Database Services tab and a specific database tab that matches the MySQL or MS SQL database you are connecting to.

Step 8. Confirm that **`Use Encrypted Connection`** is set to `true`, and click **Save** at the top of the view. This property provides flexibility should you need to turn off secure encrypted communication.

CAUTION: For normal operation, this property defaults to true, otherwise your data can be compromised by someone with malicious intent.

Step 9. Click the **Set Orion Database** button, select the database you just configured from the drop-down list and click **Ok**.

CAUTION: Changing the Orion database removes ALL DATA from any current Orion database. After designating the Orion database, you must restart the Supervisor station.

Step10. Click **Restart Station**, and click **Ok** to confirm the restart.
The station restarts. The station name, visible at the top right corner of the interface, changes color or dims until the station is available again. After station restart, the station name displays in the normal color.

Establishing two-way communication using discovery

The first step in setting up a network is to establish secure communication between the controller station and the Supervisor station.

Prerequisites:
You are working in the Supervisor station using the web UI.

Step 1. To connect to the Supervisor station (localhost), open a browser and enter the address: `localhost`.
The web UI opens to the **Login** window.

Step 2. Enter your PC (localhost) credentials, and click **Login**.
The web UI home view opens.

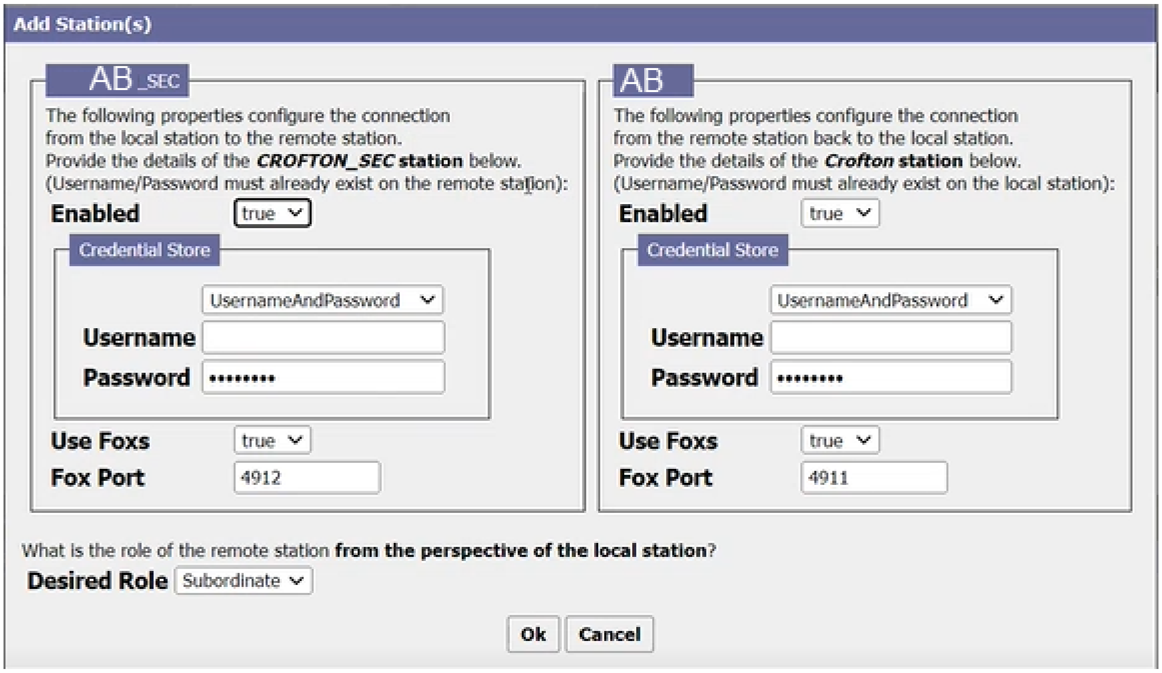
Step 3. Click **System Setup** > **Remote Devices** > **Station Manager**, and verify that the Discover button ( ) is active (not grayed out).

Step 4. Click Discover ( ).
The Supervisor station broadcasts a call, and all stations on the local subnet (not on the other side of a router) respond. As each remote station identifies itself, the system populates the Discovered pane, indicating that the Station Manager is in learn mode.

Because of each station’s configuration, communication can only occur using a secure (HTTPS) port.

CAUTION: This discovery job may take several minutes to complete, depending on the number of stations on the network and network speed. Do not refresh or close the view until the job completes. Failure to allow the job to complete may result in duplicate or incomplete record sets in the Supervisor’s station manager database.

Step 5. Select the station in the Discovered pane and click Add ( ).
The Add Station(s) window opens.



Add Station(s)

AB_SEC

The following properties configure the connection from the local station to the remote station. Provide the details of the ***CROFTON_SEC* station** below. (Username/Password must already exist on the remote station):

Enabled true

Credential Store

UsernameAndPassword

Username

Password ••••••••

Use Foxs true

Fox Port 4912

AB

The following properties configure the connection from the remote station back to the local station. Provide the details of the ***Crofton* station** below. (Username/Password must already exist on the local station):

Enabled true

Credential Store

UsernameAndPassword

Username

Password ••••••••

Use Foxs true

Fox Port 4911

What is the role of the remote station **from the perspective of the local station**?

Desired Role Subordinate

This window sets up the network account for the Supervisor and all selected stations. The properties on the left are for the Supervisor station. The properties on the right are for the controller station.

Step 6. Read the sentence above **`Desired Role`** carefully and make sure you understand that, from the perspective of the Supervisor (local station), the controller station is a `Subordinate` station.

Step 7. When you have configured both sides for secure communication (**`Use Foxs`** = `true` and **`Fox Port`** = `4911`), click **Ok**.
The system saves the configuration and returns to the Station Manager view.

Step 8. To verify the connection, select the station and click Ping ( ).
The system confirms the state of the connection.

Establishing two-way communication manually

Establishing a connection between a remote station to a Supervisor station prepares the two for a join or replicate. The software assumes a peer relationship, that is, it assumes you are connecting two remote stations. To connect a remote station to a Supervisor station requires the definition of the remote station's role in the relationship.

Prerequisites:
Both stations are running. You are working in the Supervisor station running on a PC.

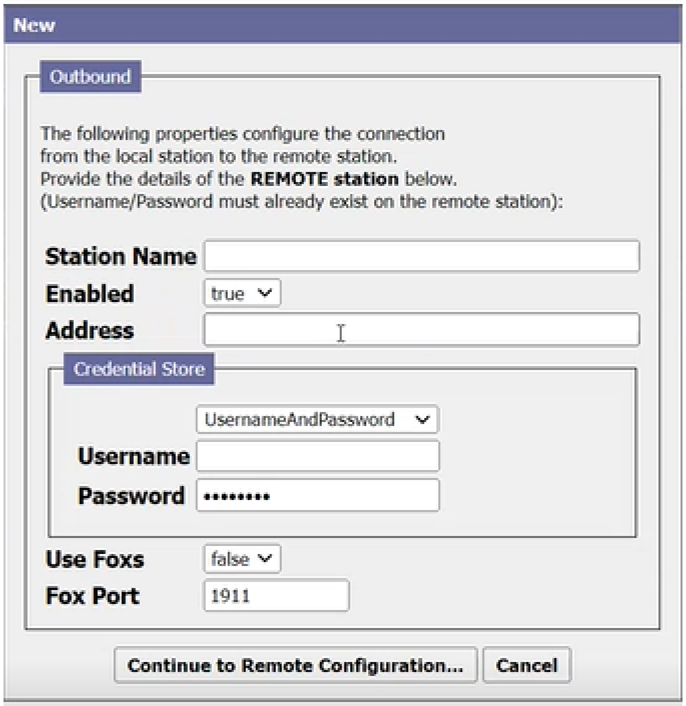
Step 1. Open your browser and log in to the Supervisor station (localhost).

Step 2. Using the same browser, log in to the controller station.

Step 3. In the Supervisor station, click **System Setup** > **Remote Devices** > **Station Manager**.
The Station Manager view opens.

Step 4. Click the New button ( ).

The **New** connection window opens.



The following properties configure the connection from the local station to the remote station. Provide the details of the **REMOTE station** below. (Username/Password must already exist on the remote station):

Station Name

Enabled true

Address

UsernameAndPassword

Username

Password ••••••••

Use Foxs false

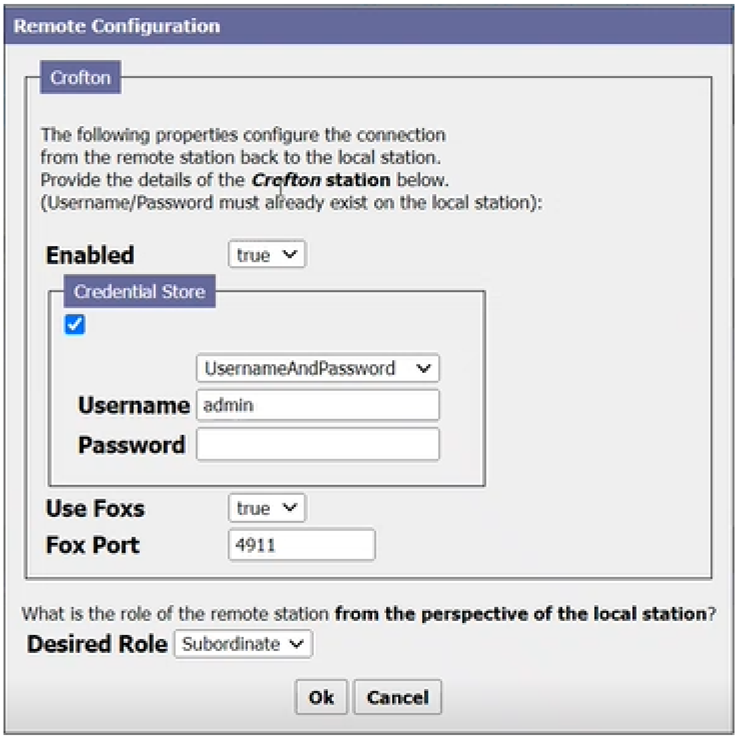
Fox Port 1911

This window configures the information about the remote controller that the Supervisor needs to connect to the remote.

Step 5. Fill in the properties as follows and click **Continue to Remote Configuration...**.

- **`Station Name`** is the name of the remote station.
- **`Enabled`** must be set to `true`.
- **`Address`** is the IP address of the remote controller.
- **`Username`** and **`Password`** are the credentials for logging in to the remote station. The example uses the credentials for an M2M (Machine-to-Machine) user.
- **`Use Foxs`** set to `true` and **`Fox Port`** set to `4911` together configure the connection for secure communication.

The system connects the Supervisor to the remote station and opens the Remote Configuration window from the standpoint of the remote station.



Remote Configuration

Crofton

The following properties configure the connection from the remote station back to the local station. Provide the details of the **Crofton station** below. (Username/Password must already exist on the local station):

Enabled true

Credential Store

☑

UsernameAndPassword

Username admin

Password

Use Foxs true

Fox Port 4911

What is the role of the remote station **from the perspective of the local station**?

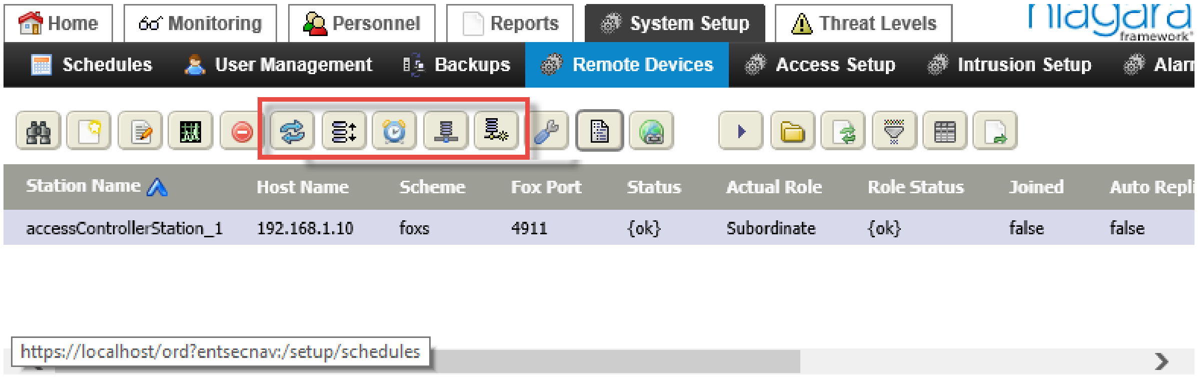
Desired Role Subordinate

Step 6. Fill in or confirm the properties as follows, then click **Ok**.

- **`Enabled`** must be set to `true`.
- The credentials are those that the Supervisor station requires.
- **`Use Foxs`** set to `true` and **`Fox Port`** set to `4911` together configure the connection for secure communication.
- Desired Role defines the role that the remote station assumes in relationship to the Supervisor station. This role defaults to `Subordinate`.

The system attempts to connect back to the Supervisor station. If it does not work, try connecting from the controller, then connect again from the Supervisor. You will notice the differences in the above windows.

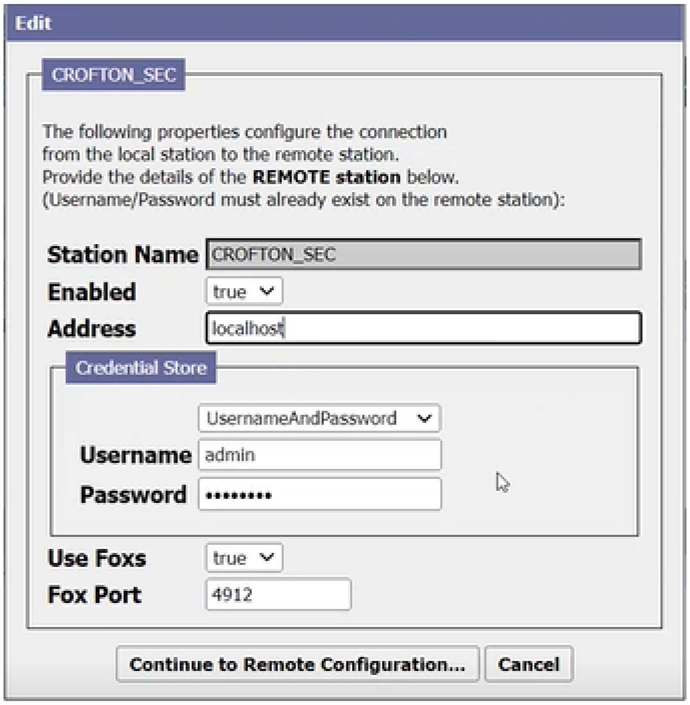
Whether or not the stations connect, the remote station appears in the Station Manager view of the Supervisor station and the Supervisor appears in the Station Manager view of the remote station.



Station Name	Host Name	Scheme	Fox Port	Status	Actual Role	Role Status	Joined	Auto Repli
accessControllerStation_1	192.168.1.10	foxs	4911	{ok}	Subordinate	{ok}	false	false

https://localhost/ord?entsecnav:/setup/schedules

Step 7. To edit the station details select the station and edit 📝 icon. Edit window opens.



The following properties configure the connection from the local station to the remote station. Provide the details of the **REMOTE station** below. (Username/Password must already exist on the remote station):

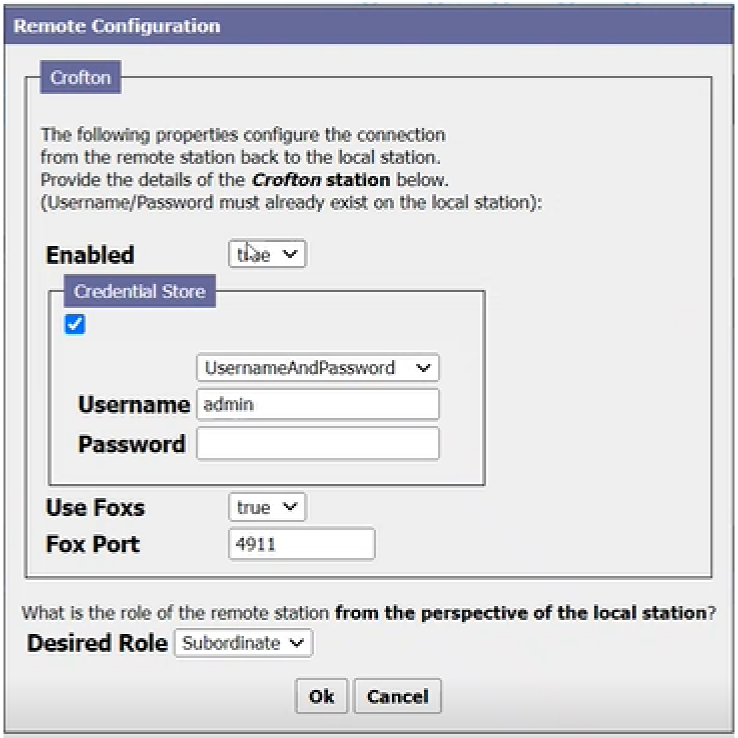
Station Name CROFTON_SEC
Enabled true
Address localhost

UsernameAndPassword
Username admin
Password ••••••••

Use Foxs true
Fox Port 4912

Step 8. Update the required details and click **Continue to Remote Configuration**.

Remote Configuration window opens. to save the changes click **OK**.



Remote Configuration

Crofton

The following properties configure the connection from the remote station back to the local station. Provide the details of the ***Crofton* station** below. (Username/Password must already exist on the local station):

Enabled true

Credential Store

☑

UsernameAndPassword

Username admin

Password

Use Foxs true

Fox Port 4911

What is the role of the remote station **from the perspective of the local station**?

Desired Role Subordinate

Step 9. In the Supervisor station, verify that Status is `{ok}` and that the role of the controller is `Subordinate`.

Five new columns (Joined, Auto Replicate, Replication Status, Last Replication, and User Status) and five new buttons (highlighted in the screen capture) appear.

Step10. To ping the controller, select its row and click Ping (▦).

Step11. Log in to the controller station, click **Controller Setup** > **Remote Devices** > **Station Manager**. The Station Manager view opens.

Step12. Verify that Status is `{ok}` and the **`Actual Role`** of the Supervisor station is `Supervisor`.

Result
You are ready to join the stations.

Station join best practices

Once you install or upgrade the software, you join each remote controller station to its Supervisor. This adds Schedules, tenants, access rights and personnel data that are stored on a single remote controller.
Before the join:

- Delete or rename any access rights that exist on a single controller if they match an access right that is currently in the Supervisor station.
- Delete any calendar schedules that exist on a single controller.
- Secure communication between the Supervisor and remote station is very important and must include both data encryption and server authentication. Since each station (Supervisor and remote controller) can serve as both a client and a server, each station requires a root CA certificate in its Trust Store and a unique, signed server certificate in its Key Store. Confirm that this is the case before you complete the join.

NOTE:

If you do not set up your certificates in advance, the join requires you to approve the self-signed certificate. This process requires the Web Launcher.

Joining a controller station to the Supervisor station

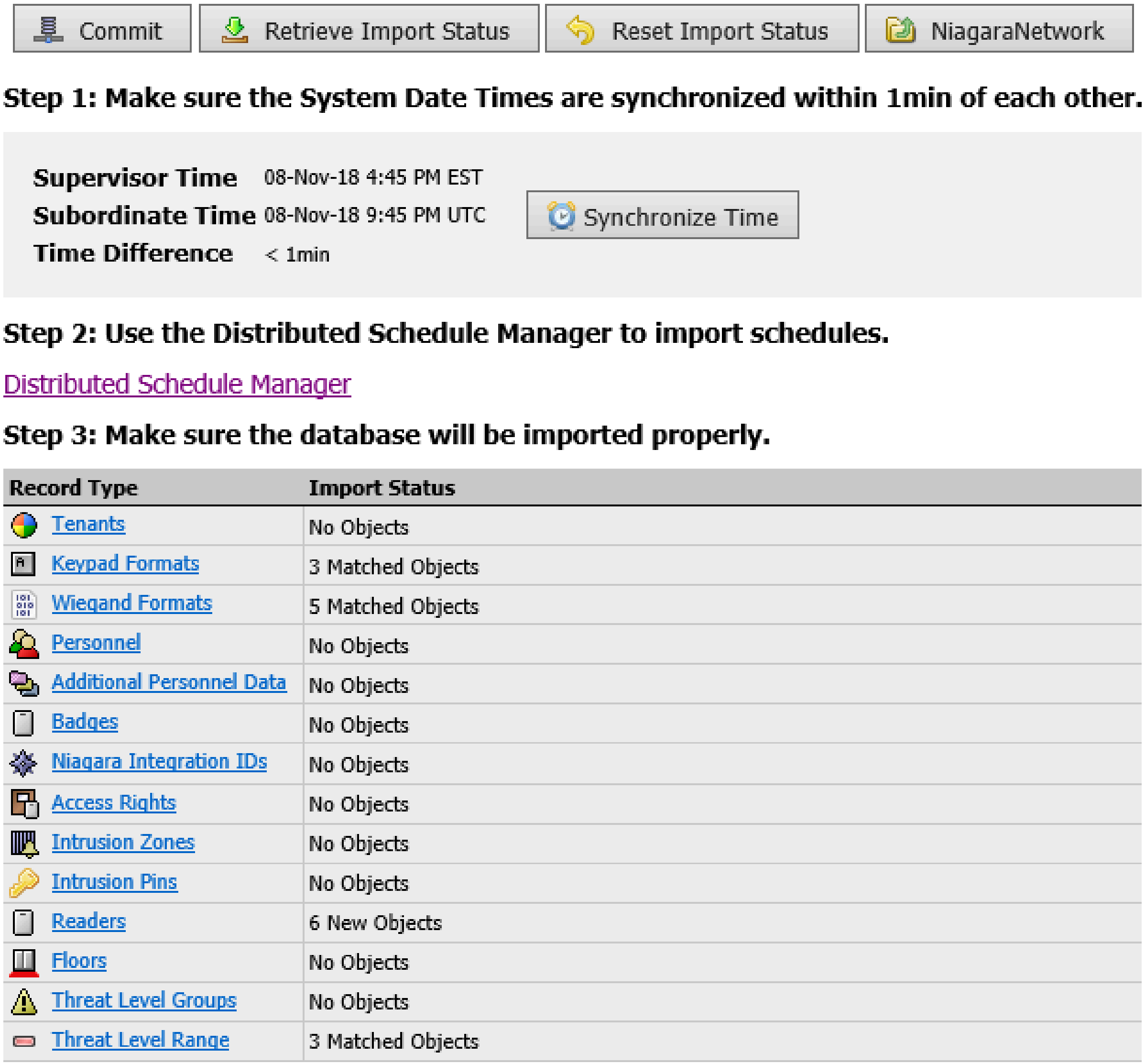
Joining the two stations updates the Supervisor’s Orion database (My SQL or MSSQL) with data from the controller’s HSQL database.

Prerequisites:
The controller and Supervisor stations are connected with the controller station configured as the subordinate station.

Step 1. From the Supervisor Home page, expand **System Setup** > **Remote Devices** and click **Station Manager**.
The Station Manager view opens. This view lists the stations that are currently part of the Supervisor station database. The table is empty if no stations are in the database.

Step 2. Select a single station and click the Join button ( ) at the top of the view.

The Join Manager view opens with the station name as the title of the view.



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

Supervisor Time	08-Nov-18 4:45 PM EST
Subordinate Time	08-Nov-18 9:45 PM UTC
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.

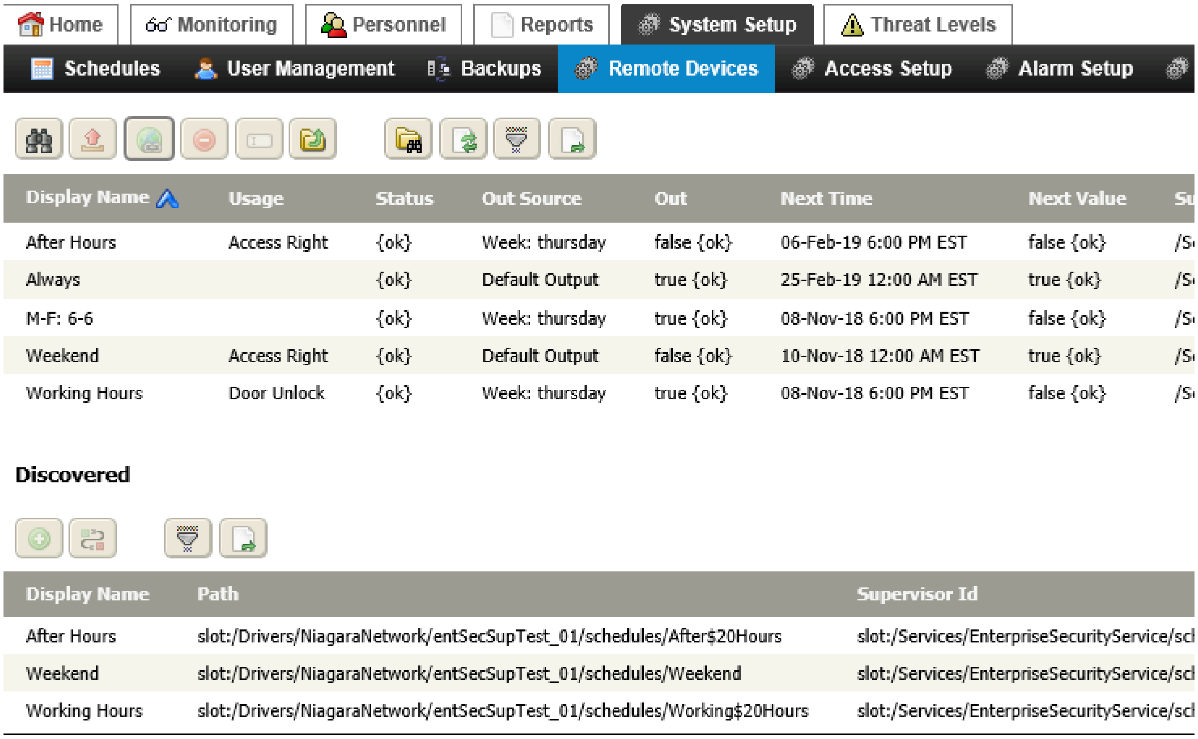
Record Type	Import Status
Tenants	No Objects
Keypad Formats	3 Matched Objects
Wiegand Formats	5 Matched Objects
Personnel	No Objects
Additional Personnel Data	No Objects
Badges	No Objects
Niagara Integration IDs	No Objects
Access Rights	No Objects
Intrusion Zones	No Objects
Intrusion Pins	No Objects
Readers	6 New Objects
Floors	No Objects
Threat Level Groups	No Objects
Threat Level Range	3 Matched Objects

Step 3. If the `Time Difference` property is greater than one minute (displays in red), click **Synchronize Time.**
A **Synchronize Time** window opens and, after confirming your choice, the time synchronization job brings the time of both systems to within one minute of each other. This ensures that records, which are added to the Supervisor station during the join process, have a common time reference.

Step 4. To return to the Join Manager view, click the Back to Join Manager button (📂).

Step 5. Click the Distributed Schedule Manager link.

The Distributed Schedule Manager view opens.



Display Name	Usage	Status	Out Source	Out	Next Time	Next Value	Su
After Hours	Access Right	{ok}	Week: thursday	false {ok}	06-Feb-19 6:00 PM EST	false {ok}	/S
Always		{ok}	Default Output	true {ok}	25-Feb-19 12:00 AM EST	true {ok}	/S
M-F: 6-6		{ok}	Week: thursday	true {ok}	08-Nov-18 6:00 PM EST	false {ok}	/S
Weekend	Access Right	{ok}	Default Output	false {ok}	10-Nov-18 12:00 AM EST	true {ok}	/S
Working Hours	Door Unlock	{ok}	Week: thursday	true {ok}	08-Nov-18 6:00 PM EST	false {ok}	/S

Discovered

Display Name	Path	Supervisor Id
After Hours	slot:/Drivers/NiagaraNetwork/entSecSupTest_01/schedules/After$20Hours	slot:/Services/EnterpriseSecurityService/scl
Weekend	slot:/Drivers/NiagaraNetwork/entSecSupTest_01/schedules/Weekend	slot:/Services/EnterpriseSecurityService/scl
Working Hours	slot:/Drivers/NiagaraNetwork/entSecSupTest_01/schedules/Working$20Hours	slot:/Services/EnterpriseSecurityService/scl

This step transfers schedules that originate in the remote host station to the Supervisor station and subordinates them to the master schedules in the Supervisor station. These schedules are not part of the Orion data.

Step 6. To find the subordinate schedules in the host controller station, click the Discover button ( ), select and Add ( ) or Match ( ) the appropriate schedules to the join job.

Step 7. Click **Retrieve Import Status.**
By default, the Import Status for all records is `Not Configured`. A direct correlation exists between this list of Record Types and the actual table structure of the Database in the Supervisor station. Clicking **Retrieve Import Status** aligns the information in the host station with the database in the Supervisor station.

Step 8. Visually verify that the import Status for each Record Type makes sense. You should have a feel for how many people, badges, access rights and readers exist in the controller.
The process asks you to confirm the return to the not-configured state.

Step 9. If needed, use the **Reset Import Status** button to undo the Import Status.

NOTE: All record types must be configured to identify matching objects (if any). The **Commit** button is not available until all the record types are configured. If there are conflicts between data on the Supervisor and the remote stations, a Recovery operation may be required instead of a join.

Step10. To see the details of any synchronized record, click a link under the Record Type column.
If there are no schedules in the remote station to import, you can skip the next steps.

Step11. When the Import Status is configured for all Record Types, click the **Commit** button.
The system reports the status of the join.

Replicating a configuration

Replication is a network management function used to speed the configuration of remote controllers. It configures each remote secondary controller from an already-configured primary controller.

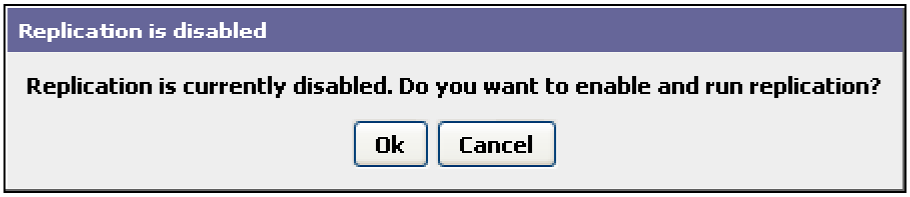
Prerequisites:
The software versions for both the Supervisor and remote station(s) are compatible. The system is open in a browser running on your Supervisor PC.

Step 1. To navigate to the Station Manager view, click **System Setup** > **Remote Devices** > **Station Manager**.
The Station Manager view opens.

Step 2. Click the Replicate button ( ).

NOTE: Join must be performed before replication can take place.

After configuring all record types, the **Commit** button is available for completing the join process. If Replication is disabled, a window prompts you to enable and run replication.



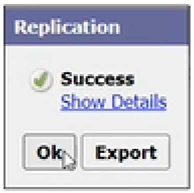
Replication is disabled

Replication is currently disabled. Do you want to enable and run replication?

Step 3. To enable replication, click the **Ok**.

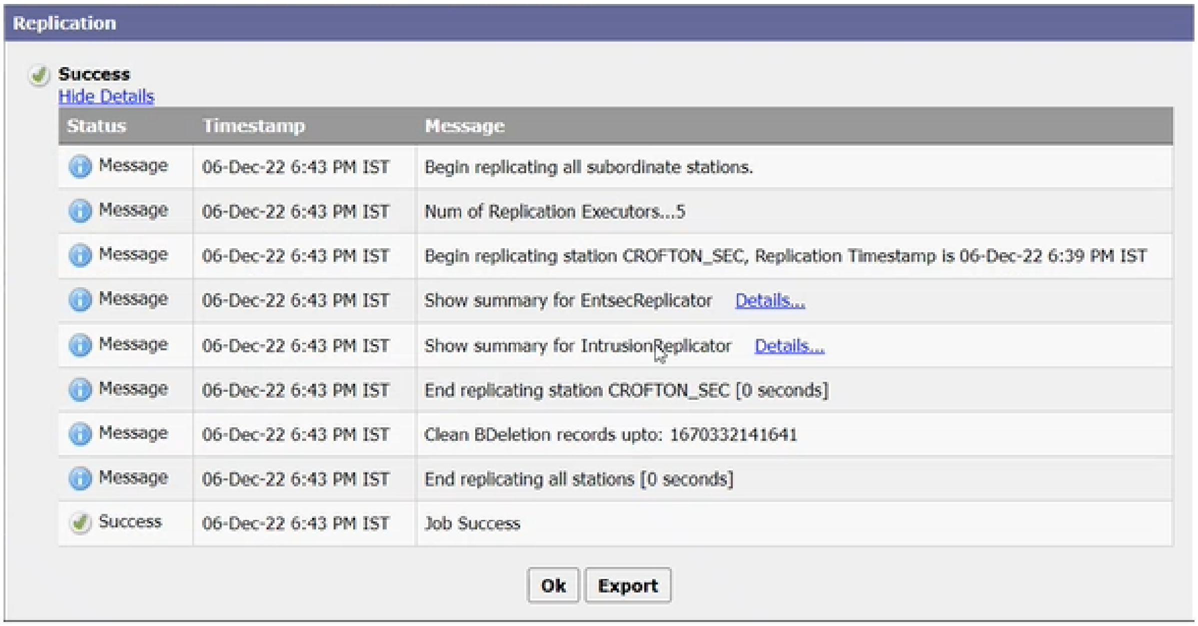
Step 4. To start the replication job, click Replicate ( ).
Once the replication job starts, a progress bar marks job progress until the replication job completes successfully or fails, as indicated by the final job status window.

Step 5. Once the job is successful Replication success window appears. To see the details click **Show Details**.



Replication

Success



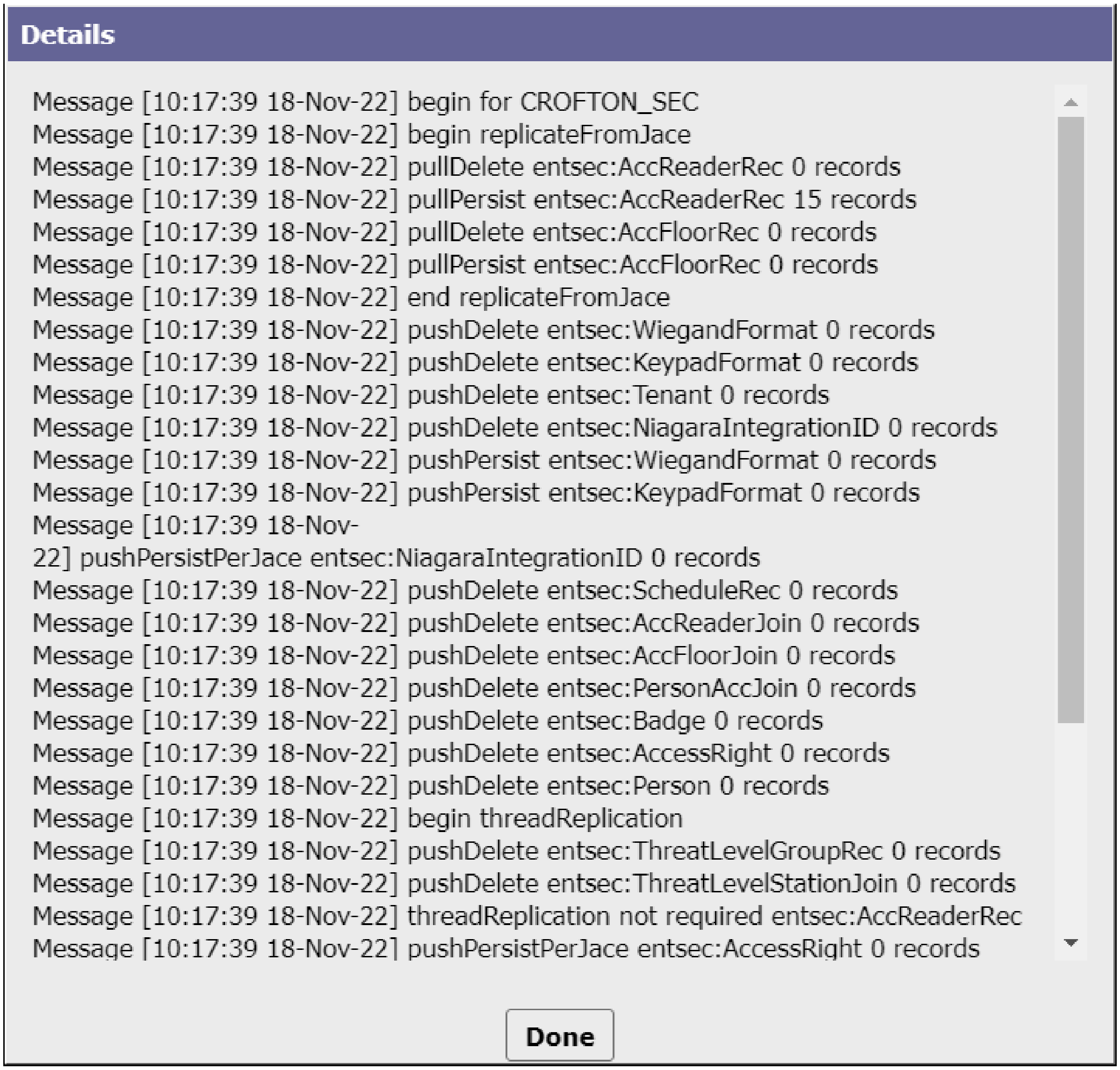
✓ Success

Hide Details

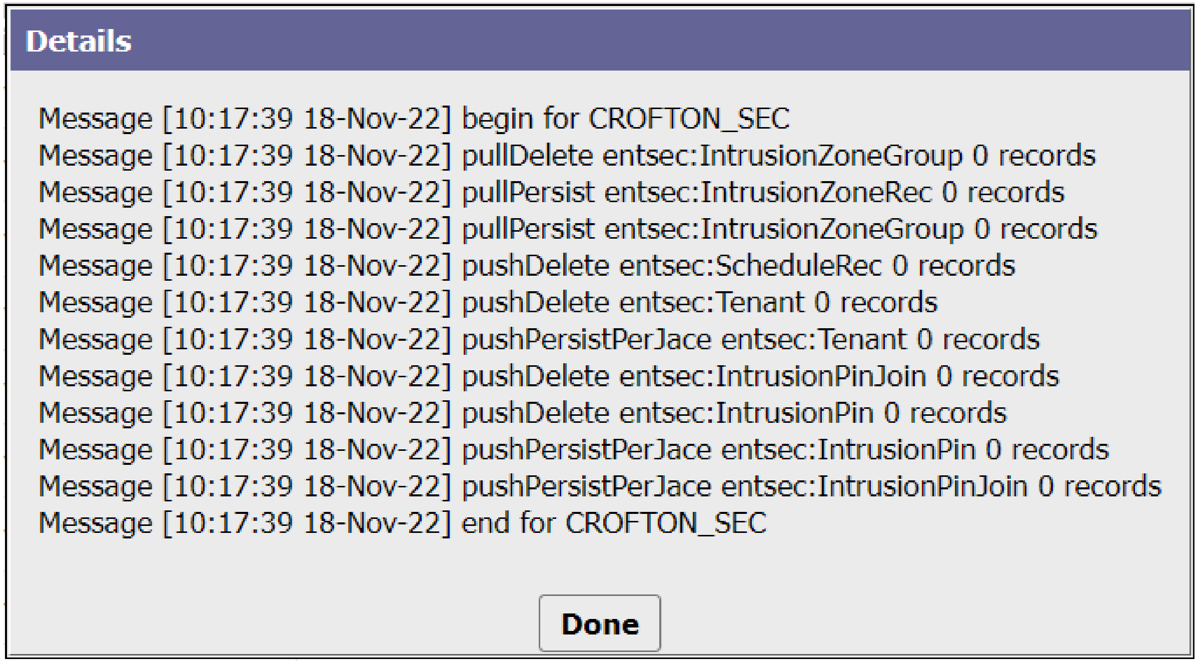
Status	Timestamp	Message
Message	06-Dec-22 6:43 PM IST	Begin replicating all subordinate stations.
Message	06-Dec-22 6:43 PM IST	Num of Replication Executors...5
Message	06-Dec-22 6:43 PM IST	Begin replicating station CROFTON_SEC, Replication Timestamp is 06-Dec-22 6:39 PM IST
Message	06-Dec-22 6:43 PM IST	Show summary for EntsecReplicator Details...
Message	06-Dec-22 6:43 PM IST	Show summary for IntrusionReplicator Details...
Message	06-Dec-22 6:43 PM IST	End replicating station CROFTON_SEC [0 seconds]
Message	06-Dec-22 6:43 PM IST	Clean BDeletion records upto: 1670332141641
Message	06-Dec-22 6:43 PM IST	End replicating all stations [0 seconds]
Success	06-Dec-22 6:43 PM IST	Job Success

Replication details window opens.

For more details of Replication click on **Details**. This gives additional information about the records. Following is the window that displays details for **EntsecReplicator** and **IntrusionReplicator** respectively.



```
Message [10:17:39 18-Nov-22] begin for CROFTON_SEC
Message [10:17:39 18-Nov-22] begin replicateFromJace
Message [10:17:39 18-Nov-22] pullDelete entsec:AccReaderRec 0 records
Message [10:17:39 18-Nov-22] pullPersist entsec:AccReaderRec 15 records
Message [10:17:39 18-Nov-22] pullDelete entsec:AccFloorRec 0 records
Message [10:17:39 18-Nov-22] pullPersist entsec:AccFloorRec 0 records
Message [10:17:39 18-Nov-22] end replicateFromJace
Message [10:17:39 18-Nov-22] pushDelete entsec:WiegandFormat 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:KeypadFormat 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:Tenant 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:NiagaraIntegrationID 0 records
Message [10:17:39 18-Nov-22] pushPersist entsec:WiegandFormat 0 records
Message [10:17:39 18-Nov-22] pushPersist entsec:KeypadFormat 0 records
Message [10:17:39 18-Nov-
22] pushPersistPerJace entsec:NiagaraIntegrationID 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:ScheduleRec 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:AccReaderJoin 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:AccFloorJoin 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:PersonAccJoin 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:Badge 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:AccessRight 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:Person 0 records
Message [10:17:39 18-Nov-22] begin threadReplication
Message [10:17:39 18-Nov-22] pushDelete entsec:ThreatLevelGroupRec 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:ThreatLevelStationJoin 0 records
Message [10:17:39 18-Nov-22] threadReplication not required entsec:AccReaderRec
Message [10:17:39 18-Nov-22] pushPersistPerJace entsec:AccessRight 0 records
```



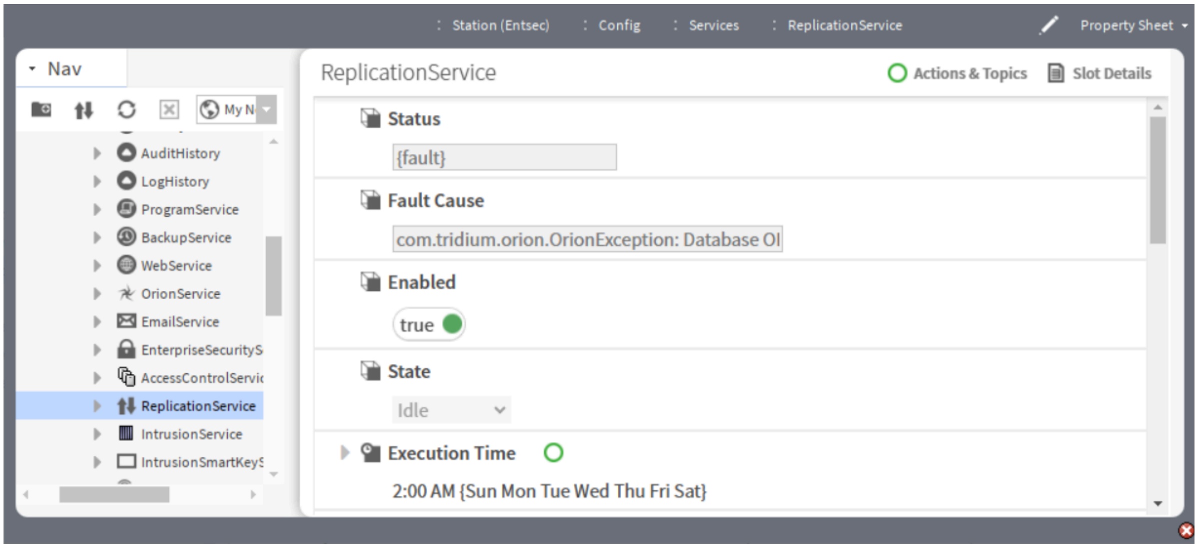
Details

```
Message [10:17:39 18-Nov-22] begin for CROFTON_SEC
Message [10:17:39 18-Nov-22] pullDelete entsec:IntrusionZoneGroup 0 records
Message [10:17:39 18-Nov-22] pullPersist entsec:IntrusionZoneRec 0 records
Message [10:17:39 18-Nov-22] pullPersist entsec:IntrusionZoneGroup 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:ScheduleRec 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:Tenant 0 records
Message [10:17:39 18-Nov-22] pushPersistPerJace entsec:Tenant 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:IntrusionPinJoin 0 records
Message [10:17:39 18-Nov-22] pushDelete entsec:IntrusionPin 0 records
Message [10:17:39 18-Nov-22] pushPersistPerJace entsec:IntrusionPin 0 records
Message [10:17:39 18-Nov-22] pushPersistPerJace entsec:IntrusionPinJoin 0 records
Message [10:17:39 18-Nov-22] end for CROFTON_SEC
```

Replicating a configuration to NAC server

The replication service replicates data to the **NAC server** according to the configurations applied to the **NAC controllers.**

Step 1. Navigate to Workbench, expand **Station** > **Config** > **Services** > **Replication Service.**



ReplicationService

Status: {fault}

Fault Cause: com.tridium.orion.OrionException: Database Ol

Enabled: true

State: Idle

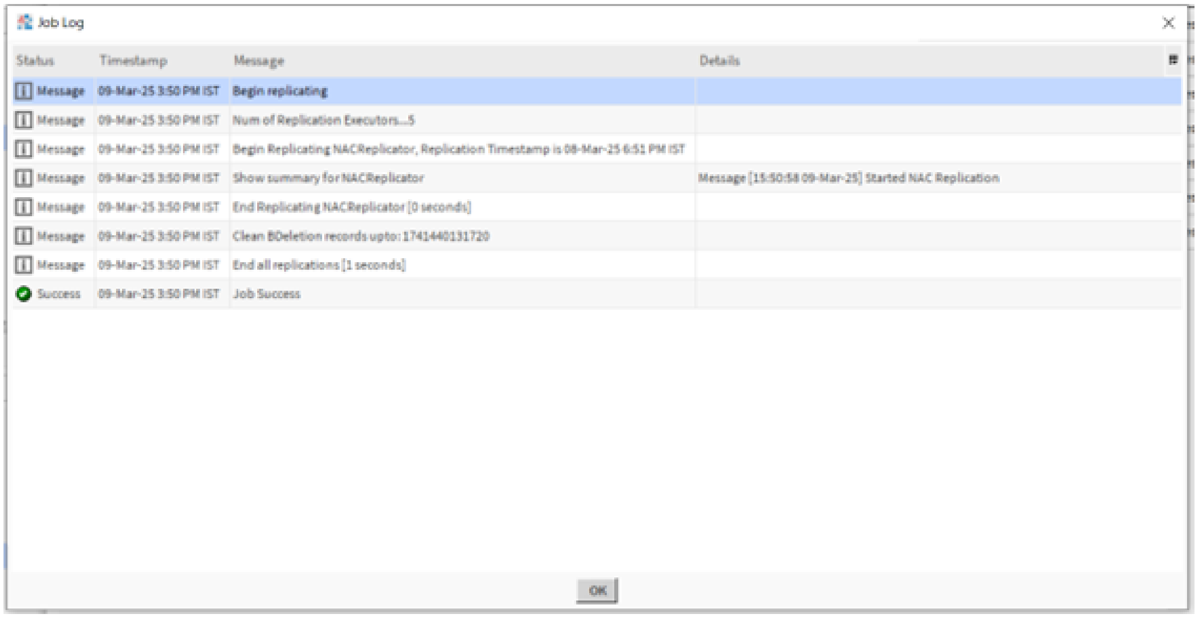
Execution Time: 2:00 AM {Sun Mon Tue Wed Thu Fri Sat}

The Replication Property Sheet Opens.

Step 2. Right-click on the **Replication Service**, select **Actions** > **Execute as Job.**

Replication job starts. When the replication job begins, a progress bar tracks its progress until it is either completed or fails, as shown in the final job status window.

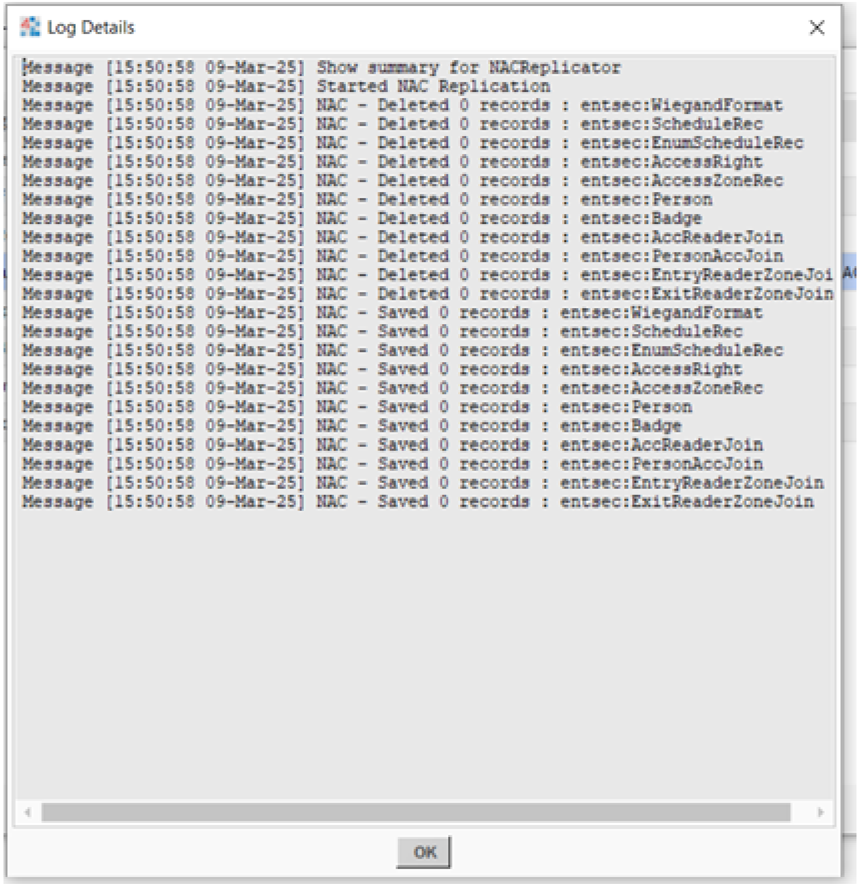
Step 3. To verify the replication status, navigate to **Config** > **Services** > **Job Service.** When the Job window appears, click on the **Replication** Job.



Status	Timestamp	Message	Details
Message	09-Mar-25 3:50 PM IST	Begin replicating	
Message	09-Mar-25 3:50 PM IST	Num of Replication Executors...5	
Message	09-Mar-25 3:50 PM IST	Begin Replicating NACReplicator, Replication Timestamp is 08-Mar-25 6:51 PM IST	
Message	09-Mar-25 3:50 PM IST	Show summary for NACReplicator	Message [15:50:58 09-Mar-25] Started NAC Replication
Message	09-Mar-25 3:50 PM IST	End Replicating NACReplicator [0 seconds]	
Message	09-Mar-25 3:50 PM IST	Clean BDeletion records upto: 1741440131720	
Message	09-Mar-25 3:50 PM IST	End all replications [1 seconds]	
Success	09-Mar-25 3:50 PM IST	Job Success	

Job Log Window Opens.

Step 4. Click on the success message to get the job details.



```
Message [15:50:58 09-Mar-25] Show summary for NACReplicator
Message [15:50:58 09-Mar-25] Started NAC Replication
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:WiegandFormat
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:ScheduleRec
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:EnumScheduleRec
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:AccessRight
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:AccessZoneRec
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:Person
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:Badge
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:AccReaderJoin
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:PersonAccJoin
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:EntryReaderZoneJoi
Message [15:50:58 09-Mar-25] NAC - Deleted 0 records : entsec:ExitReaderZoneJoin
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:WiegandFormat
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:ScheduleRec
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:EnumScheduleRec
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:AccessRight
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:AccessZoneRec
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:Person
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:Badge
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:AccReaderJoin
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:PersonAccJoin
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:EntryReaderZoneJoin
Message [15:50:58 09-Mar-25] NAC - Saved 0 records : entsec:ExitReaderZoneJoin
```

NOTE: Only the access control data related to the **NAC controller** is replicated to the **NAC server**.

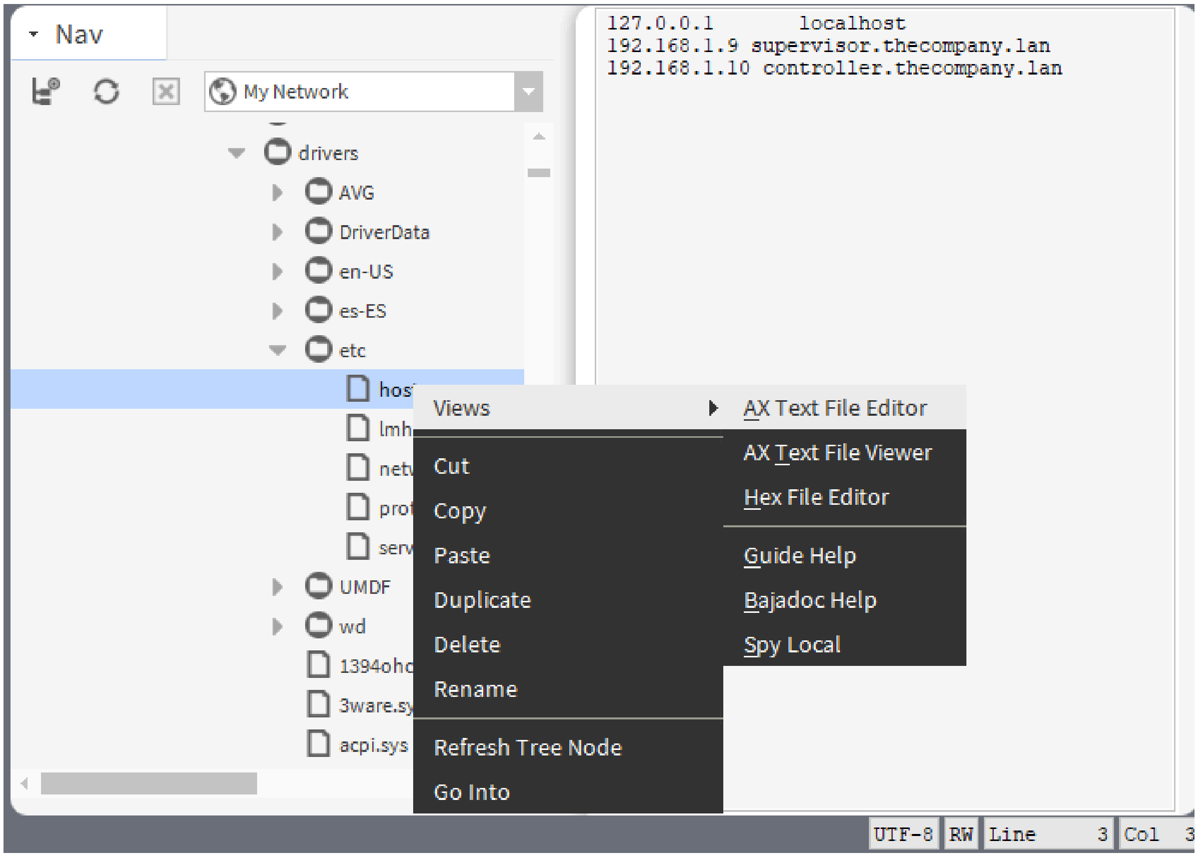
Setting up domain names

In the absence of a DNS (Domain Name System) server, the system can correlate station IP addresses with domain names. Domain name connections may be easier to remember than IP addresses.

Prerequisites:
You are connected to a computer and running Workbench.

Step 1. Open Workbench using **Run as administrator** (right-click the icon on the desktop and click **Run as administrator**, or right-click the application in the start menu and click **More** > **Run as administrator**.

Step 2. In the Nav tree, expand **My File System** > **C:** > **Windows** > **System32** > **drivers** > **etc**, right-click `hosts` and click **AX Text File Editor**.
The hosts file opens in the AX Text File Editor view editor.



```
127.0.0.1        localhost
192.168.1.9 supervisor.thecompany.lan
192.168.1.10 controller.thecompany.lan
```

Step 3. Scroll to the end of the document, place your cursor at the end of the last line and press Enter to create a new line.

Step 4. Type a line for each Supervisor and controller:
`<999.999.99.99  >` where:

- `<999.999.99.99>` is the IP address on the network of the PC or controller.
- `<domainName>` is the domain name the system can use to connect to the controller.

There must be at least one space between the IP address and the domain name on each line.

Step 5. Click the Save button (💾).

Step 6. To verify that the hosts file contains the domain names, open a platform connection to your localhost and double-click **TCP/IP Configuration**.

Step 7. To open the **`Hosts File`**, click the double down arrows (⇊).

Step 8. If needed, scroll to the bottom of the file and confirm that the IP addresses are associated with the correct display names.

Chapter 10. Personnel setup

Before regular office procedures for processing new people can be set up, the personnel manager or other administrative person must set up access rights, badges, and a number of optional configurations, including Niagara Integration IDs, tenants, threat level groups, and, possibly, additional personnel data to be maintained by the system.

The term "person" refers to a human being, usually an employee, who possesses one or more rights to enter and use a facility. A "user" refers to a person who is authorized to manage the system. For example, an employee who works in manufacturing is a person with a badge for entering and exiting the building. In addition to being a person with a badge, a Human Resources associate is a user of the system who enters new employees and issues badges.

While you may add personnel to the database without assigning access rights or badges, to successfully add personnel, access rights, schedules, and access zones should already exist before you add people.

If your topology includes a Supervisor computer and one or more remote controllers, set up all personnel and assign badges only at the Supervisor station that serves the company–wide system.

CAUTION: Enter all personnel information using the Supervisor station ONLY and not using any remote controller station. If you enter personnel information at the remote controller, duplicate personnel records may occur in the system. The system disables some control buttons when you work connected to a subordinate station.

This does not apply to a single controller functioning without a Supervisor computer. If yours is a small company with a single controller, connect a computer to the network and launch the software from your computer.

Personnel data from the LDAP server

The following topics describe how to install and configure an Lightweight Directory Access Protocol (LDAP) network in a Enterprise Security system. Topics describe how to connect to an LDAP server to import personnel information from the server to your personnel database.

The more you know about the LDAP attributes that you are working with, the easier it is to map them to system properties and import personnel records from the Ldap server to the station database.

Adding an LDAP network

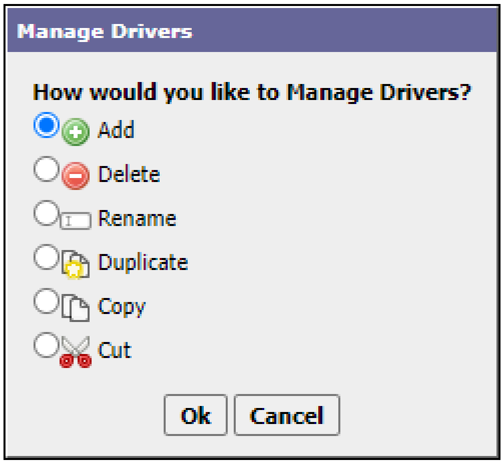
This procedure describes how to add an **Ldap Network**.

Prerequisites:
You are logged in toEnterprise Security Web UI.

Step 1. From the main menu, select **System Setup** > **Remote Devices**, and click **Remote Drivers**.

Step 2. Click the Manage Drivers button (⚙).

The **Manage Drivers** window opens.

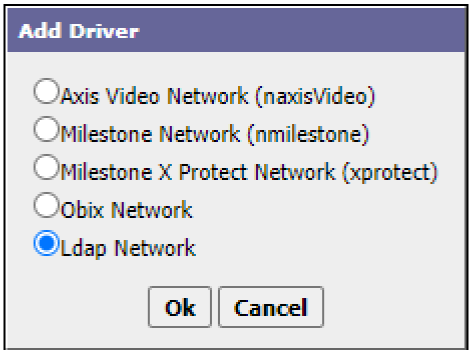


Manage Drivers

How would you like to Manage Drivers?

- ● Add
- ○ Delete
- ○ Rename
- ○ Duplicate
- ○ Copy
- ○ Cut

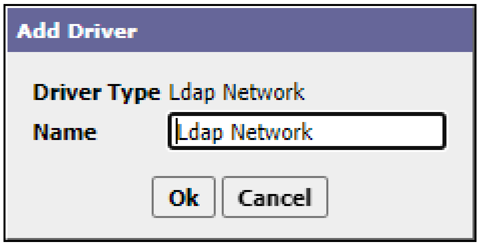
Step 3. To add a new network select **Add** and click **OK**.
The **Add Driver** window opens.



Add Driver

- ○ Axis Video Network (naxisVideo)
- ○ Milestone Network (nmilestone)
- ○ Milestone X Protect Network (xprotect)
- ○ Obix Network
- ● Ldap Network

Step 4. Select **Ldap Network** and click **OK**.
Another **Add Driver** window opens.



Add Driver

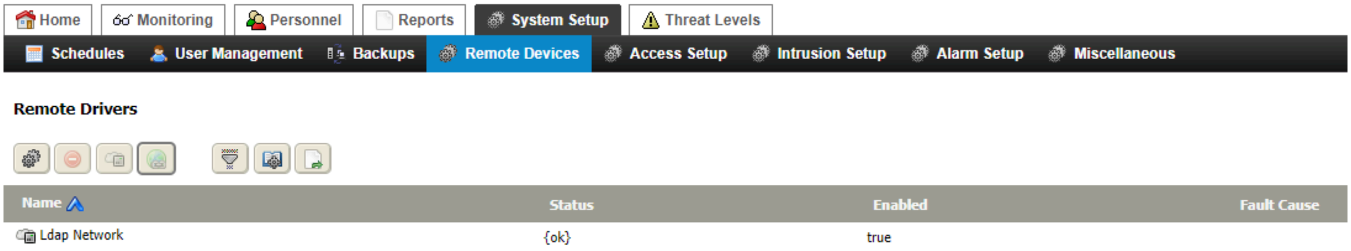
Driver Type Ldap Network

Name Ldap Network

Step 5. Name the network or accept the default name and click **OK**.

Result

This adds **Ldap Network** to the **Remote Devices**.



Remote Drivers

Name	Status	Enabled	Fault Cause
Ldap Network	{ok}	true	

Adding an Ldap server

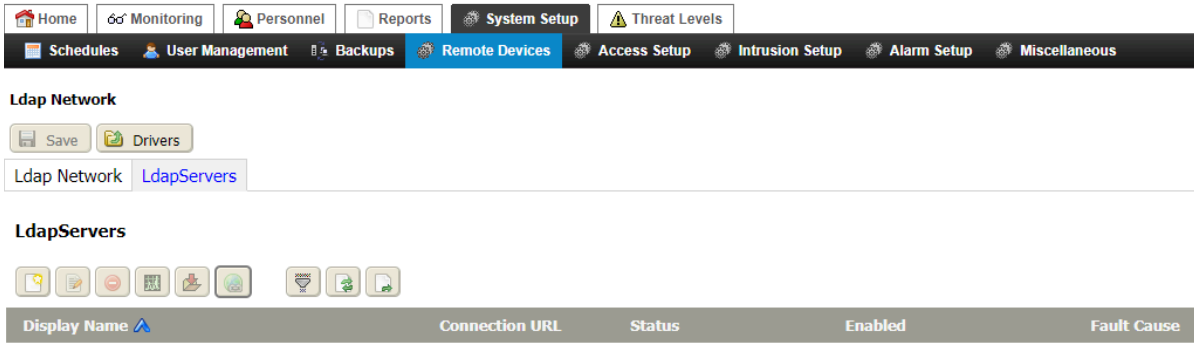
This procedure explains how to add an **Ldap Server** to an existing **Ldap Network**.

Prerequisites:

You added the **Ldap Network**.

Step 1. From the main menu, select **System Setup** > **Remote Devices**, click **Remote Drivers** and double-click on **Ldap Network**.

Step 2. Select the **LdapServers** tab.

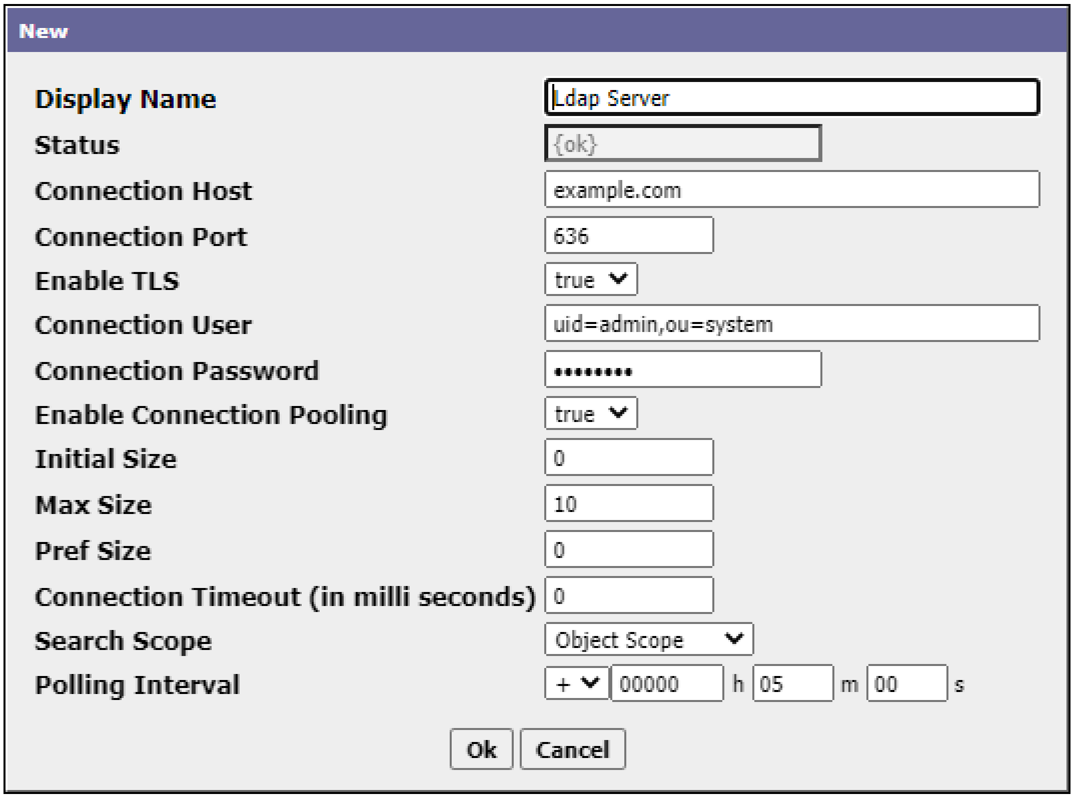


Ldap Network

LdapServers

Display Name	Connection URL	Status	Enabled	Fault Cause

Step 3. To add a new **Ldap Server** click the new button ( ).



New

Display Name	Ldap Server
Status	{ok}
Connection Host	example.com
Connection Port	636
Enable TLS	true
Connection User	uid=admin,ou=system
Connection Password	••••••••
Enable Connection Pooling	true
Initial Size	0
Max Size	10
Pref Size	0
Connection Timeout (in milli seconds)	0
Search Scope	Object Scope
Polling Interval	+ 00000 h 05 m 00 s

A **New** window opens.The *Niagara Enterprise Security Reference* documents these properties.

Step 4. To add the server click **OK**.
The Ldap server is added.

Step 5. To establish the connection, click the **Ping** button ( ) .
It takes a few seconds for the server row to update in the table.

Step 6. Check that the status of the server indicates that the connection is `{OK}`.

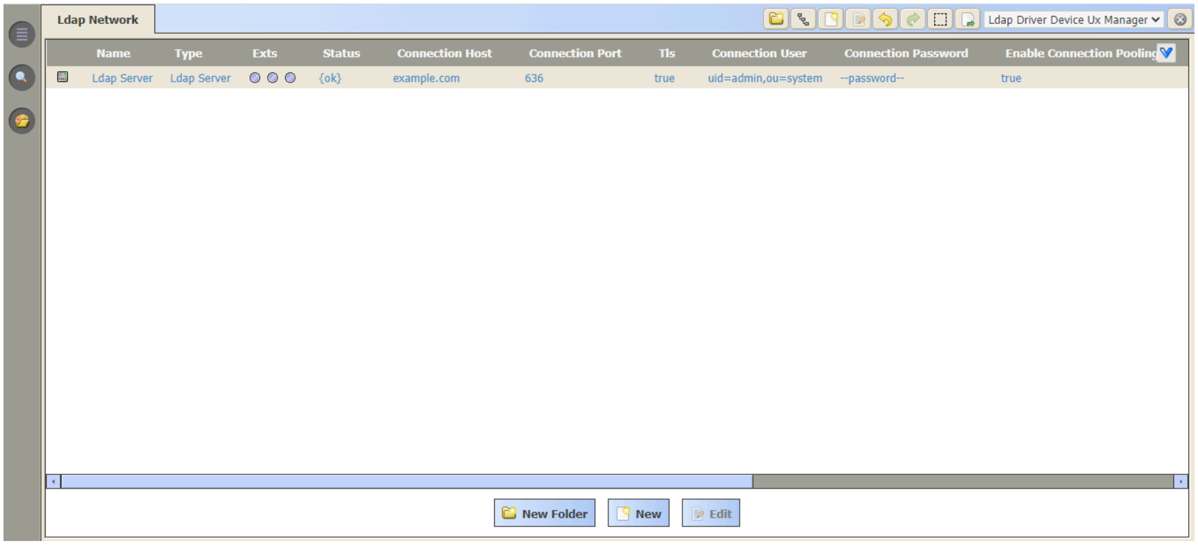
Configuring LDAP import attributes

Specifying the import attributes before importing the groups is a onetime configuration procedure.

Prerequisites:
The LDAP server has been identified and you are open at the **LdapServers** tab.

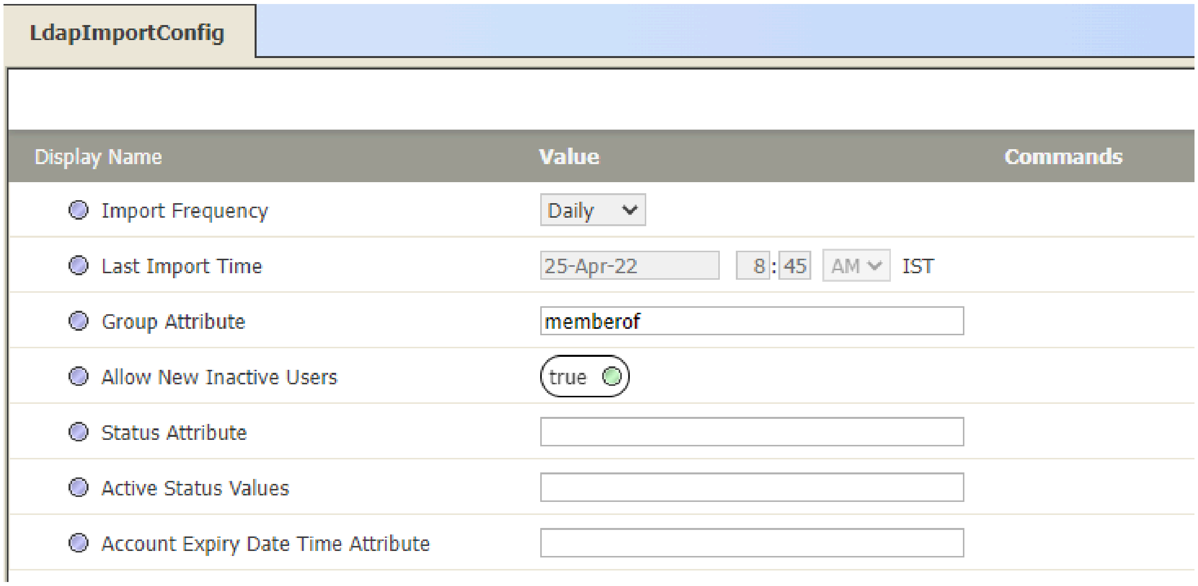
Step 1. From the main menu, select **System Setup** > **Remote Devices**, click **Remote Drivers** and double-click on **Ldap Network**.

The **Ldap Driver Device UX Manager** window opens.



Name	Type	Exts	Status	Connection Host	Connection Port	Tls	Connection User	Connection Password	Enable Connection Pooling
Ldap Server	Ldap Server	○ ○ ○	{ok}	example.com	636	true	uid=admin,ou=system	--password--	true

Step 2. Navigate to **ldap Server** > **Views** > **Property Sheet**, click **Ldap Import Config**.
The Property Sheet opens.



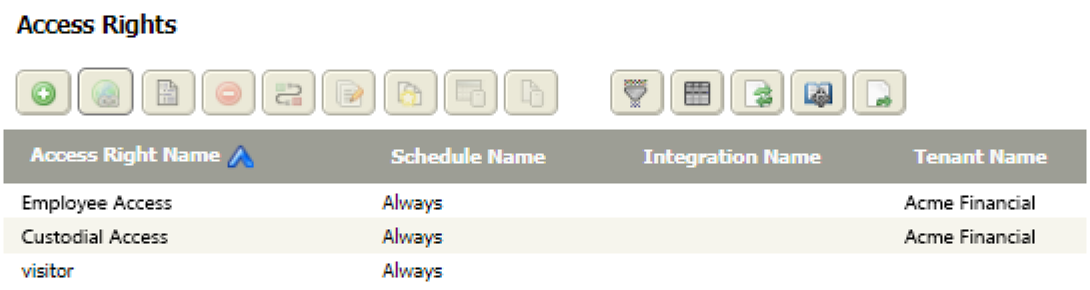
Display Name	Value	Commands
Import Frequency	Daily	
Last Import Time	25-Apr-22 8:45 AM IST	
Group Attribute	memberof	
Allow New Inactive Users	true	
Status Attribute		
Active Status Values		
Account Expiry Date Time Attribute		

Step 3. Configure the LDAP parameters and click **Save**. Refer to *Niagara Enterprise Security Reference* for further details.

Creating access rights for LDAP importing

This task describes how to create access rights in the system. You can use access rights to import Ldap personnel records from an Ldap server.

Step 1. From the main menu, select **System Setup** > **Personnel** and click **Access Rights**.

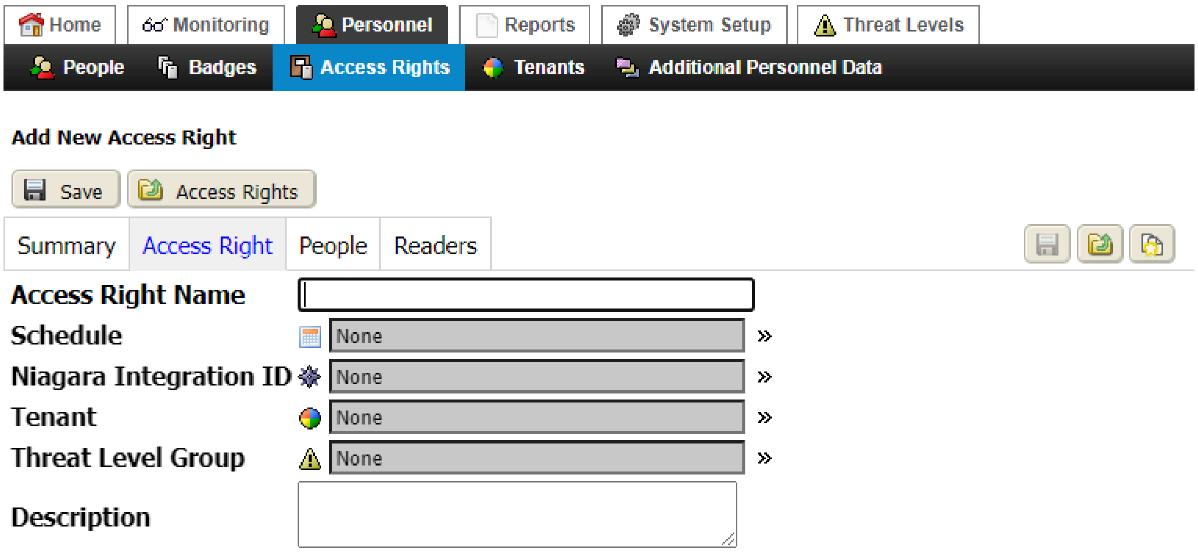


Access Rights

Access Right Name	Schedule Name	Integration Name	Tenant Name
Employee Access	Always		Acme Financial
Custodial Access	Always		Acme Financial
visitor	Always		

The **Access Rights** window opens.

Step 2. To add a new access right click, the **Add** button (⊕).



Add New Access Right

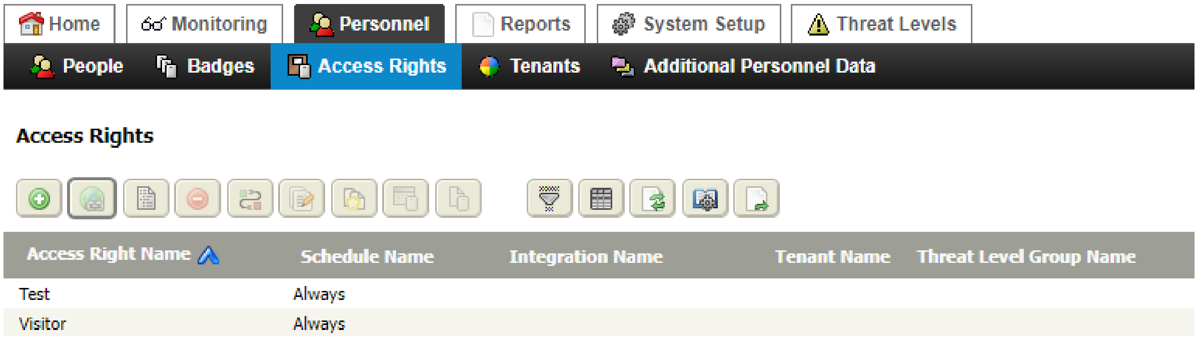
Access Right Name	
Schedule	None »
Niagara Integration ID	None »
Tenant	None »
Threat Level Group	None »
Description	

The **Add New Access Right** view opens.Refer to

Step 3. Enter the following details:

- **Access Right Name**: Access Right Name associates this right with the role of the system user, for example, "LDAP."
- **Schedule**: Schedule controls when this right is in operation. It opens a **Ref Chooser** window.
  a. **Niagara Integration ID**: Niagara Integration ID associates this access right with a specific tenant who is identified by this ID.
  b. **Tenant**: Tenant identifies the tenant to which this access right applies.
  c. **Threat Level Group**: To select the threat level group click (»). The **Ref Chooser** window opens. Select the tenant and click **Ok** or click **Add** button (⊕).
  d. **Description**: Enter a brief description for the access right.

Step 4. To add the access right click **Save**.



Access Rights

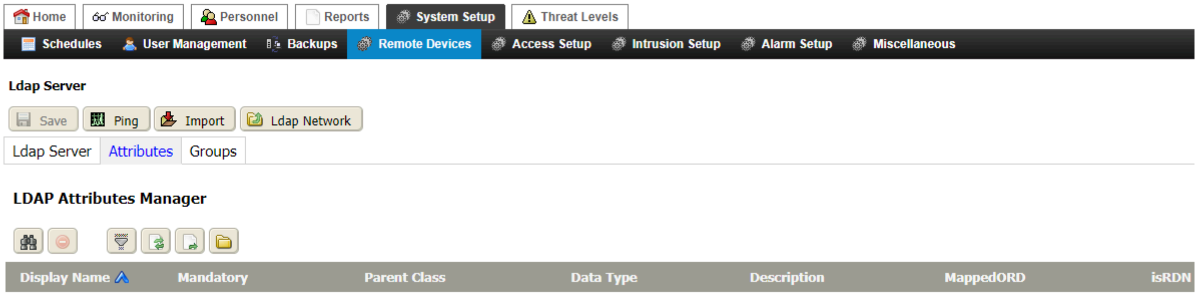
Access Right Name	Schedule Name	Integration Name	Tenant Name	Threat Level Group Name
Test	Always			
Visitor	Always			

Discovering and assigning attributes for ldap importing

Discovering and assigning attributes is an important part of successfully importing personal records.

Step 1. From the main menu, select **Remote Devices** > **Remote Drivers**, double-click **Ldap Network**, click the **Ldap Server** tab and double-click the **Ldap Server** row in the table.
The **Ldap Server** view opens.

Step 2. Click on **Attributes** tab.



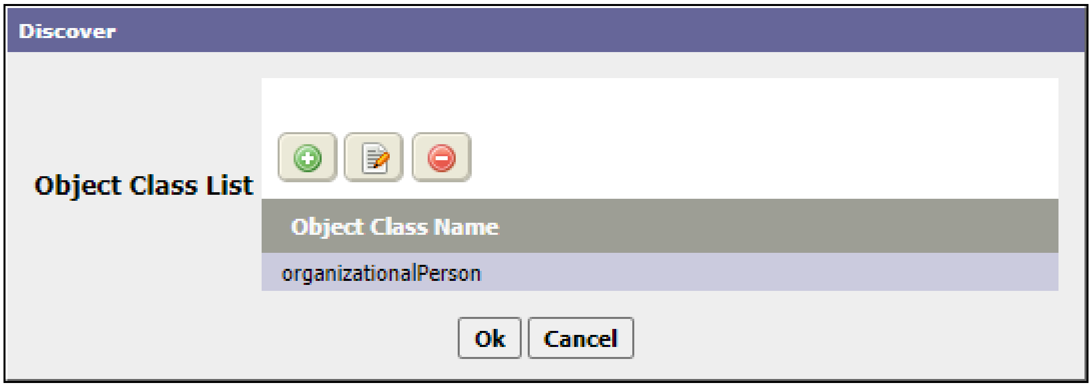
Ldap Server

LDAP Attributes Manager

Display Name	Mandatory	Parent Class	Data Type	Description	MappedORD	isRDN

LDAP Attribute Manager view opens.

Step 3. To discover attributes from the **LDAP Server**, click the **Discover** button (🔍).



Discover

Object Class List

Object Class Name
organizationalPerson

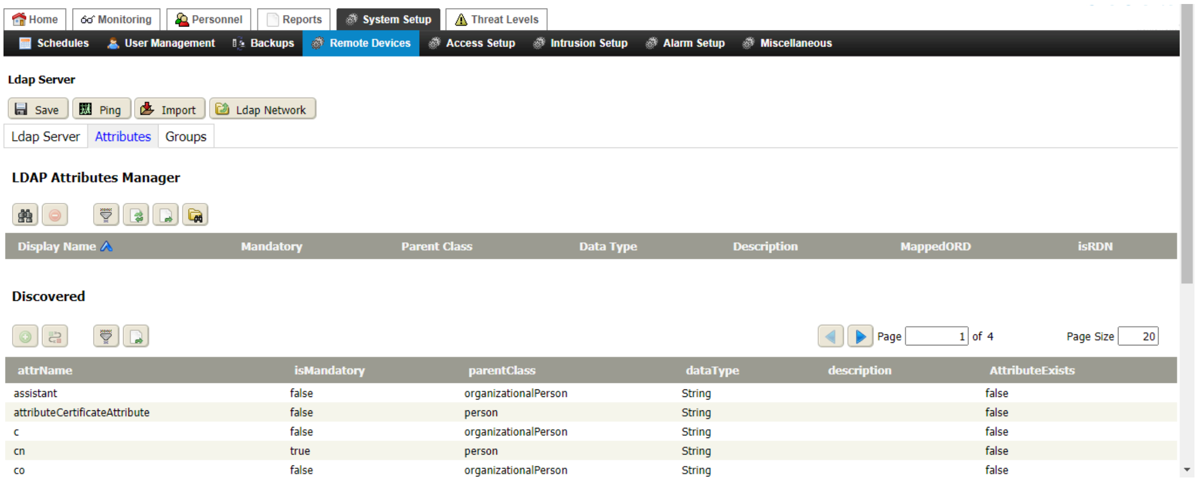
The **Discover** window opens.

The Object Class identifies the group of personnel records to import from the LDAP server.

Step 4. To manage the Object Class List, click add (button), edit (button) or delete (button).

Step 5. To discover, select the object class attribute (for example, "organizationalPerson" or "User") and click **Ok**.

Step 6. The discovered attributes are displayed in **Discovered** pane.



Ldap Server

LDAP Attributes Manager

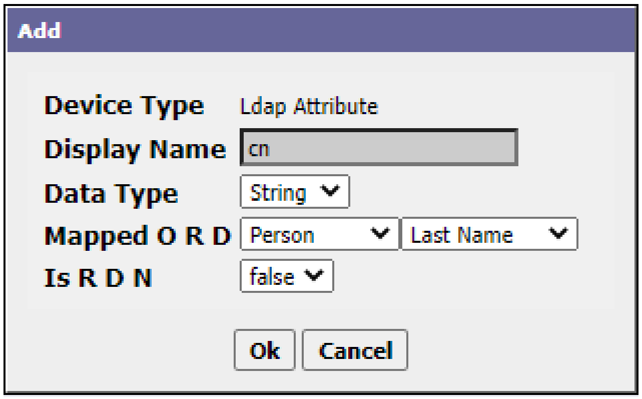
Display Name	Mandatory	Parent Class	Data Type	Description	MappedORD	isRDN

Discovered

Page 1 of 4 Page Size 20

attrName	isMandatory	parentClass	dataType	description	AttributeExists
assistant	false	organizationalPerson	String		false
attributeCertificateAttribute	false	person	String		false
c	false	organizationalPerson	String		false
cn	true	person	String		false
co	false	organizationalPerson	String		false

Step 7. Select a discovered attribute and click Add (button) (⊕).



Device Type Ldap Attribute

Display Name cn

Data Type String

Mapped O R D Person Last Name

Is R D N false

The **Add** window opens.

Step 8. To add the attribute to database pane, fill the following details and click **OK**:

a. **Display Name** cannot be changed. This remains as it is in LDAP server.

b. **Data Type** provides two options `String` or `Binary`.

c. **Mapped O R D** selects `Person` or `PersonInfo` or `Badge`. **Last Name** is the mandatory attribute.

d. **Is R D N** selects `true` or `false` from the drop-down list.

Result

This adds the discovered attributes to the database.

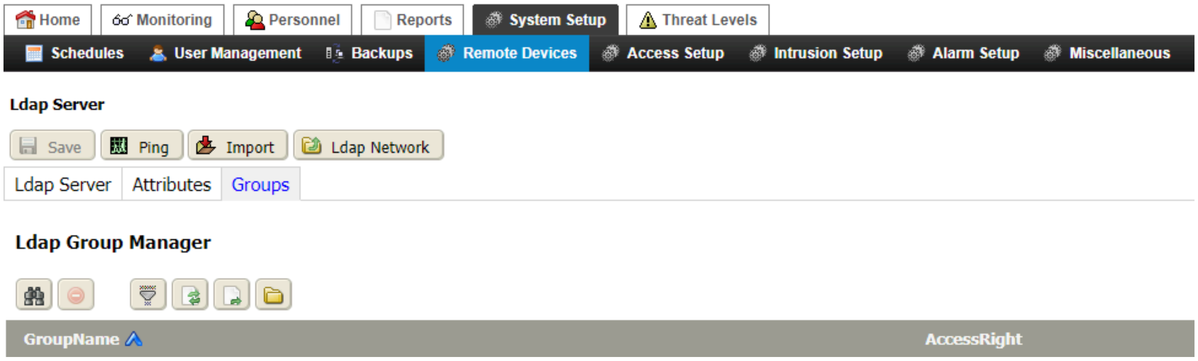
Discovering, selecting and configuring groups for Ldap importing

Discovering, selecting and configuring groups filters the records coming in from the LDAP server. The group of users are given specific access rights.

Step 1. From the main menu, select **Remote Devices** > **Remote Drivers**, double-click **Ldap Network**, click

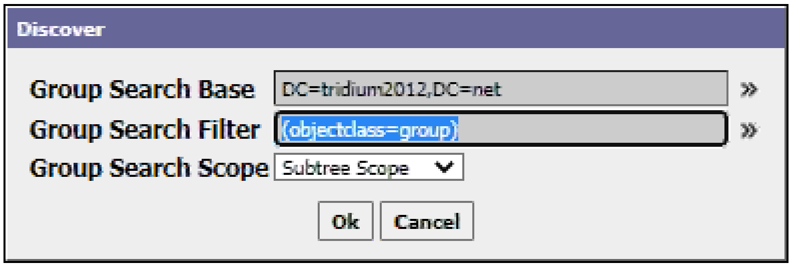
the **Ldap Server** tab and double-click the **Ldap Server** row in the table.
The **LdapServer** view opens.

Step 2. Click on the **Groups** tab.



LDAP Group Manager view opens.

Step 3. To discover the groups from **LDAP Server**, click Discover icon (⌕).



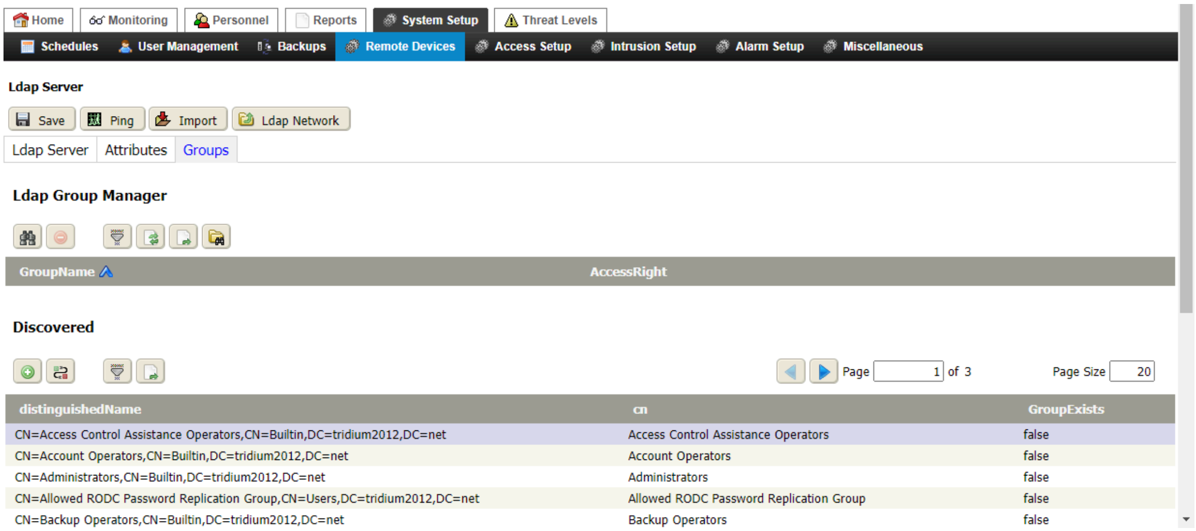
Group Search Base: DC=tridium2012,DC=net

Group Search Filter: (objectclass=group)

Group Search Scope: Subtree Scope

The **Discover** window opens.The discovered groups are displayed in **Discovered** pane.

Step 4. Identify the groups associated with access rights.



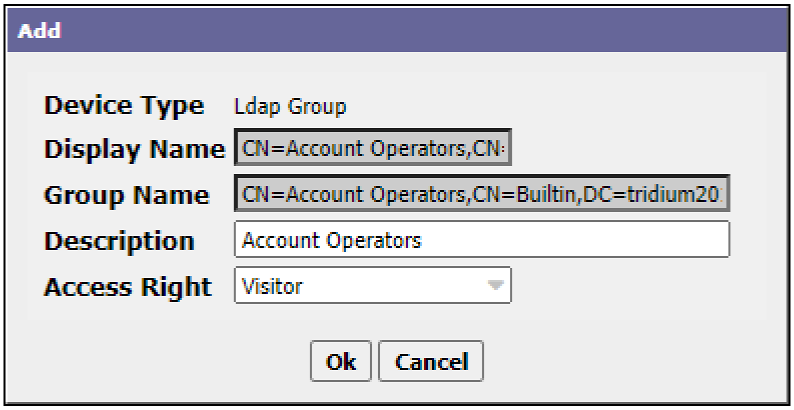
distinguishedName	cn	GroupExists
CN=Access Control Assistance Operators,CN=Builtin,DC=tridium2012,DC=net	Access Control Assistance Operators	false
CN=Account Operators,CN=Builtin,DC=tridium2012,DC=net	Account Operators	false
CN=Administrators,CN=Builtin,DC=tridium2012,DC=net	Administrators	false
CN=Allowed RODC Password Replication Group,CN=Users,DC=tridium2012,DC=net	Allowed RODC Password Replication Group	false
CN=Backup Operators,CN=Builtin,DC=tridium2012,DC=net	Backup Operators	false

This helps the system identify which access rights should be given to each employee.

Step 5. Select the discovered groups and click the **Add** button (⊕).

The **Add** window opens.

Step 6. You can change the **Description** if needed. you can select the **Access Right** from the drop-down list. To add the user to database, click **OK**.



Device Type	Ldap Group
Display Name	CN=Account Operators,CN:
Group Name	CN=Account Operators,CN=Builtin,DC=tridium20
Description	Account Operators
Access Right	Visitor

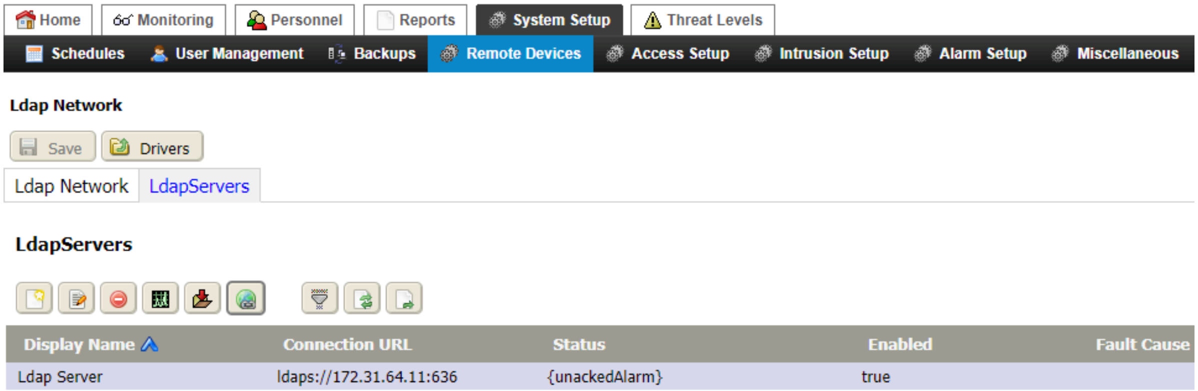
Importing users from ldap server

Importing multiple personal records from the LDAP server saves time.

Prerequisites:
The LDAP server is on line.

Step 1. Expand **Remote Devices** > **Remote Drivers**, double-click **Ldap Network**

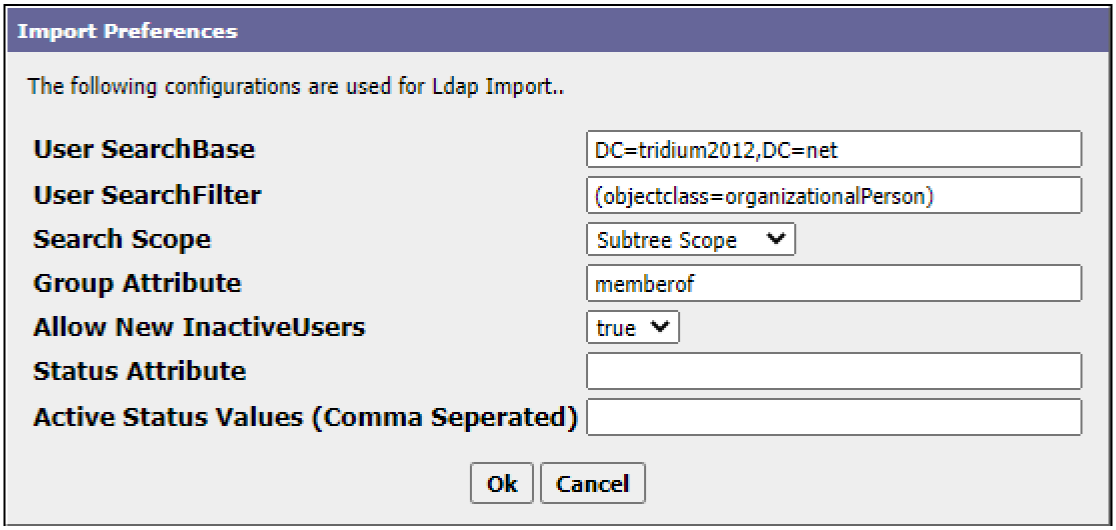
Step 2. Click the **Ldap Server** tab and double-click on **LdapServer**.



Display Name	Connection URL	Status	Enabled	Fault Cause
Ldap Server	ldaps://172.31.64.11:636	{unackedAlarm}	true	

Step 3. To import records from **Ldap Server** click the **Import** button (⬇).
The **Import Preferences** window opens.

Step 4. Configure the properties to import users. and Click **OK**.



Import Preferences

The following configurations are used for Ldap Import..

User SearchBase	DC=tridium2012,DC=net
User SearchFilter	(objectclass=organizationalPerson)
Search Scope	Subtree Scope
Group Attribute	memberof
Allow New InactiveUsers	true
Status Attribute	
Active Status Values (Comma Seperated)	

- **User SearchBase** configure the parent class to import the records associated with the parent class.
- **User SearchFilter** configure the object class for the record import.

Result
LDAP server imports the records.

Badges

Assigned badges help keep a person uniquely identified. You can create individual badges using the procedure in the *Operator's Guide*. More likely, you should create a batch of badges (cards) at one time.

Automatic badge association

During a join, if a person has no badge assigned and the person's uuid matches the uuid of a badge record in the database, the system automatically matches the badge with the person. If the person has no badge and no uuid matches, the system creates a new-person record.

Barcodes on badges

The system does not support adding and scanning barcodes.

However, a person's record contains 10 additional data fields. To use barcodes, you would assign a credential to the person just as you would for a proxy card. You then associate that credential with a barcode field on the card template you build in the Asure ID application. That barcode can be printed on a card. When the Wiegand reader scans the barcode, our system compares it to the assigned credential.

Card formats

A card format describes what a number means or how the system uses it to grant access. The format interprets the number, and, therefore, is separate and distinct from the number itself.

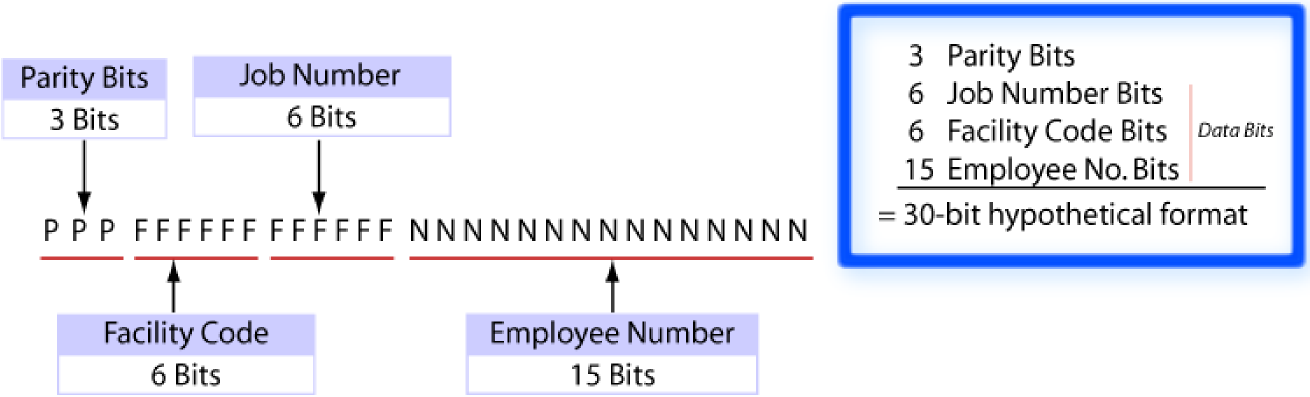
Different format technologies support a variety of bit-sizes for cards and readers. Bit size alone is not an indicator of a particular format type. For example, within the Wiegand family of formats are many possible bit sizes (26, 34, and many others). This system supports up to a 256-bit Wiegand format.

A format may comprise this information:

- Data bits contain such information as Facility Code, Credential Number, Job Number, and other information. The details of the format specification designate how many data bits are available for each element of information.

- Parity bit(s) serve as a simple accuracy check for the transmitted binary data.
- Total bits is the sum of the parity bit(s) and the data bits. This number is associated with the format name. For example: 26–bit Wiegand, 36–bit HID.

Figure 21. Example of a hypothetical 30-bit format



The example above shows how a format might be set up. The data bits include: six bits for Job Number, six bits for Facility Code, 15 bits for Employee Number, and three parity bits, for a total of 30 bits.

Within a given format bit length, the size and location of the data element, such as, Credential Number or Facility Code may vary. For example, a single 34-bit format may have an eight-bit Facility Code starting with bit number two, or it may have a 12-bit Facility Code starting at bit number 21.

You use the Wiegand Format Editor to create and view card formats, which require this information:

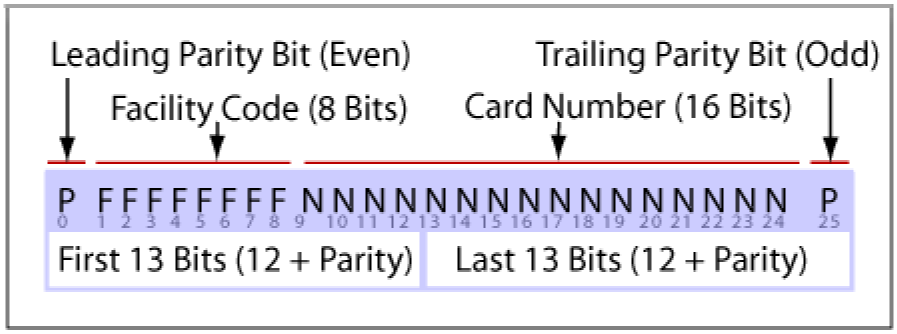
- Total bits
- Number and location of (if any) parity bits
- Parity bit format: odd or even
- Bit total and beginning bit number for Facility Number bits
- Bit total and beginning bit number for Credential bits
- Layout (format) for each parity bit

About the Wiegand format

The name “Wiegand” occurs in a variety of contexts. For the purposes of this document, it refers to the badge format or the associated reader-to-controller interface. The Wiegand Format Editor is required to define badge formats.

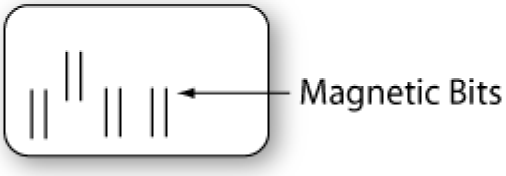
The system supports from 25–bit to 256–bit Wiegand formats.

Figure 22. Standard 26–bit Wiegand format


Leading Parity Bit (Even)
Trailing Parity Bit (Odd)
Facility Code (8 Bits)
Card Number (16 Bits)
P F F F F F F F F N N N N N N N N N N N N N N N N P
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
First 13 Bits (12 + Parity)
Last 13 Bits (12 + Parity)

The parity bit confirms the accuracy of the transmitted binary data by totalling the number of ones (1). If the total is an odd number, the format sets the parity bit to zero (0). If the total number of ones is even, it sets the parity bit to one (1).

Figure 23. Wiegand badge with embedded wire



Wiegand badges contain strips of wire embedded in the badge. When a person inserts a badge into or passes it through the set of magnetic field coils in a Wiegand reader, each strip sends a binary signal back to the reader.

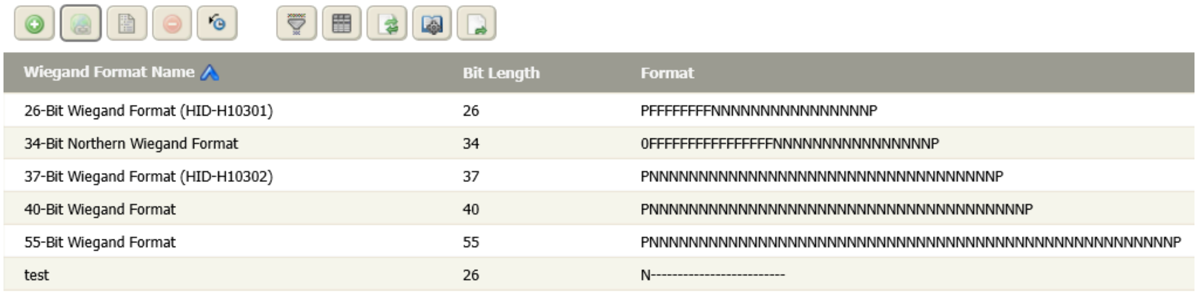
Creating (or editing) a card format

The popular Wiegand format provides many options. This procedure documents how to use the Wiegand Format Editor to create a Wiegand care format.

Prerequisites:
You are connected to the controller station and working in the web UI. If you are creating your own format, you have the specification that defines the format properties.

Step 1. Click **Controller Setup** > **Access Setup** > **Card Formats**.

The Card Formats view opens.



Wiegand Format Name	Bit Length	Format
26-Bit Wiegand Format (HID-H10301)	26	PFFFFFFFFNNNNNNNNNNNNNNNNP
34-Bit Northern Wiegand Format	34	0FFFFFFFFFFFFFFFFNNNNNNNNNNNNNNNNP
37-Bit Wiegand Format (HID-H10302)	37	PNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNP
40-Bit Wiegand Format	40	PNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNP
55-Bit Wiegand Format	55	PNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNP
test	26	N-------------------------

Step 2. Do one of the following:

- To create a new default format, click the Add From Default Card Formats button (

  ), and select a default format from the list and click **Ok**.

  A default format is useful if you deleted a format and want it back, or if you upgraded your system and do not already have these formats available.

- To design your own card format, click the Add button (

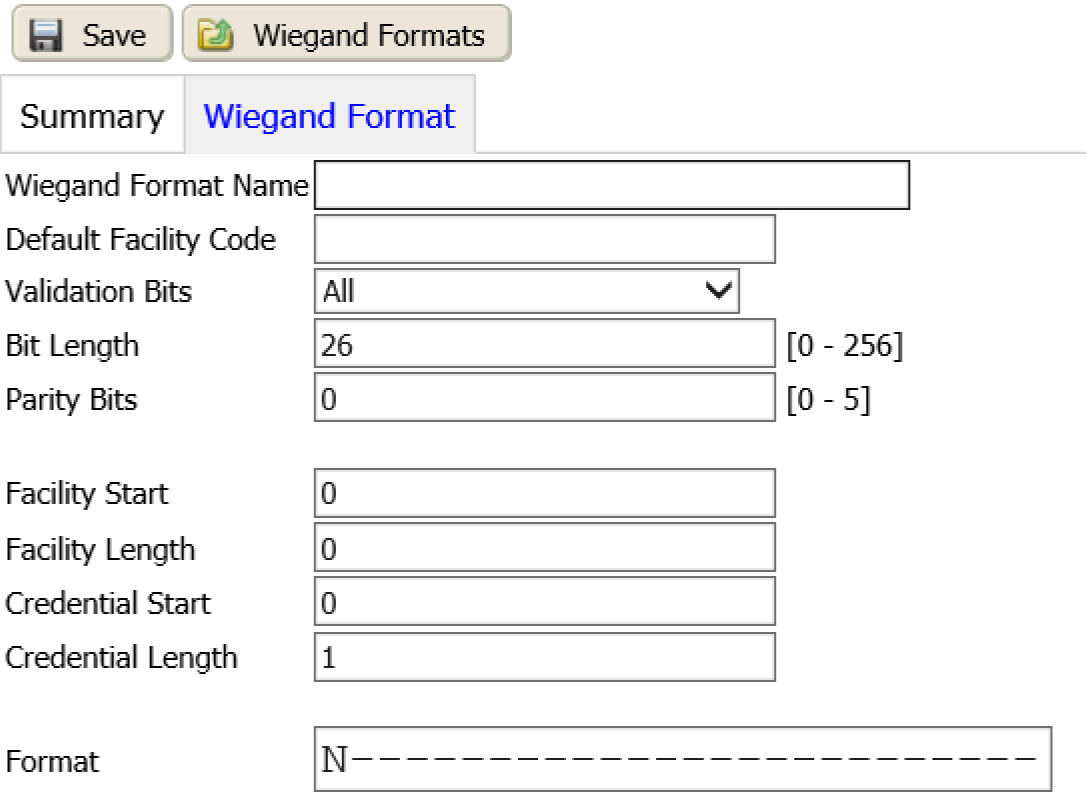
).

- To edit an existing format, select the format row, click the Hyperlink button (

) and click the Wiegand Format tab.

  NOTE: You cannot edit or delete a card format that is in use (assigned to a badge). In-use card formats display as read-only in the View Existing Wiegand Format view. Card formats that are not currently associated with a badge display in the Wiegand Format Editor view and may be edited.

If you clicked the Add button the Wiegand Format Editor (Add New Wiegand Format) view opens to the Wiegand Format tab.

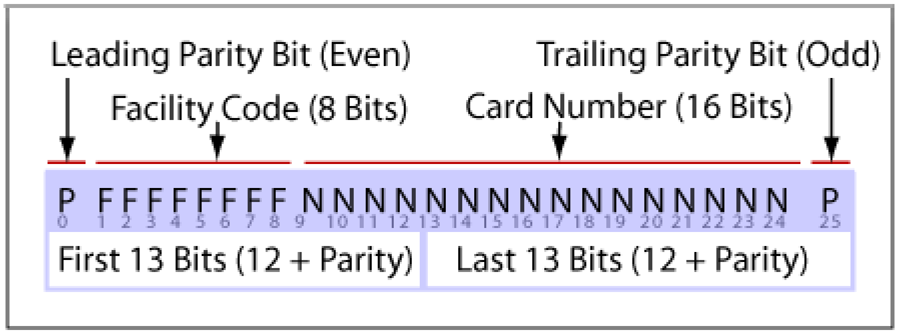


Wiegand Format Name		
Default Facility Code		
Validation Bits	All	
Bit Length	26	[0 - 256]
Parity Bits	0	[0 - 5]
Facility Start	0	
Facility Length	0	
Credential Start	0	
Credential Length	1	
Format	N-------------------------	

Step 3. Carefully fill in each property and click **Save**.
Parity Bits specifies the number of parity bits in the format. It does not identify the bit location(s).

Step 4. Define **`Facility Start`** and **`Facility Length`**, as well as **`Credential Start`** and **`Credential Length`**.

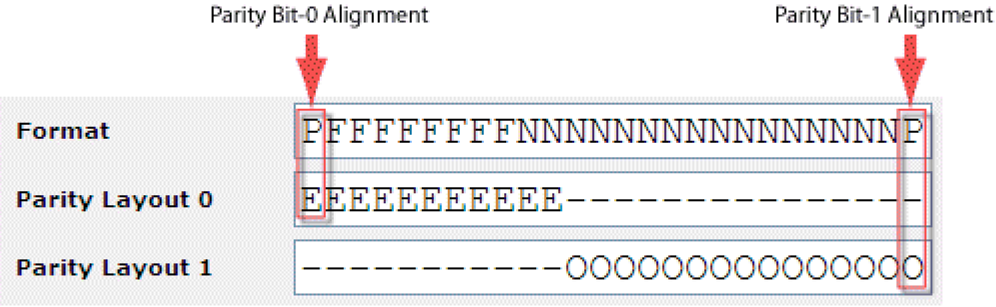
Step 5. Enter the format characters in the **`Format`** property.


Leading Parity Bit (Even)
Trailing Parity Bit (Odd)
Facility Code (8 Bits)
Card Number (16 Bits)
P F F F F F F F F N N N N N N N N N N N N N N N N P
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
First 13 Bits (12 + Parity)
Last 13 Bits (12 + Parity)

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)

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.



Format	PFFFFFFFFNNNNNNNNNNNNNNNNP
Parity Layout 0	EEEEEEEEEEE---------------
Parity Layout 1	-----------OOOOOOOOOOOOOOO

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.

Setting up usable credential numbers

A reader or keypad requires that a person present a valid badge, or key in a valid credential number followed by the # key. Credential numbers can be very long. Their use is prone to error when someone has to key in a long string of numbers including leading zeros. You can create a custom, 16-bit credential number (00001 to 65535), which is easier to enter.

Step 1. Create a new Wiegand format.

Step 2. Configure these properties and click **Save**:

- Validation Bits: All
- Bit Length: 16
- Credential Length: 16
- Format: NNNNNNNNNNNNNNNN (the letter "N" entered 16 times)

Step 3. To assign this format to a badge, click **Controller Setup** > **Personnel** > **Badges**.

Step 4. To create a new badge, click the Add button (⊕).

Step 5. Enter a five-digit custom credential in the **`Credential`** property (00001 to 65535).

Step 6. Click the chevron to the right of the Wiegand Format property and select the 16-bit format you created from the Ref Chooser and click **Ok**.

Step 7. To save the configuration, click **Save**.

Creating multiple badges (batch-create)

You can create a group of badges that have common properties.

Prerequisites:
You are working at the Supervisor station.

Step 1. From the system's home view, select **Personnel** > **Badges**.
The Badges view opens.

Step 2. Click the Batch Enroll button (❐).
The Batch Enroll Badges view opens.

Step 3. Complete the properties that are to be shared for all badges scanned, including **`Description`**, **`Wiegand Format`**, **`Status`**, **`Issue Date`**, **`Expiration Date`**, **`Owner`**, **`Tenant`**, and **`Enrollment Reader`**.

Step 4. Swipe a set of cards (a batch) one at a time.
As you swipe each card, the card data displays in the **`New Badges`** property.

NOTE: If badge numbers do not appear, the corresponding Wiegand format has not been defined.

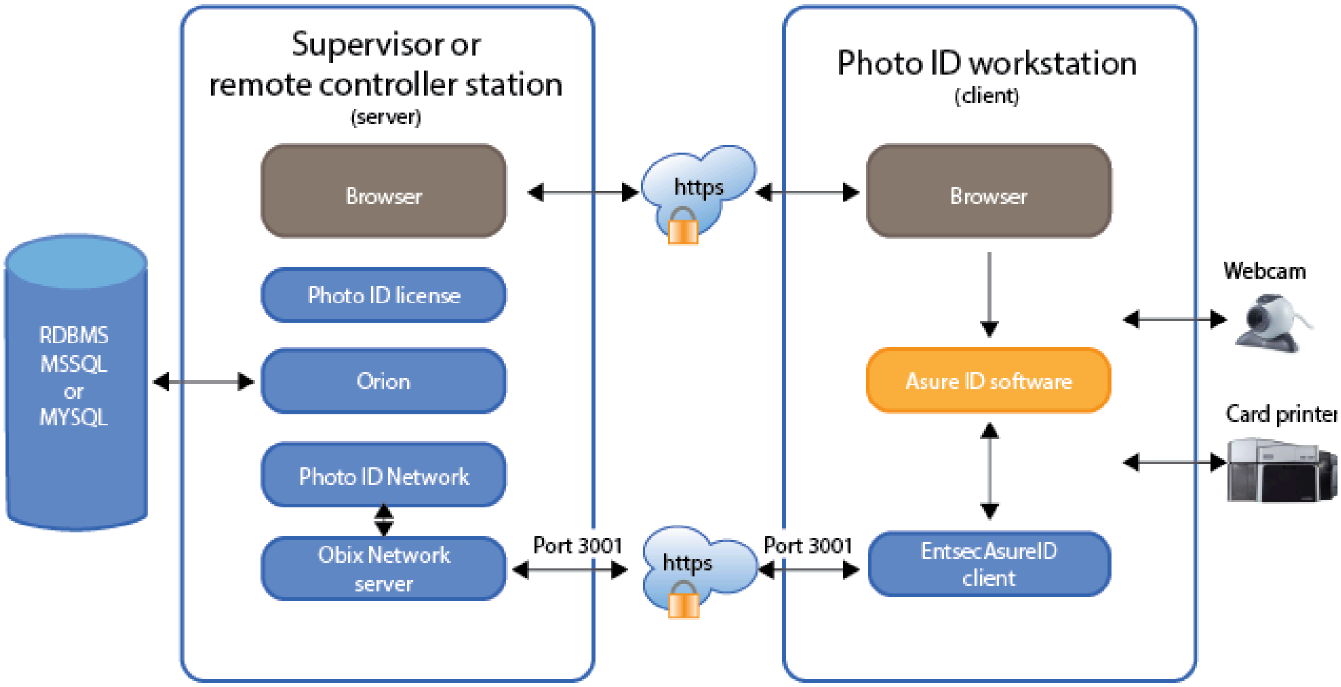
Step 5. To complete the batch-badge creation process, click the **Save** button.
The system saves the badges, and opens the Edit Badges view. The new badges appear in the table of badges.

Photo ID badges

Before you install and configure the Photo ID software, take a few moments to understand how the various elements work together.

RDBMS and Orion

Figure 24. Photo ID architecture



If you are seeing the above illustration in color, the blue boxes represent the framework's features that support Photo ID including RDBMS, license, networks and EntsecAsureID applet. The other boxes and internet clouds represent third-party software.

The Relational DataBase Management System (RDBMS) contains all personnel, badge (card), and other system records. It may be located on the Supervisor PC or on another network server. The OrionService in the station connects to the RDBMS.

Supervisor or remote controller station

This station, running in the Supervisor PC or in a stand-alone remote controller, connects the (Native Badge Printing Application) supported from EntSec 4.15 with the RDBMS .

- The Photo ID license authorizes use of this feature.
- The OrionService connects the station to the RDBMS.
- Secure communication over the Obix Network requires a machine-to-machine user, password, and `HTTPBasicScheme` authentication.

While you may access the Supervisor station using Workbench, it is recommended to use the web UI running in a browser.

Photo ID workstation

Although the Supervisor station and Photo ID workstation may share the same platform, separating them provides the most secure configuration. Installations with a single, stand-alone controller require a separate Photo ID workstation. The Supervisor station and Photo ID workstation communicate via the Internet or local area network.

- A browser lets you access the Supervisor or remote controller station remotely.

- The third-party Asure ID software manages the webcam and prints photo IDs using personnel data retrieved from the database. Asure ID relates to the Photo ID Network as a device on the network.
- EntsecAsureID running in the Photo ID workstation relates as a child to the oBIX Network.

Installation summary

The variety of applications that make up the Photo ID feature require several separate procedures. Photo ID installation and configuration involves these tasks:

- Decide on names and password clue.
- Set up the Photo ID Network and discover the Native Badge Designs device.
- Create a px view for Native Badge Designs template.
- Create a template for a badge.
- Assign a template to a badge.
- Configure Photo ID options in the station.

Names and password clue

You will have the opportunity to name various items and create oBIX credentials (username and password) during the configuration process. If you have only one Photo ID workstation you can accept the default names. With multiple workstations, it helps to differentiate among them. The table that follows provides a place to keep track of configuration names.

NOTE:

For security reasons, do not write the password itself in the table. Rather write a clue that will help you remember what the password is.

Table 24. Required names and credentials

Name	Where used	When created	Name	Other name/notes
oBIX machine-to-machine role	Sets up Obix Network access permissions	User Management > Roles tab	Suggested role name: obix	
oBIX machine-to-machine user	Sets Obix Network user, password, and assigns the machine-to-machine role	User Management > Users	Suggested user name: obix	Password clue:
Photo ID Network	Manages Asure ID client and badge templates	System Setup (Controller Setup) > Remote Devices > Remote Drivers	Name defaults to Photo ID Network	
Obix Network	Manages the connection between Third party software and the Photo ID network	System Setup (Controller Setup) > Remote Devices > Remote Drivers	Name defaults to Obix Network	
Photo ID Viewer Name	Associates a camera with a view in the software.	Photo ID > Photo ID Viewers (tab)	Suggestion: name the viewer for location of the camera in the building.	
Templates Display Name	Used to assign a template to a badge.	Entered when you discover template(s).	Name defaults to the name used when you created the template. Suggestion: name the template for the tenant company.	
Badge Description	Used to select the badge	Entered on the Personnel > Badge tab.	Suggestion: use a name to describe the type of badge.	

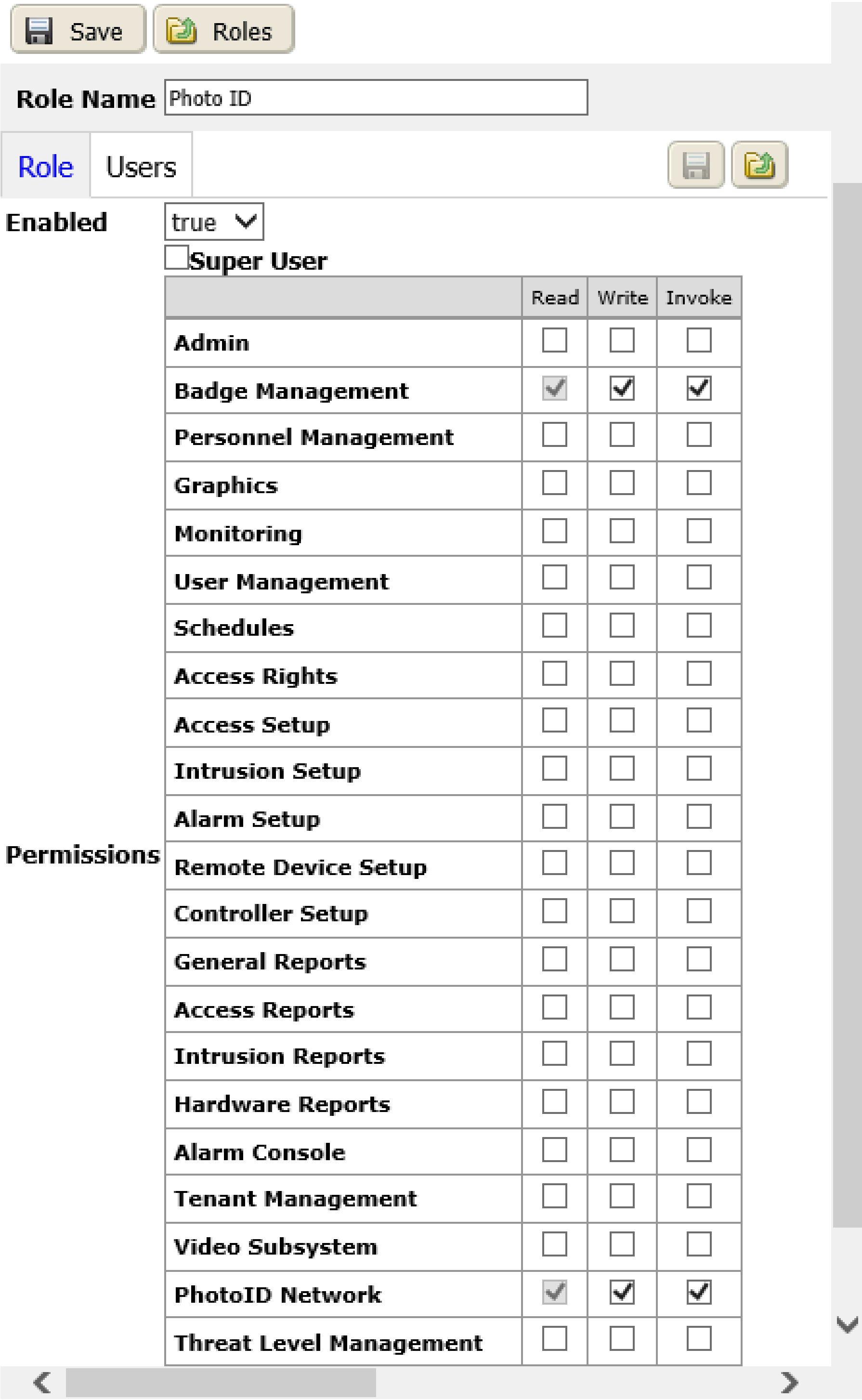
Setting up the Obix role

A machine-to-machine oBIX role sets up the permissions required for the EntsecAsureID to access the Obix Network.

Prerequisites:
Using the web UI, you are connected to the Supervisor station.

Step 1. From the main menu, click **System** > **User Management** > **Roles**.

Step 2. To create the role, click the Add button (⊕).
The Add New Role view opens.



Role Name Photo ID

Enabled true

☐ **Super User**

Permissions

	Read	Write	Invoke
Admin	☐	☐	☐
Badge Management	☑	☑	☑
Personnel Management	☐	☐	☐
Graphics	☐	☐	☐
Monitoring	☐	☐	☐
User Management	☐	☐	☐
Schedules	☐	☐	☐
Access Rights	☐	☐	☐
Access Setup	☐	☐	☐
Intrusion Setup	☐	☐	☐
Alarm Setup	☐	☐	☐
Remote Device Setup	☐	☐	☐
Controller Setup	☐	☐	☐
General Reports	☐	☐	☐
Access Reports	☐	☐	☐
Intrusion Reports	☐	☐	☐
Hardware Reports	☐	☐	☐
Alarm Console	☐	☐	☐
Tenant Management	☐	☐	☐
Video Subsystem	☐	☐	☐
PhotoID Network	☑	☑	☑
Threat Level Management	☐	☐	☐

Step 3. Enter `obix` for the **Role Name**.

Step 4. Grant full access to the **`Badge Management`** and the **`Photo ID Network`**, then click **Save**.

Result

If you recently upgraded your system from AX, the migration tool may have created an `obix` role for you.

Setting up the oBIX user

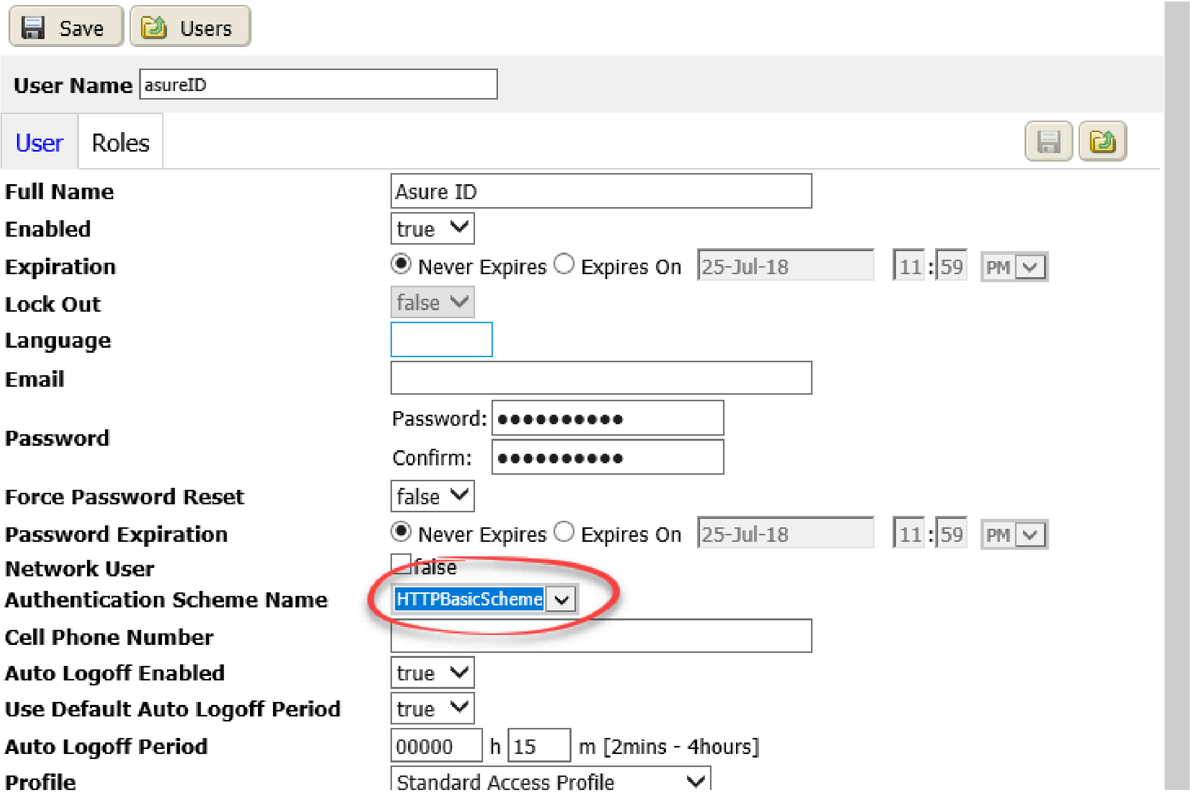
This user configures credentials that permit the EntsecAsureID to access the Obix Network.

Prerequisites:

You are using the web UI and are connected to the Supervisor station.

Step 1. From the main menu, navigate to **System Setup** > **User Management** and click **Users**.
The User Management view opens.

Step 2. To create the user, click the Add button (⊕).
The New User view opens.



User Name	asureID
Full Name	Asure ID
Enabled	true
Expiration	● Never Expires ○ Expires On 25-Jul-18 11:59 PM
Lock Out	false
Language	
Email	
Password	Password: ●●●●●●●●●● Confirm: ●●●●●●●●●●
Force Password Reset	false
Password Expiration	● Never Expires ○ Expires On 25-Jul-18 11:59 PM
Network User	□ false
Authentication Scheme Name	HTTPBasicScheme
Cell Phone Number	
Auto Logoff Enabled	true
Use Default Auto Logoff Period	true
Auto Logoff Period	00000 h 15 m [2mins - 4hours]
Profile	Standard Access Profile

Step 3. Enter the **`User Name`**, which is just below the **Save** button.
Use the name you planned. If you are upgrading from AX, the migration tool may have created and configured a user for you with the name `obix`.

Step 4. To set up the credentials for accessing the oBIX network, enter a password that meets N4 standards and an **`Authentication Scheme Name`** of `HTTPBasicScheme`.
New users default to the `DigestScheme`, which does not work for machine-to-machine users.

NOTE: If the `HTTPBasicScheme` is not available, use Workbench to add it to your installation. Refer to “Setting up the authentication scheme for Asure Id and Easy Lobby” in this document.

Step 5. To assign the Photo ID role to this user, click the Roles tab, click the Assign Mode button (▤), select the role in the Unassigned pane, click the Assign button (⊕), and click **Save**.

Step 6. If needed, make a note of the User name and Password so that later you can enter for any third party application software required to establish communication.

Setting up the Photo ID Network

The Photo ID Network manages the Native Badge printing application supported by the EntSec 4.15 version.

Step 1. Click **System Setup** > **Remote Devices** > **Remote Drivers**.

Step 2. Click the Manage Drivers button (⚙), select **Add** and click **Ok**.
The **Add Driver** window opens.

Step 3. Select **Photo ID Network** and click **Ok**.
The **Add Driver** window opens.

Step 4. Name the network, and click **Ok**.
The system adds the Photo ID Network to the database and displays the restart-station message.

Step 5. To restart the station, click **Ok**.
The **Status** column for the Photo ID Network indicates `{fault}` as the station restarts (this could take several minutes). During restart the station display name in the upper right of the browser view dims. When the station is running again the station display name appears normal.

Native Badge Designs Device under photo id network

The Native Badge Design Device allows for Badge Printing without third-party software. Follow the steps below to verify if the Native Badge Designs exist under the photoId network.

Step 1. Click **System Setup** > **Remote Devices** > **Remote Drivers**.
The **Remote Drivers** view opens.

Step 2. Confirm that the **`Status`** column for Photo ID Network indicates, `OK`.

Step 3. Double-click on the **Photo ID Network** row in the table to open it. Confirm that the **`Status`** column for **Photo ID Network** indicates `OK`.

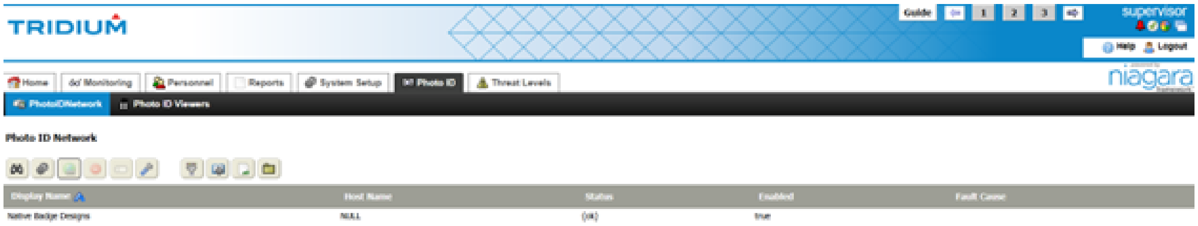


Photo ID Network

Display Name	Host Name	Status	Enabled	Fault Cause
Native Badge Designs	NULL	{ok}	true	

The **Photo ID Network** view opens.

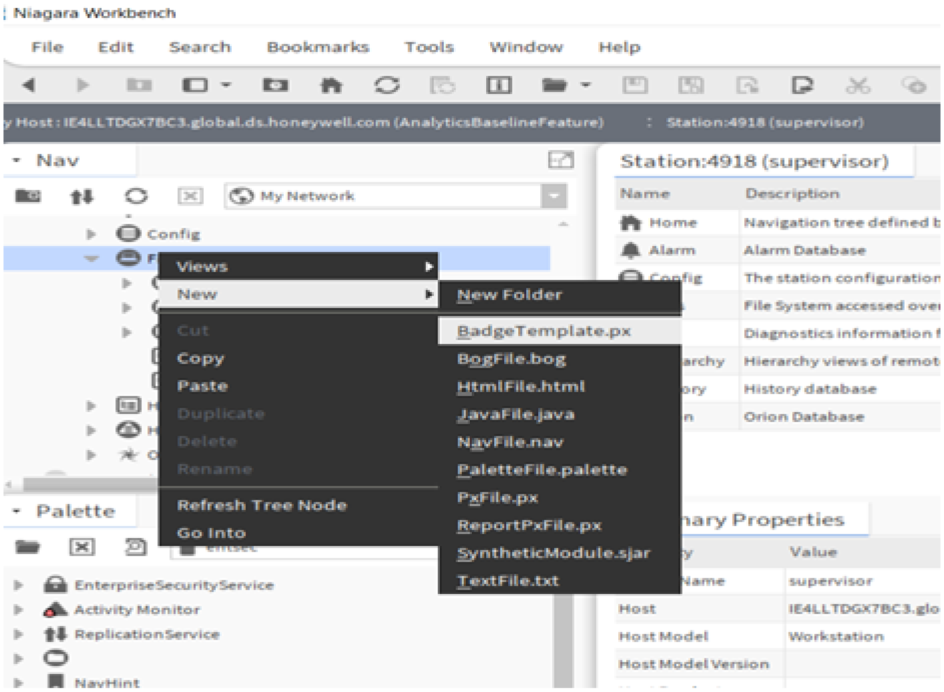
Step 4. Check the **Native Badge Designs** device is present under the photo ID network.

Create a px view for the Native Badge design template

Once the Native Badge Design Device is configured, you must create a new template linked to the badge "Template. Px." Each badge design template consists of two files or properties, "Front Design and Back Design," that must be associated with the px created by the users under the workbench; follow the below steps to create px for the Badge Design Template.

Step 1. Navigate to the station under the Workbench and open the **Files** folder.

Step 2. Right-click on **New** under Files, then rename `BadgeTemplate.px` as required.

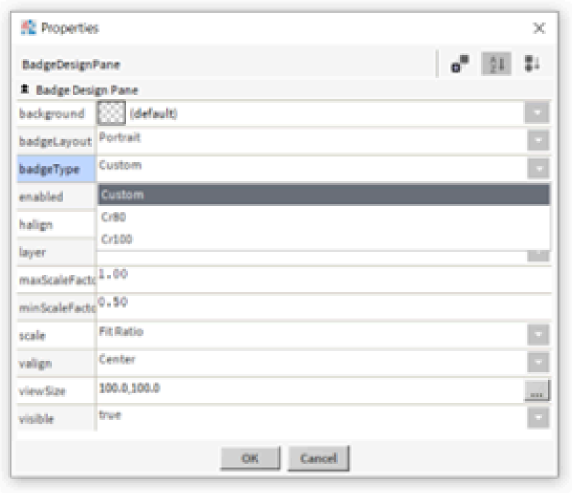


Name	Description
Home	Navigation tree defined b
Alarm	Alarm Database
Config	The station configuration
	File System accessed ove
	Diagnostics information f
archy	Hierarchy views of remot
ory	History database
n	Orion Database

y	Value
Name	supervisor
Host	IE4LLTDGX7BC3.glo
Host Model	Workstation
Host Model Version	

Step 3. Right-click on the file created and select **view** > **px editor**, the px file opens in px file in edit mode, with **BadgeDesignPane** as the default pane.

Step 4. Double-click on the **BadgeDesignPane** under the widget tree, and update the required badge Layout and badge type property on **BadgeDesignPane** based on the card type.



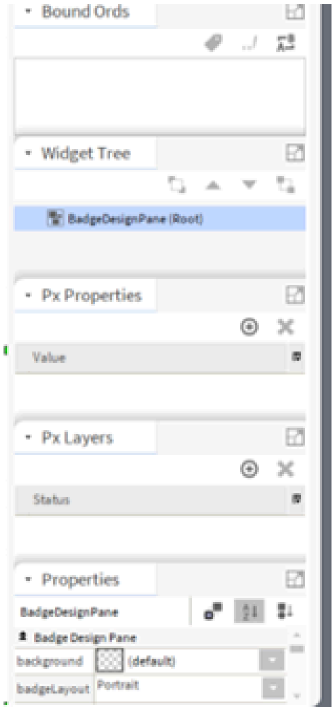
Properties

BadgeDesignPane

Badge Design Pane

background (default)
badgeLayout Portrait
badgeType Custom
Custom
Cr80
Cr100
enabled
halign
layer
maxScaleFactc 1.00
minScaleFactc 0.50
scale Fit Ratio
valign Center
viewSize 100.0,100.0
visible true

OK Cancel



Bound Ords

Widget Tree

BadgeDesignPane (Root)

Px Properties

Value

Px Layers

Status

Properties

BadgeDesignPane

Badge Design Pane

background (default)
badgeLayout Portrait

We currently support two types of standard cards, CR80 and CR100, the industry's most commonly used ID cards. The card size will automatically update based on the selected badge type and layout properties.

The default view size for the Badge type property is listed below:

Badge Type	Badge Layout	Width	Height
CR80	Portrait	153	243
CR80243		243	153
CR100	Portrait	189	279
CR100	Landscape	279	189

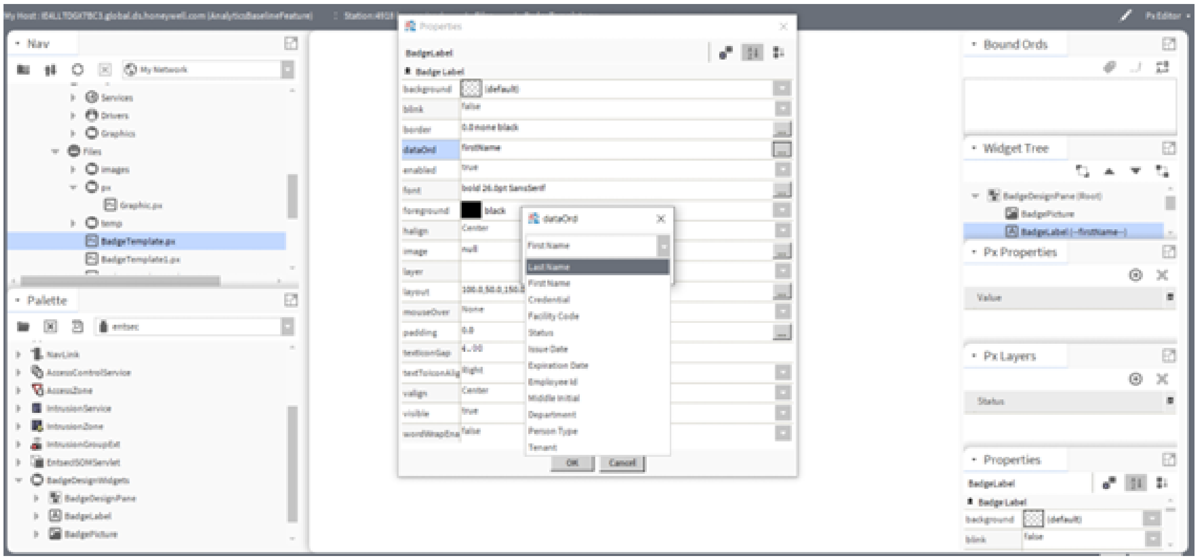
NOTE:

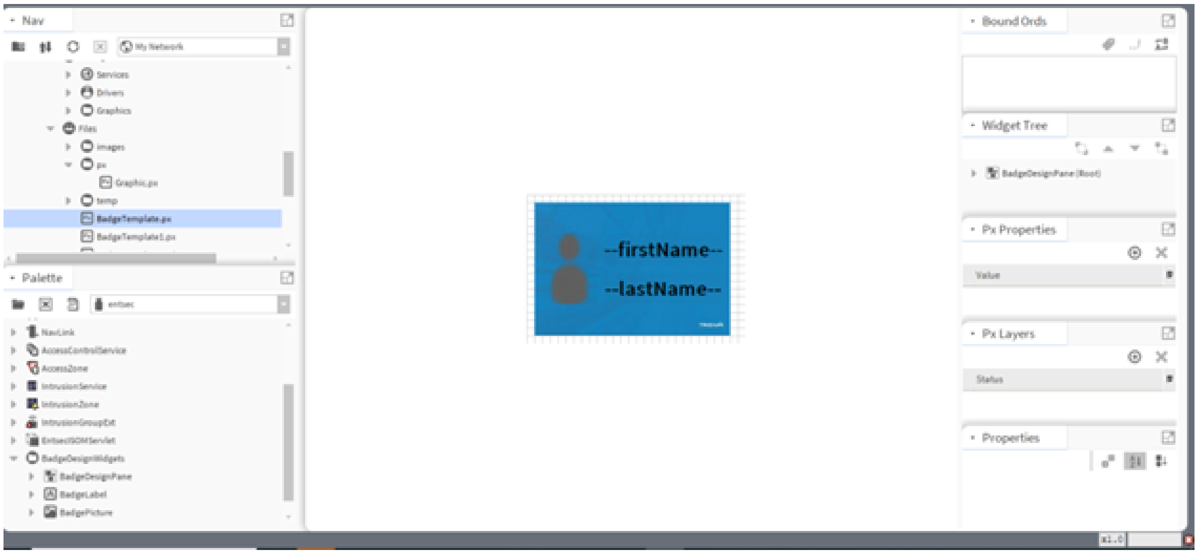
If the user needs to create a custom card, they can directly update the width and height under the view size property. The badge type will automatically be updated to 'Custom.' However, the badge layout property does not apply to the custom badge type.

Step 5. After updating the badge type and layout, you can design the badge using existing widgets such as Label and Picture and two new design widgets: BadgeLabel and BadgePicture.

- **BadgePicture:** The BadgePicture widget automatically retrieves the individual's image from the database.
- **BadgeLabel:** The BadgeLabel widget fetches the necessary person and badge properties from the database.

  Here are some properties of dataOrd for the BadgeLabel widgets that could be retrieved from the database:





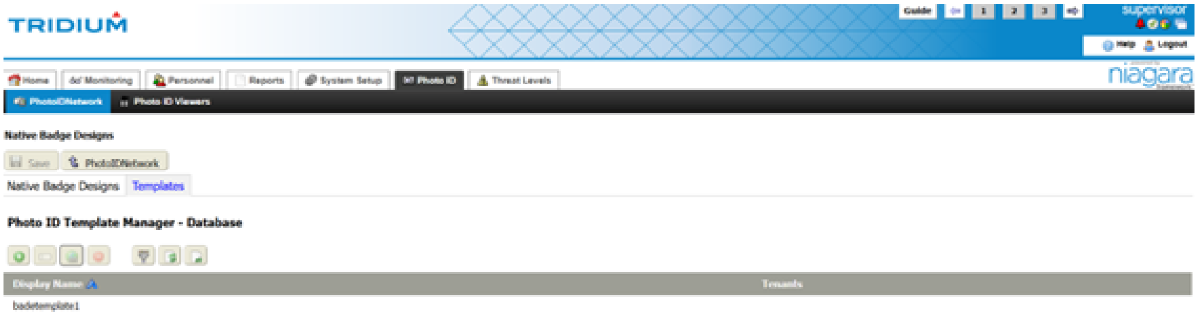
Step 6. After designing the badge, you can save it as a Px file and then return it to the Enterprise Security appliance view in the browser.

Create a badge template

Create a template for Native Badge Designs located under the **photoIdNetwork** section.

Step 1. Login to the station and click on **photo Id** > **photoIDNetwork.**

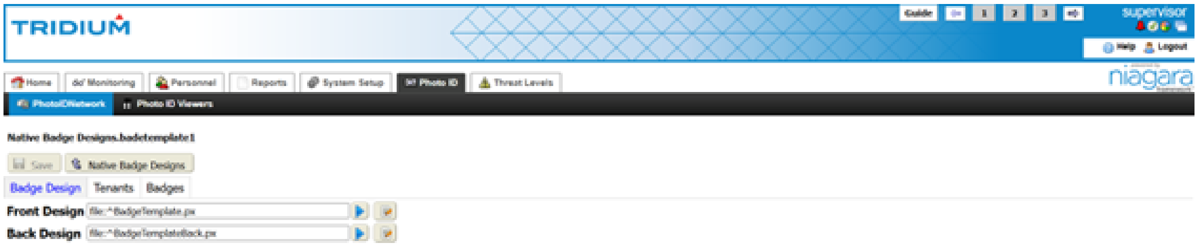
Step 2. Under **photoIDNetwork** double click on **NativeBadgeDesigns** > **Templates.**



Step 3. To create a template, click the **Add** button and select **New Template**, update the name, and click

OK .

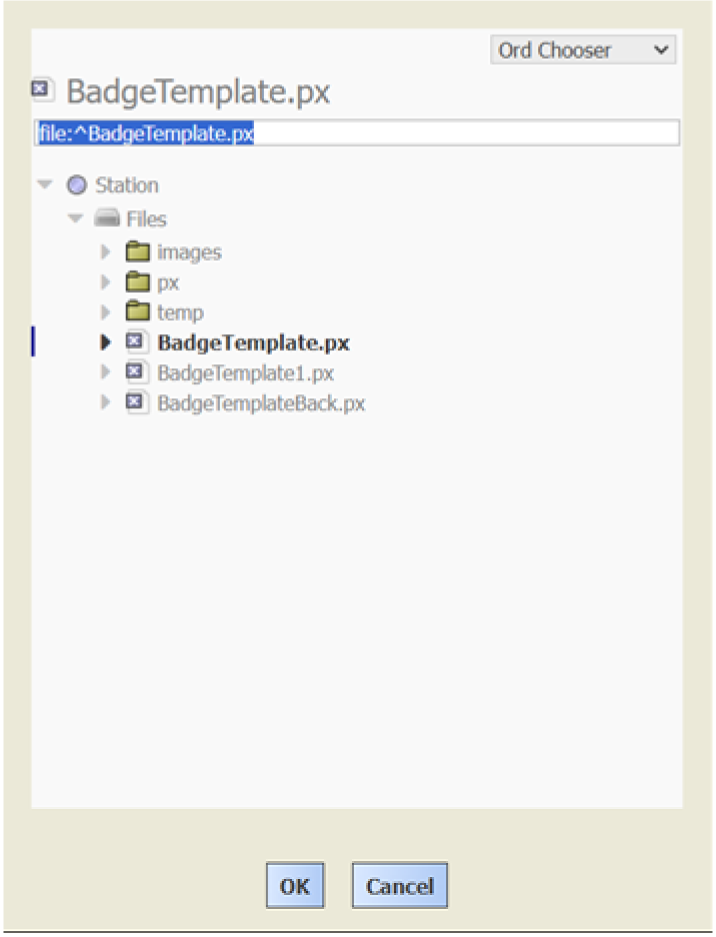
Step 4. Once the template is created, click on the 📝 button to select the px file created in the workbench for FrontDesign and BackDesign.



Native Badge Designs.badetemplate1

Front Design file:^BadgeTemplate.px

Back Design file:^BadgeTemplateBack.px



file:^BadgeTemplate.px

The **FileordChooser** window opens.

Step 5. Select the appropriate px file ord from the list and click OK .

NOTE: Please note that if the front design is updated, the badge will only be printed on one side. If double-sided badge printing is required, the Front and Back Designs must be updated with appropriate px files.

Step 6. Once both the orders are selected, click on the Save button.

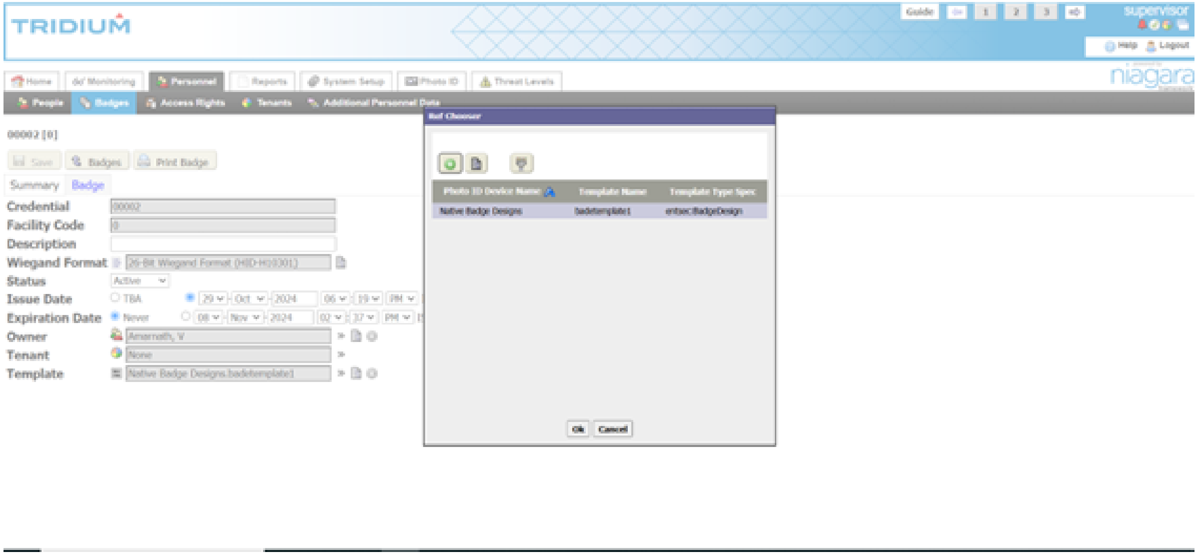
Assigning a template to a badge

The system defines each badge by associating it with a specific Native Badge Designs template.

Step 1. From the home view, click **Personnel** followed by clicking the **Badges** tab.
The **Badges** view opens.

Step 2. To add one or more badges, click the add button (⊕) or scan the badge.
How to add a badge is explained in detail elsewhere.
The **Add New Badge** view opens.

Step 3. Click the chevron next to the **Template** property.
The **Ref Chooser** window opens.



00002 [0]

Credential	00002
Facility Code	0
Description	
Wiegand Format	26-Bit Wiegand Format (HID-H10301)
Status	Active
Issue Date	○ TBA ● 29 Oct 2024 06 19 PM
Expiration Date	● Never ○ 08 Nov 2024 02 37 PM
Owner	Amarnath, V
Tenant	None
Template	Native Badge Designs.badetemplate1

Ref Chooser

Photo ID Device Name	Template Name	Template Type Spec
Native Badge Designs	badetemplate1	entsec:BadgeDesign

Step 4. Select the badge, click **Ok** and click **SAVE**.

Setting up a camera

Viewers associate cameras connected to the Photo ID workstation with the Photo ID Network.

Prerequisites:
You use the web user interface and are connected to the Supervisor station or remote controller.

Step 1. Expand the **Photo ID** and double-click the **Photo ID Viewers** node.
The viewer's view opens.

Step 2. Click the Add button (⊕).

Step 3. Enter the name of the camera and click **Ok**.

Configure photo options

The system displays the photo associated with an individual employee badge side-by-side with the feed from a surveillance video camera. You may add and configure all properties related to network device setup, such as how long to leave the photo up.

Step 1. From the home view, click **Photo ID** and the preferences button.
The Configure window opens.

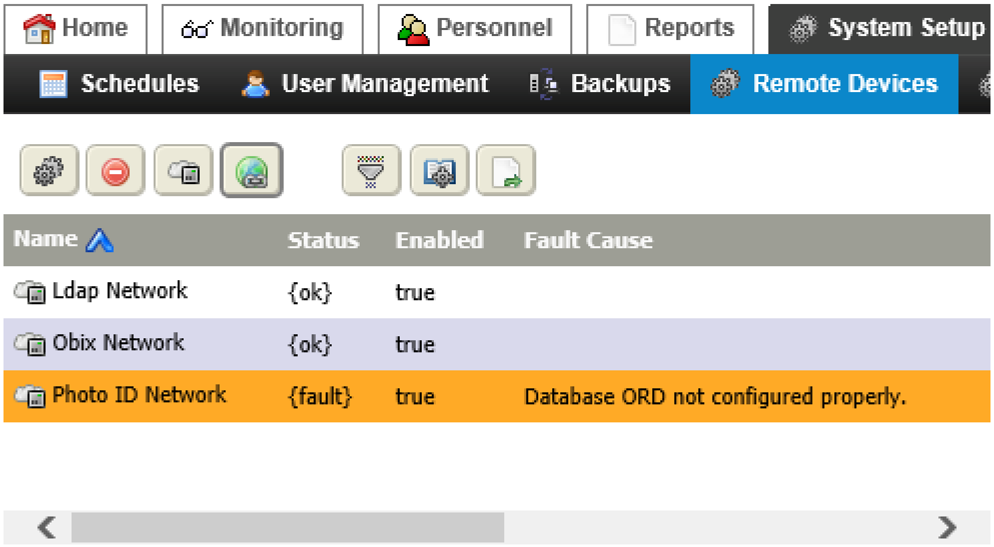
Step 2. Change the properties as necessary, and click `OK`.

Adding the Obix Network

The Obix Network, functioning as a server, enables communication between the framework and third party application software if required to establish communication through Obix network.

Prerequisites:
You are using the web UI and are connected to the Supervisor station.

Step 1. Click **System Setup** > **Remote Devices** > **Remote Drivers**.
The Remote Drivers view opens.



Name	Status	Enabled	Fault Cause
Ldap Network	{ok}	true	
Obix Network	{ok}	true	
Photo ID Network	{fault}	true	Database ORD not configured properly.

Step 2. Click the Manage Devices button ( ).
The **Manage Drivers** menu opens.

Step 3. Click **Add**.
The **Add Driver** menu opens.

Step 4. Select **Obix Network** and click **Ok**.
The **Add Driver** window opens.

Step 5. Optionally, you can change the name of the driver followed by clicking **Ok**.

Step 6. Check the **Status** column on the **Remote Drivers** view. It should read, `{ok}`.

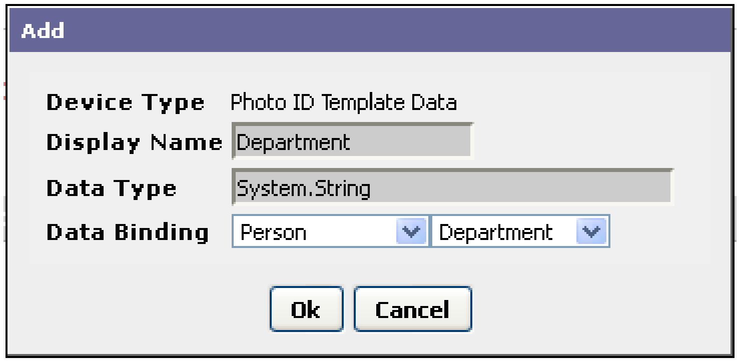
Binding template data properties to database properties

Data that appear on a badge need to be associated with individual database fields. The process of binding these data establishes these associations.

Step 1. Double-click on the newly added template.
The **Template** view opens, this time with three tabs: **Template Data**, **Tenants**, and **Badges**.

Step 2. Click the Discover button ( ).
The **Discovered** pane shows the properties you set up previously using the Asure ID software.

Step 3. Select the property row and click the Add button ( ).



Add

Device Type: Photo ID Template Data

Display Name: Department

Data Type: System.String

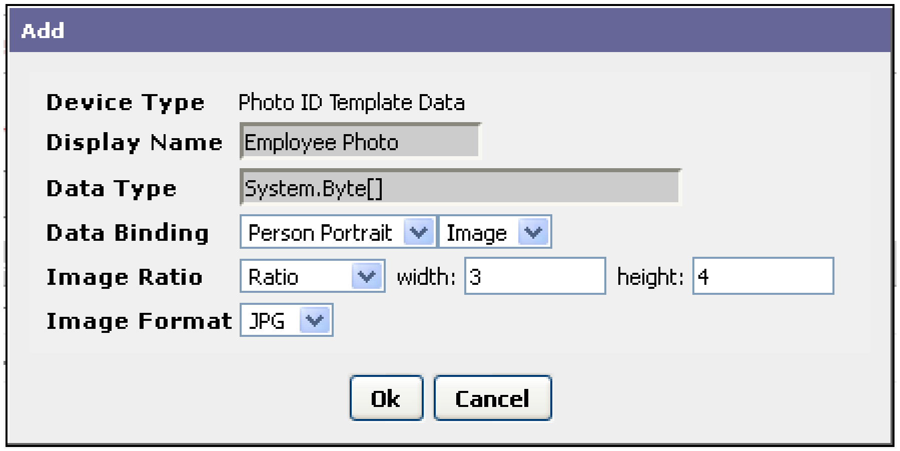
Data Binding: Person | Department

Step 4. Accept the default binding or change the **Data Binding** using the two options lists, and click **Ok**.

NOTE: You must bind each property individually, but you only need to do this once.

The first option list provides the set of options for the second option list. So, for example, to bind a person's department you would select `Person` in the first property. The `Person` option includes `Department` (and other options) in the second property. Then you can select `Department` in the second option list.

When you add the Photo property, **Image Ratio** and **Image Format** properties appear in the **Add** window. You can specify these parameters, as needed.



Add

Device Type: Photo ID Template Data

Display Name: Employee Photo

Data Type: System.Byte[]

Data Binding: Person Portrait | Image

Image Ratio: Ratio width: 3 height: 4

Image Format: JPG

Step 5. Configure the binding, enter the aspect ratio (for **Photo** properties) you used with you created the template and click **Ok**.
When finished, the **Template Data** database view reflects the new values in its **Data Binding** column.

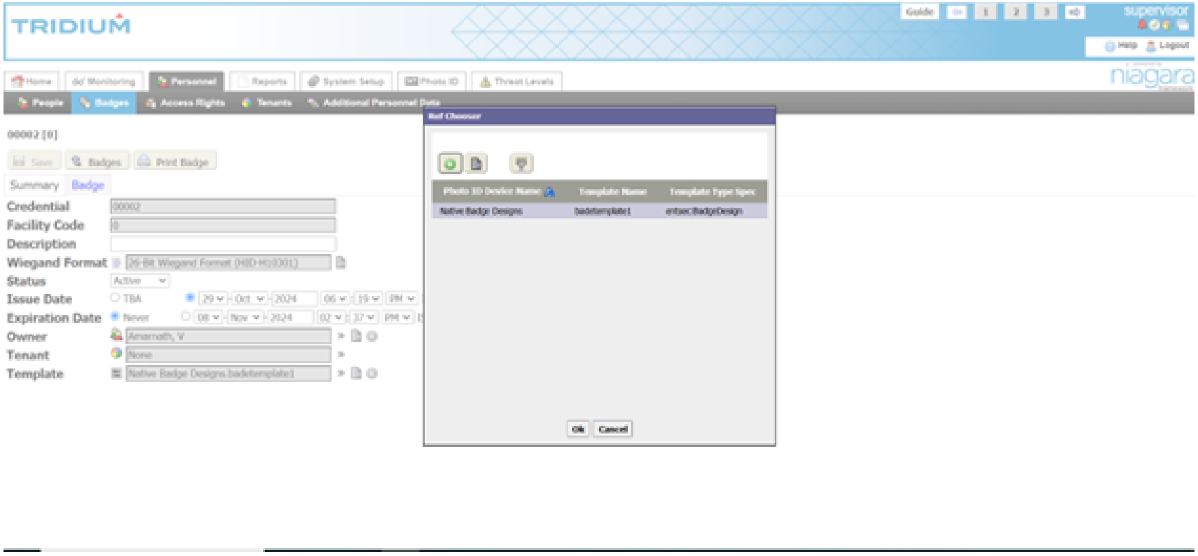
Assigning a template to a badge

The system defines each badge by associating it with a specific Native Badge Designs template.

Step 1. From the home view, click **Personnel** followed by clicking the **Badges** tab.
The **Badges** view opens.

Step 2. To add one or more badges, click the add button (⊕) or scan the badge.
How to add a badge is explained in detail elsewhere.
The **Add New Badge** view opens.

Step 3. Click the chevron next to the **Template** property.
The **Ref Chooser** window opens.



00002 [0]

Credential: 00002
Facility Code: 0
Description:
Wiegand Format: 26-Bit Wiegand Format (HID-H10301)
Status: Active
Issue Date: ○ TBA ● 29 - Oct - 2024 06 : 19 PM
Expiration Date: ● Never ○ 08 - Nov - 2024 02 : 37 PM
Owner: Amarnath, V
Tenant: None
Template: Native Badge Designs.badetemplate1

Photo ID Device Name	Template Name	Template Type Spec
Native Badge Designs	badetemplate1	entsec:BadgeDesign

Step 4. Select the badge, click **Ok** and click **SAVE**.

Setting up a camera

Viewers associate cameras connected to the Photo ID workstation with the Photo ID Network.

Prerequisites:
You use the web user interface and are connected to the Supervisor station or remote controller.

Step 1. Expand the **Photo ID** and double-click the **Photo ID Viewers** node.
The viewer's view opens.

Step 2. Click the Add button (⊕).

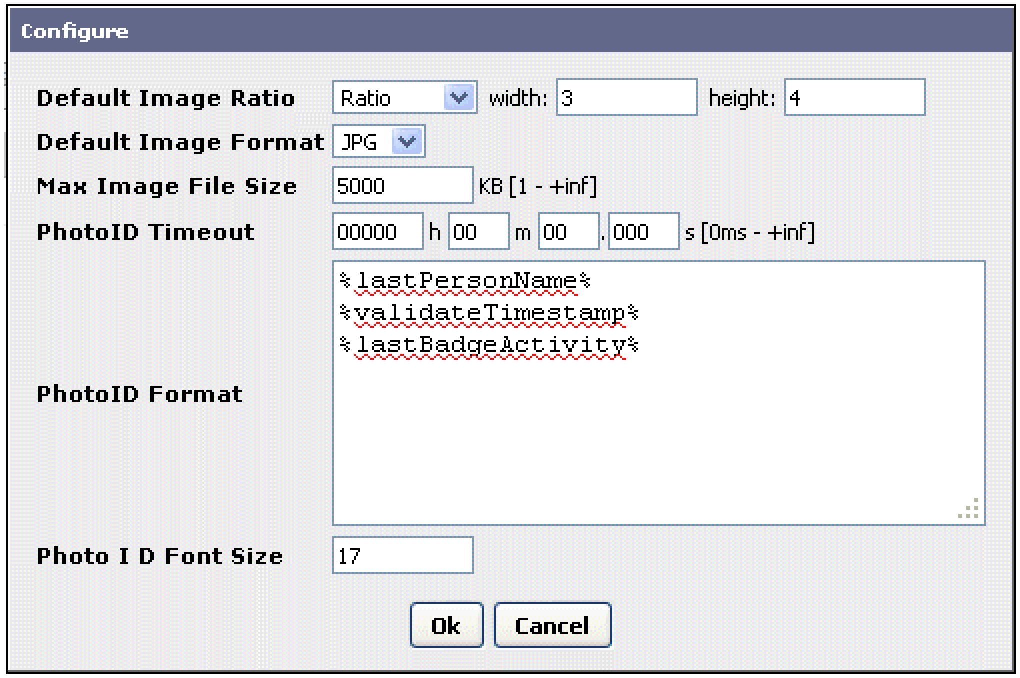
Step 3. Enter the name of the camera and click **Ok**.

Configuring photo options

The system displays the photo associated with an individual employee badge side-by-side with the feed from a surveillance video camera. You may add and configure all properties related to network device setup, such as how long to leave the photo up.

Step 1. From the home view, click **Photo ID** and click the preferences button (🔧).

The **Configure** window opens.



Configure

Default Image Ratio: Ratio width: 3 height: 4

Default Image Format: JPG

Max Image File Size: 5000 KB [1 - +inf]

PhotoID Timeout: 00000 h 00 m 00 . 000 s [0ms - +inf]

PhotoID Format:

```
%lastPersonName%
%validateTimestamp%
%lastBadgeActivity%
```

Photo I D Font Size: 17

Step 2. Change the properties as necessary, and click **Ok**.
For example, the **PhotoID Timeout** defaults to zero (0), which indicates no timeout. Configuring this value determines how long to display a photo from a swiped badge to keep the display current.

Configuring Asure ID alarms

Misuse of a badge to access a building generates an alarm. This procedure configures the alarm information collected from the Photo ID computer.

Prerequisites:

NOTE: This alarm indicates that communication is NOT active. For example, if the Photo ID workstationr is a notebook PC that only gets started to take pictures, you should not use this alarm.

Step 1. On the Photo ID Network view, double-click the AsureID Client Device row.

Step 2. Click the chevron next to **Alarm Source Info**.
The view expands to display alarm options.

Step 3. Configure alarm text as desired.
The **Video Setup** button enables video.

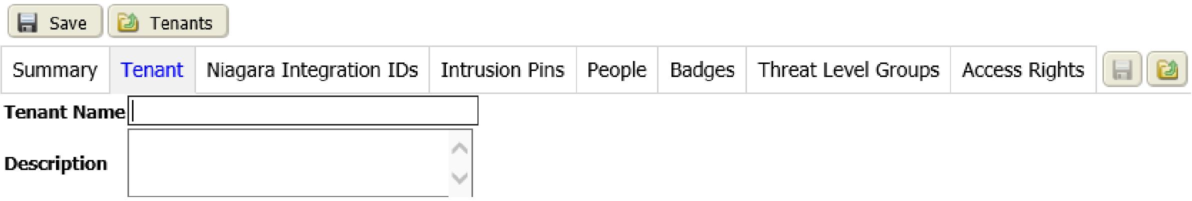
Creating a new tenant

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

Step 1. Click **Personnel** > **Tenants**
The Tenants view opens.

Step 2. Click the **Add** (⊕) button.

The **Add New Tenant** view opens.



Tenant Name

Description

Step 3. Provide the **Tenant Name** and an optional **Description** for the tenant.

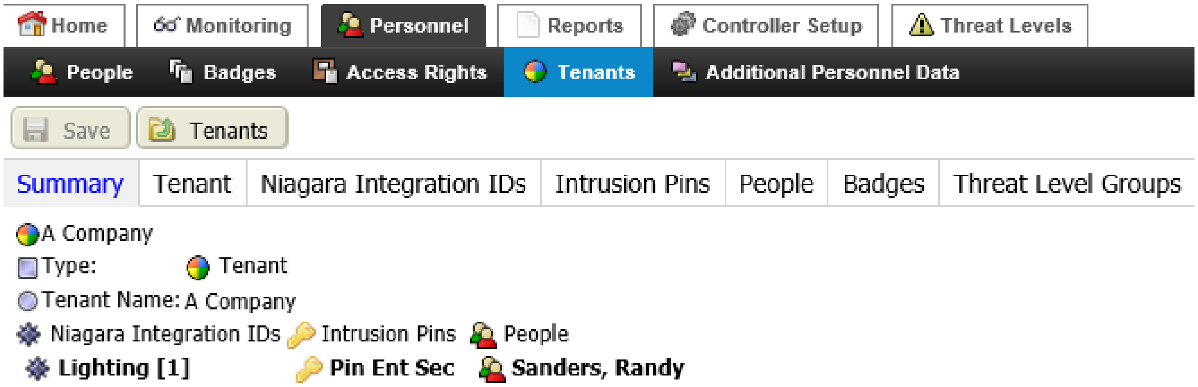
Step 4. Configure the individual tabs for each tenant and click **Save**.
Each tab provides a set of standard control buttons and two tables. The tables include assigned and unassigned assets (people, integration IDs, access rights, and badges) to associate with the specific tenant.
The new tenant is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

Editing an existing tenant

Once created, you may edit tenant information as required.

Step 1. Click **Personnel** > **Tenants**.
The Summary tab of the Tenants view opens.

Step 2. To edit a tenant, double-click the tenant row in the table.
The view associated with that particular tenant opens.



A Company

Type: Tenant

Tenant Name: A Company

Niagara Integration IDs	Intrusion Pins	People
Lighting [1]	**Pin Ent Sec**	**Sanders, Randy**

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

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

Setting up additional personnel properties

The Person tab of the Add New Person view collects basic personnel information (name, employee ID, etc.). You may have other information to collect. For example, you may need to know the level of security clearance the employee obtained or the person's rank in the military. You set up additional properties as information templates, which appear on the Person tab as additional properties.

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

Step 2. Click **Additional Personnel Data**.
The view opens.

Step 3. To add a property, click the Add button (⊕).
The Info Template tab opens.

Step 4. Give the new property a name and default value.

Step 5. To set up a string chooser from which to select a drop-down list of options, set **`Smart Sense`** to `true`.

Step 6. If the information to collect requires more than a single line of text, set **`Multi Line`** to `true`.

Step 7. To save your template, click **Save**.
The system adds the template as a property to the end of the Person tab.

Setting up person types

You can configure person types based on your organization’s needs. Only persons whose person type is designated as “supervisor” are eligible to be assigned as a supervisor for a specific access zone.

Prerequisites:
No person types exist yet in the system.

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

Step 2. Add a new person by clicking the Add button (⊕).
This can be a test person record, which you may delete later.
The Person tab opens.

Step 3. Enter a value in the **`Person Type`** property along with other properties, including a **`PIN`**, and click **Save**.
The system adds the person to the database. In the process, it uses the **`Person Type`** value you entered as the first person type in the system.

Step 4. Open the person record you created by double-clicking it in the table, and click the Person tab.
The Person tab opens.

Step 5. Click the chevron (>>) to the right of the **`Person Type`** property.
The String Chooser window opens.

Step 6. Select the person type you created.
This action enables the Add button (

⊕

) in the String Chooser.

Step 7. Add additional employee types and click **Ok**.

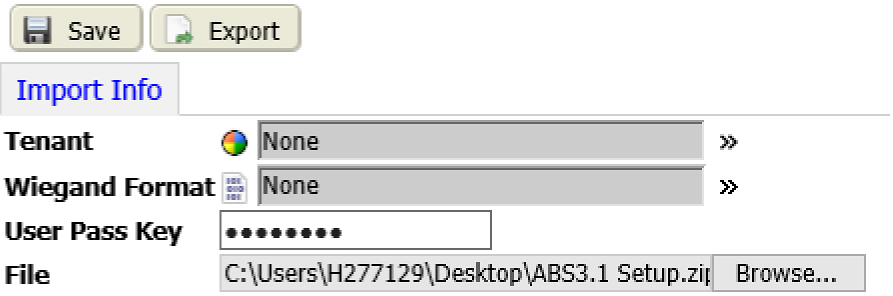
Importing personnel data from a CSV file

Importing personnel data is the quickest way to set up personnel records in the station database. This procedure imports the data into the Supervisor station’s database.

Prerequisites:
The CSV (Comma-Separated Values) file that contains personnel information exists and is ready to use. The Wiegand format has been identified or created and is ready. A Wiegand Format has been selected.

NOTE: The Import Info function only works at a Supervisor station.

Step 1. Navigate to **System Setup** > **Access Setup** > **Additional Personnel Entry**.
The Additional Personnel Entry view opens.



Tenant: None
Wiegand Format: None
User Pass Key: ••••••••
File: C:\Users\H277129\Desktop\ABS3.1 Setup.zi|

Step 2. Open the **`Tenant`** Ref Chooser () and select the tenant name.

Step 3. Open the **`Wiegand Format`** Ref Chooser and select the card format.

Step 4. Enter the **`User Pass Key`** and click the **Browse** button to find the CSV file.

Step 5. To initiate the import, click **Save**.

NOTE: When you open an exported CSV file, long credential numbers display in scientific notation.

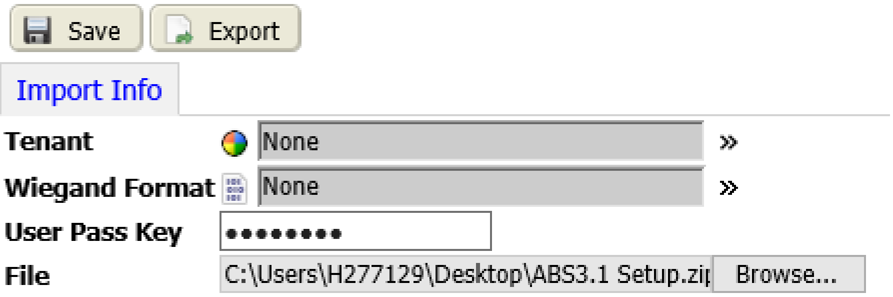
The import process runs as a job and displays a list of errors (if any) at the end of the process.

Step 6. To confirm that the data are in the station database, click **Personnel**, followed by clicking **People**, **Badges**, **Access Rights** and observing the new data.

Exporting personnel data from a CSV file

Exporting additional personnel data to a CSV file makes the data available to import into another Supervisor database or to use for some other purpose. Exported data are password protected by a **`Pass Key`** you create when you export the file. At import, the same pass key is required to successfully import the personnel data.

Step 1. Navigate to **System Setup** > **Access Setup** and click **`Additional Personnel Entry`**.
The Additional Personnel Entry view opens.



Tenant: None
Wiegand Format: None
User Pass Key: ••••••••
File: C:\Users\H277129\Desktop\ABS3.1 Setup.zi|

Step 2. Open the **`Tenant`** Ref Chooser and select the tenant name.

Step 3. Open the **`Wiegand Format`** Ref Chooser and select the card format.

Step 4. Create the **`User Pass Key`**.

Step 5. Enter the name of the CSV file to create and click the **Export** button.

Chapter 11. Intrusion zone management

An intrusion zone combines multiple sensors into logical groups for arming and disarming a defined space (zone) within a building. A group of points defines a single intrusion zone. Grouping points from other connected stations can become part of the single intrusion zone. A single intrusion zone status point represents the state of the intrusion zone and identifies, by sensor, any alarms generated in the zone.

The system offers flexibility when it comes to arming and disarming intrusion zones. To manage multiple zones from a single location, a single reader or keypad may be assigned to several zones. To allow arming and disarming a single zone from multiple locations, several devices may be assigned to a single zone. Intrusion zones may be controlled by schedules, hardware inputs, and by configuring properties in a browser interface.

Grouping includes points from other connected stations as part of a single intrusion zone. This lets you extend the zone to include readers, points, or relays that are under those additional stations. In addition to extending the intrusion zone physically, this allows sharing of arming status and zone enabled. For example, to view or control a zone's status (armed or disarmed) from a peer station or a Supervisor station, you can do so if they are grouped.

The system logs all activity regarding enabling, disabling, and alarms within an intrusion zone. In addition, it independently logs by zone and source sensor any alarms generated by a sensor in the intrusion zone.

Devices used to enable and disable intrusion zones

Depending on the requirements and available hardware configuration, the enabled and disabled status of an intrusion zone may be controlled by different methods. If a single reader is assigned to more than one intrusion zone, then that reader enables or disables all zones to which it is assigned.
The system allows you to associate these devices and methods with intrusion zones:

- Card reader
- SmartKey device (SmartKey device provides keypad for entering a PIN and for arming, disarming, and displaying the status of intrusion zones.)
- Schedule
- Contact input
- A manually-configure method using the browser interface.

You configure the zone-device relationship by assigning the device to the zone or the zone to the device.

Intrusion zone status indicators

The behavior and display color of designated LED indicators indicate the current status and operation of the intrusion zone (armed, disarmed, arming, disarming, waiting for exit, waiting for PIN, and other indications).

Audible beepers indicate current status and operation of the intrusion zone (armed, disarmed, arming, disarming, and other states).

Audible beeper patterns indicate current status and operation of the intrusion zone (armed, disarmed, arming, disarming, and other states).

Zone alarms related to groups can initiate system actions, including:

- Output to a relay
- Email notification
- Dialer interface

Grouping

Creating a group adds peer-to-peer and subordinate stations to an existing intrusion zone. In so doing, it relates the remote host's intrusion zone to the Supervisor station. Specifically:

- Stations to group must be joined in either a peer-to-peer or Supervisor-to-subordinate relationship.
- The Entry Reader and Exit Reader tabs display only on the local controller readers.
- You can only add readers to intrusion zones when you are connected to the reader's assigned station. Readers are not visible and cannot be configured from remotely-grouped stations.

Using both a schedule and a PIN

If you plan to use both a schedule and a PIN:

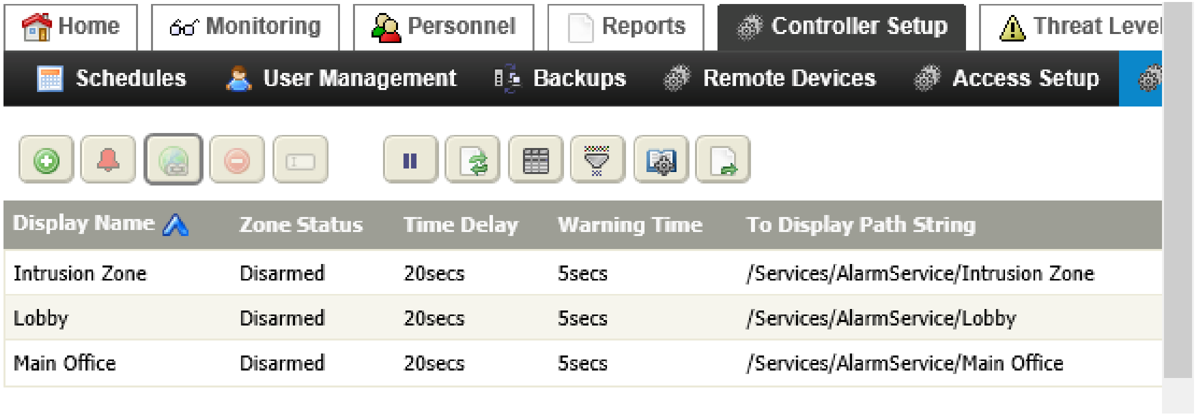
- If the zone is armed using a schedule, the PIN can disarm the zone. To arm the zone again, the schedule must change state to disarm and back to arm.
- If the zone is armed using a schedule, and the zone is already armed, entering the PIN arms it again. The system counts down again, but the state stays the same. If the zone is armed by a PIN and a schedule changes to the arm state, nothing happens.

Adding or editing an intrusion zone

This procedure documents how to add or edit an intrusion zone in a remote host controller. This is the first step in setting up a building's intrusion zone.

Prerequisites:
You are connected to the remote host controller station.

Step 1. Click **Controller Setup** > **Intrusion Setup** > **Intrusion Zones.**
The Intrusion Zones view opens.



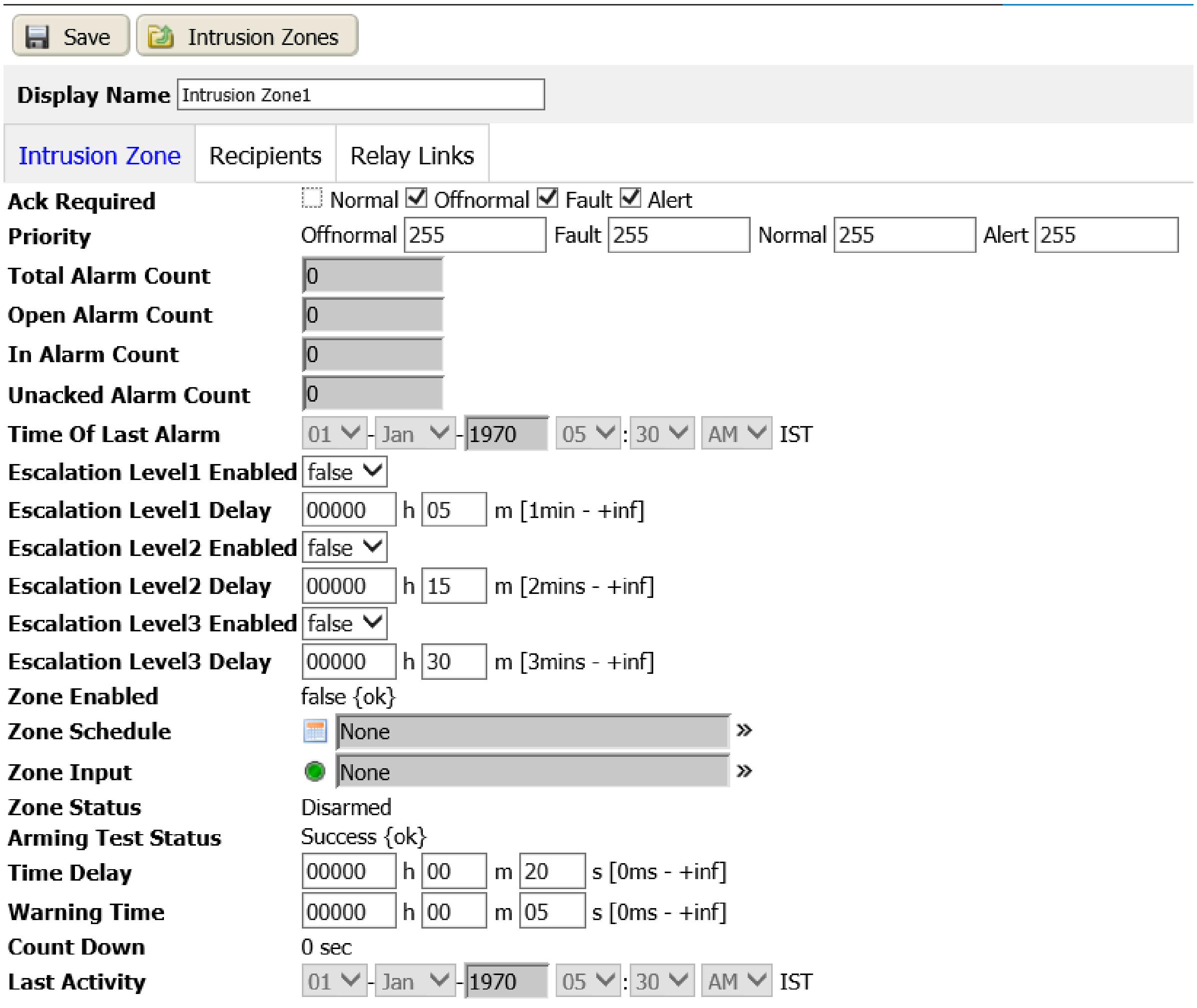
Display Name	Zone Status	Time Delay	Warning Time	To Display Path String
Intrusion Zone	Disarmed	20secs	5secs	/Services/AlarmService/Intrusion Zone
Lobby	Disarmed	20secs	5secs	/Services/AlarmService/Lobby
Main Office	Disarmed	20secs	5secs	/Services/AlarmService/Main Office

Step 2. Do one of the following:

- To add an intrusion zone, click the Add button (

).
- To edit an existing zone, double-click the zone in the table or select the zone, click the Hyperlink button (

), and click the Intrusion Zone tab.
The Add New Intrusion Zone or edit view opens.



Display Name Intrusion Zone1

Ack Required	□ Normal ☑ Offnormal ☑ Fault ☑ Alert
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	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

Step 3. Create or edit the **Display Name** for the zone.

Step 4. Use the Ref Chooser to select the custom schedule you created in the **Zone Schedule** property.
You may use a schedule to automatically arm a system as the only arming/disarming method or in conjunction with a keypad. (The last one to arm or disarm wins.)

Step 5. Define a **Time Delay** and **Warning Time**.
The time delay allows personnel to exit the zone after arming, as well as an alarm delay for disabling the zone when entering it.

You configure these times in the Supervisor intrusion zone. The system pushes them down to remote host controller intrusion zone in just a few seconds…no replication necessary.

Step 6. Enable one escalation level in the Supervisor intrusion zone.
Intrusion zones can employ up to three levels of alarm escalation. Use this feature to notify up to three people if alarms go unacknowledged. You may also use this feature to give an operator a chance to acknowledge and clear an alarm before notifying an off-site monitoring company.

Step 7. Define other properties and click the **Save** button at the top of the view.

The system creates or updates the intrusion zone record in the database of the local station. The *Niagara Enterprise Security Reference* document explains each intrusion zone property.

Intrusion points

The points you can assign to intrusion zones relate to reader and door modules.

Point	Description
Base Reader Module.Di2, Di3	These are digital inputs that are mapped to different doors, which give the access based on the badge validity.
Base Reader Module.Door 1.Exit Request	If the door has an exit request device, This field allows you to designate the supervised input that is used for the request to exit sensor.
Base Reader Module.Door 1.Sensor	If the door has a sensor device, use an option list to designate the supervised input that is used for the door sensor. Sensor is mainly used to specify door is Locked or Unlocked.
IntrusionTimeoutExt	An alarm event that occurs if the intrusion zone is armed and the door sensor changes to true after access is granted and the intrusion zone is not disarmed before the countdown expires. The extension must be edited as an Entry Point. If the zone is disarmed before the countdown expires, the countdown ends and the alarm is inhibited. This allows for annunciation that the zone is armed.

Adding points to an intrusion zone

Any point to be monitored as part of an intrusion zone must be added to the intrusion zone.

Prerequisites:
The intrusion zone record in the local station exists. You are using the web UI connected to the remote host station.

Step 1. Navigate to **Controller Setup** > **Intrusion Setup** > **Intrusion Zones.**
The Intrusion Zone view opens.

Step 2. Double-click the zone to which you are adding the point.
The edit view for the zone opens.

Step 3. Click the Points tab and click the Assign Mode button (▭).
The Unassigned pane opens with the list of available points.

Step 4. Select one or more points to assign and click the Assign button (⊕).
The assigned points move to the Newly Assigned pane.

Step 5. To delay the alarm on a point when the system arms, select the point, and click the Edit Entry Point button (🚦).

Step 6. To cause the alarm on a point to be always enabled regardless of the arm/disarm state, select the point and click the Edit Always Armed button (🚦).

Step 7. Extend the zone to include readers, other points, or relays that are under the station.

Step 8. To complete adding points to the intrusion zone, click **Save**.

Assigning the Supervisor station

To identify the Supervisor station to which the remote host controller belongs involves creating a group. In addition to extending the intrusion zone physically, expanding the zone by adding stations shares the arming status and zone enable status with all stations in the zone. You can view or control a zone's status (armed or disarmed) from a peer station or a Supervisor station if the stations are grouped.

Prerequisites:
You are using the web UI in the remote host station.

Step 1. From the main menu, click **Controller Setup** > **Intrusion Setup** > **Intrusion Zones**, and double-click an existing intrusion zone.
The Intrusion zone view opens. The name of the view reflects the name of the zone.

Step 2. Click the Grouping tab, and click the Assign Mode button (▤).
The Unassigned pane opens with a list of available stations.

Step 3. Select the Supervisor station to assign to the group and click the `Assign` button (⊕).
The system assigns the station to the intrusion zone group. The Supervisor station now lists the original intrusion zone in its own list of intrusion zones.

Step 4. Connect to the Supervisor station you just added.

Step 5. To view its intrusion zone properties, from the main menu click **System Setup** > **Intrusion Setup** > **Intrusion Zones**, and double-click on the existing intrusion zone.
The Intrusion Zones view opens.

Step 6. Double-click the intrusion zone.
The remote host’s intrusion zone status shows correctly in the Supervisor station’s intrusion zone. Assigning a Supervisor station causes the zone status to show correctly and updates to occur without replication.

Do not use the Reader tab on a Supervisor station.

Deleting an intrusion zone from a station

When you delete an intrusion zone from one station, which is grouped with other stations that have two-way communication, the system deletes the intrusion zone from all grouped stations. If you remove the station from the group first, and then delete the intrusion zone, the system only deletes the zone from the local station. In this case, to delete the intrusion zone from the other stations in the group requires a separate manual process on each station.

Step 1. Navigate to **Intrusion Setup** > **Intrusion Zones.**

Step 2. Select the intrusion zone and click the Delete button (⊖).

Removing a station from an intrusion zone

To un-group a station, you remove its assignment to the group.

Step 1. Navigate to **Intrusion Setup** > **Intrusion Zones**, and double-click the zone that contains the station to remove.
The edit view for the intrusion zone opens.

Step 2. Click the Grouping tab.
The list of stations with assignments to the group opens.

Step 3. Select the station with the group assignment to remove and click the Unassign button (⊖).
The system removes the station from the group.

Routing intrusion zone alarms to the Supervisor

This procedure configures the system to send intrusion zones alarms to the Supervisor station.

Prerequisites:
You have created the intrusion zone in the controller station.

Step 1. In the controller station, click **Controller Setup** > **Intrusion Setup** > **Intrusion Zones**, double-click the zone, click the Points tab, and click the Assign Mode button (▤).
The Unassigned pane lists the available points.

Step 2. Add the points in the controller station for the intrusion zone.

Step 3. Click the Grouping tab and click the Assign Mode button (▤).
The Unassigned pane lists the available Supervisor stations.

Step 4. Select the Supervisor station in the Unassigned pane, click the Assign button (⊕), and click

Save.

Step 5. Click the Recipients tab and click the Assign Mode button ( ).
The Unassigned pane lists the available alarm recipients.

Step 6. Select the Supervisor as the alarm recipient, click the Assign button ( ), and click **Save**.

Step 7. Connect to the Supervisor station, click **System Setup** > **Remote Devices** > **Station Manager**, and click the Replicate button.
You can now view the intrusion zone in the Supervisor as well as the remote controller station.

Step 8. In the Supervisor station, click **System Setup** > **Intrusion Setup** > **Intrusion Zones**, click the Add button ( ), click the Recipients tab, and click the Assign Mode button ( ).
The Unassigned pane opens with the list of available alarm recipients.

Step 9. Select the Console Recipient or other applicable recipient, click the Assign button ( ), and click **Save**.

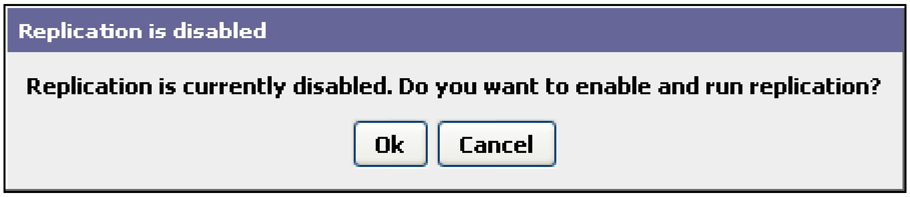
Replicating the intrusion zone from the Supervisor

This procedure ensures that the intrusion zone is viewable at the Supervisor station as well as in the remote host controller station.

Prerequisites:
Using the web UI, you are connected to the Supervisor station.

Step 1. From the main menu click **System Setup** > **Remote Devices** > **Station Manager**.
The Station Manager view opens.

Step 2. Click the Join button ( ).
After configuring all record types, the **Commit** button is available for completing the join process. If Replication is disabled, a window prompts you to enable and run replication.



Replication is disabled

Replication is currently disabled. Do you want to enable and run replication?

Step 3. To enable replication, click the **OK**.

Step 4. To start the replication job, click Replicate ( ).
Once the replication job starts, a progress bar marks job progress until the replication job completes successfully or fails, as indicated by the final job status window.

Setting up intrusion alarms in the Supervisor station

This procedure configures the console recipient for intrusion alarms.

Prerequisites:
Using the web UI, you are connected to the Supervisor station.

Step 1. From the main menu, click **System Setup** > **Intrusion Setup** > **Intrusion Zones**, double-click the intrusion zone name in the table, and click the Recipients tab.

Step 2. To display the available alarm classes, click the Assign Mode button ( ).

Step 3. Select the recipient.

Step 4. Select the recipient in the Unassigned pane and click the Assign button (⊕).

Step 5. To assign the recipient, click **Save**.

Configuring intrusion zone alarms to appear on the Supervisor

This procedure explains how to configure an intrusion zone in a remote host controller so that intrusion alarms appear in the Supervisor's alarm console.

Prerequisites:
The remote host controller is installed, you are connected to its station, the intrusion zone already exists.

Step 1. To assign the relevant Supervisor from the main menu, click **Controller Setup** > **Intrusion Setup** > **Intrusion Zones**, double-click an existing intrusion zone, click the Grouping tab, click Assign Mode (▤), select the Unassigned Supervisor station, and click Assign (⊕).

Step 2. To route intrusion zone alarms to the Supervisor, click the Recipients tab, click Assign Mode (▤), select an unassigned Supervisor recipient, and click Assign (⊕).

Step 3. Click **Save**.

Step 4. Replicate from the Supervisor.
The Supervisor station can view alarms from the remote intrusion zone.

Step 5. In Supervisor, click **System Setup** > **Intrusion Zone**, double-click the intrusion zone in the table, click the Recipients tab, and assign the console recipient or other applicable recipient.

Setting up a schedule to arm and disarm an intrusion zone

A optional schedule associated with an intrusion zone can arm and disarm an intrusion zone automatically.

Prerequisites:
For a company-wide configuration, you are using the web UI in the Supervisor station. Otherwise, you are using the web UI in the controller station.

Step 1. To begin, click **Controller (System) Setup** > **Schedules**.
The Schedules view opens.

Step 2. To create a new schedule, click the Add button (⊕).
The **Add a new Schedule** window opens.

Step 3. Choose `Custom`, and click **Ok**.
The **Choose a Usage...** window opens.

Step 4. Click the chevron to the right of **`Usage`**, select `Intrusion`, and click the Assign button (⊕), and click **Ok**.
The Schedule view opens.

Step 5. Name the schedule, for example, Intrusion zone.

Step 6. Configure the **`Default output`** so that `true` = Armed, and `false` = Disarmed.

Step 7. On the Scheduler tab, set up the schedule so that the zone is disarmed during weekdays.

Step 8. To save your changes, click **Save**.

Step 9. Export the schedule from the Supervisor to the remote host controller station.

Step10. Assign the schedule to the intrusion zones in the Supervisor and the remote host controller.

Assigning the schedule to the intrusion zone

For a company-wide system you assign the schedule to the intrusion zone in both the Supervisor and the remote host controller.

Prerequisites:
You are working in the Supervisor station, followed by working in the remote controller station. The intrusion zone already exists.

Step 1. To begin in the Supervisor station, click **System Setup** > **Intrusion Setup** > **Intrusion Zones**.

Step 2. To select the intrusion zone, double-click a zone and click the Intrusion Zone tab.

Step 3. Click the chevron next to the **`Zone Schedule`** property, select the schedule you created from the **Ref Chooser**, and click **OK**.
The name of the schedule appears in the **`Zone Schedule`** property.

Result
When the schedule transitions to `true`, the system arms the zone and performs any associated actions.

Setting up an intrusion PIN

You may use a PIN (Personal Identity Number) to arm and disarm an intrusion zone. An associated schedule may determine when the PIN is valid.

Prerequisites:
Using the web UI, you are connected to the Supervisor station.

For a standalone configuration, you create an intrusion PIN in your controller station. For a company-wide configuration, you should set up intrusion PINs in the Supervisor station.

Step 1. Click **System Setup** > **Intrusion Setup** > **Intrusion PINs**.

Step 2. To add a PIN, click Add (⊕).

Step 3. Enter a name for the PIN.
This name might identify the intrusion zone.

Step 4. Enter the schedule and, if applicable, the tenant.

Step 5. Finally, enter the PIN, and click **Save**.

Step 6. If you need multiple PINs, repeat these steps for each PIN.

Step 7. To complete the configuration, click **Save**.

Assigning a PIN to an intrusion zone

You create an intrusion zone PIN in the Supervisor station and assign it in the controller station.

Prerequisites:
You are using the web UI in the Supervisor station. The PIN and intrusion zone exist.

Step 1. To begin, click **System Setup** > **Intrusion Setup** > **Intrusion Zones**, doublt-click an intrusion zone, and click the Intrusion Pins tab.
The **`Intrusion Pins`** tab opens.

Step 2. To view the available PINs, click the Assign Mode button (▣).

Step 3. Select an unassigned PIN and click the Assign button (⊕).

Step 4. Assign the Display/Keypad to the remote host controller’s intrusion zone.

Push button for arming and disarming

You may arm and disarm an intrusion zone with a hardware input, such as a **push** button.

The push button input device should be momentary rather than latching. The system toggles the zone status every time it activates the associated input. The system initiates the arm-with-delay function when you activate the button and disarms the zone. If the zone is not secured, it will not arm. There is no feedback to the user with this method unless you install additional hardware.

Niagara Touch display

The mobile Niagara Touch display locks down the browser to a specific URL and serves as an intrusion zone arming and disarming keypad. Client certificate authentication automatically logs in the display to a controller station. This section sets up a Niagara Touch display with a client certificate and connects it to a controller station. The display runs the Android operating system.

Standard tools and certificate authentication support the display. You will need a separate display, certificate, display user and nav file for each zone. To save Time, Niagara 4.10 includes a sample Px view with an onscreen keypad, default user and role in a restore distribution file. The Px file is also available in the Px folder of the Supervisor station.

NOTE: Assigning a user certificate requires the **FoxService** and **WebService** to restart. To avoid disrupting daily operations, configure a new Niagara Touch display after hours.

Files

Configuring the Niagara Touch display involves several files. As a best practice, take time to identify where you will save these files so that you can easily find them when you need them.

You can name your files differently from the names used in this table. These names are used as examples in these configuration procedures.

File	Where stored	Comments
Certificate .pem file	User home: `C:/Users/<User Name>/<Software version>/tridium/certManagement`	This file will reside in the User Key Store of the remote controller station. The remote controller is the client in this client-server relationship.
Certificate .pem file with key and .p12 file	`C:\certs`	This path should be short because you enter it when using OpenSSL to convert a .pem certificate file to a .p12 file. This certificate is destined for the display, which is the server in this client-server relationship.
Px page	**Station** > **Files** in the controller station	This page provides a sample intrusion keypad to appear on the display. Before you use the File Copier utility to copy this file to the controller station's Files folder, put it on your PC in a location that is easy to find.
Nav file	**Station** > **Files** in the controller station	This file tells the display to open the onscreen keypad when someone logs in.

Prerequisites

To install and configure the Niagara Touch display your configuration needs these prerequisites.

- Up to a 4GB USB thumb drive
- Up to an 8GB MicroSD card

These components must not exceed these sizes.

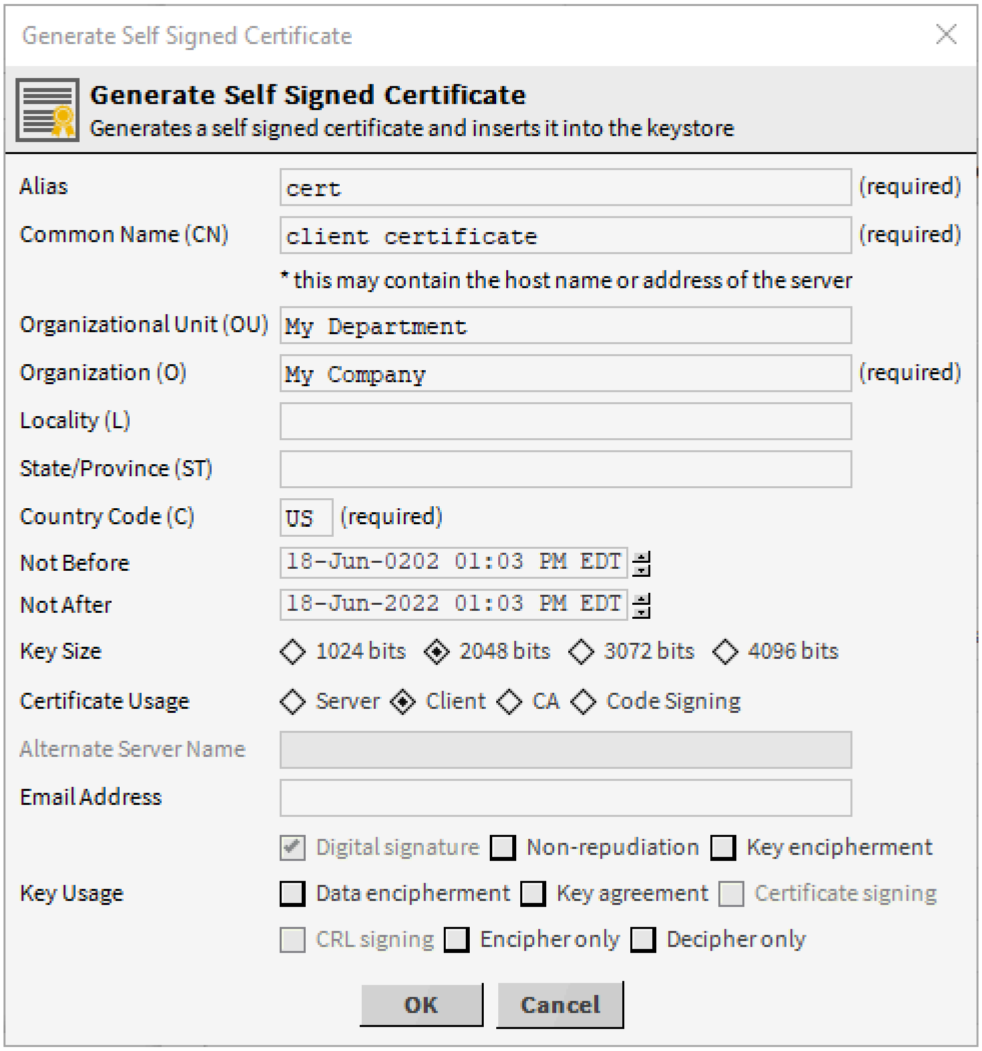
Certificate and authentication setup

Creating and exporting the client certificate

A certificate authenticates the display to the station that manages the device. You need a separate certificate for each display.

Prerequisites:
You are working in Workbench connected to the station that manages the display device.

Step 1. To create a client certificate, expand**Config** > **Services** > **PlatformServices**, double-click **CertManagerService** and click **New**.
The **Generate Self Signed Certificate** window opens.



Generate Self Signed Certificate

Generate Self Signed Certificate
Generates a self signed certificate and inserts it into the keystore

Alias	cert	(required)
Common Name (CN)	client certificate	(required)
	* this may contain the host name or address of the server	
Organizational Unit (OU)	My Department	
Organization (O)	My Company	(required)
Locality (L)		
State/Province (ST)		
Country Code (C)	US (required)	
Not Before	18-Jun-0202 01:03 PM EDT	
Not After	18-Jun-2022 01:03 PM EDT	
Key Size	○ 1024 bits ● 2048 bits ○ 3072 bits ○ 4096 bits	
Certificate Usage	○ Server ● Client ○ CA ○ Code Signing	
Alternate Server Name		
Email Address		
Key Usage	☑ Digital signature □ Non-repudiation □ Key encipherment □ Data encipherment □ Key agreement □ Certificate signing □ CRL signing □ Encipher only □ Decipher only	

Step 2. Enter values for at least these required properties:

- **Alias** provides the certificate name. Enter it as “cert.” This is a required name.
- **Common Name** should match the display user you will set up with certificate authentication.
- **Organization** is your company.
- **Country Code** is the two-character ISO CODE you can find at `countrycode.org`.

Step 3. Select `Client` for **Certificate Usage** and click **OK**.

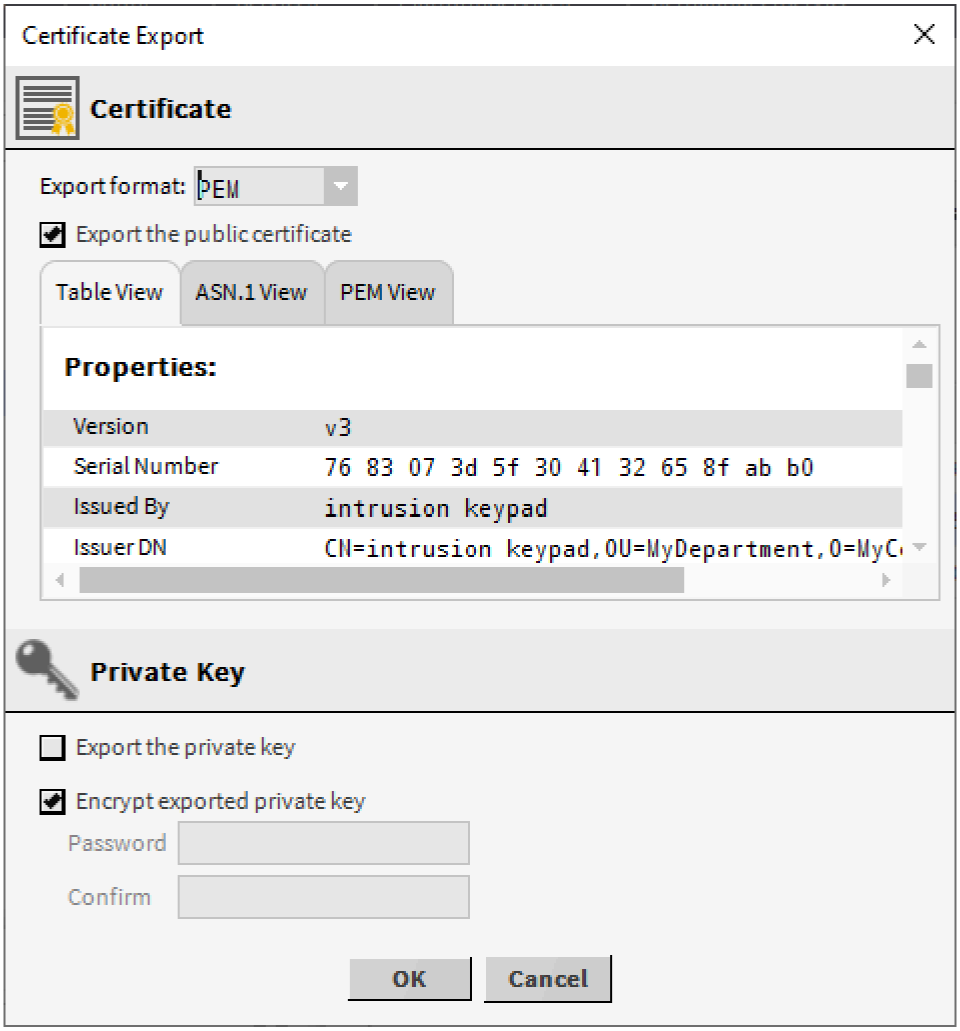
The certificate appears in the User Key Store.

The next step exports the certificate so that you can associate it with the display user you just created.

Step 4. To export the certificate, select it in the User Key Store and click **Export**.
The certificate file is located here: `C:\Users\<<your user>>\<<Niagara Version>>\tridium\certManagement` where:

- `<<your user>>` is your user name
- `<<Niagara Version>>` is the folder that contains the Niagara software

The **Certificate Export** window opens.



Export format: PEM

☑ Export the public certificate

Properties:

Version	v3
Serial Number	76 83 07 3d 5f 30 41 32 65 8f ab b0
Issued By	intrusion keypad
Issuer DN	CN=intrusion keypad,OU=MyDepartment,O=MyC

☐ Export the private key

☑ Encrypt exported private key

Password

Confirm

Do not export this certificate with its private key.

Step 5. To continue, click **OK**, store the certificate's `.pem` file where you can find it later and click **OK** again to close the **Certificate Export** window.

Next steps

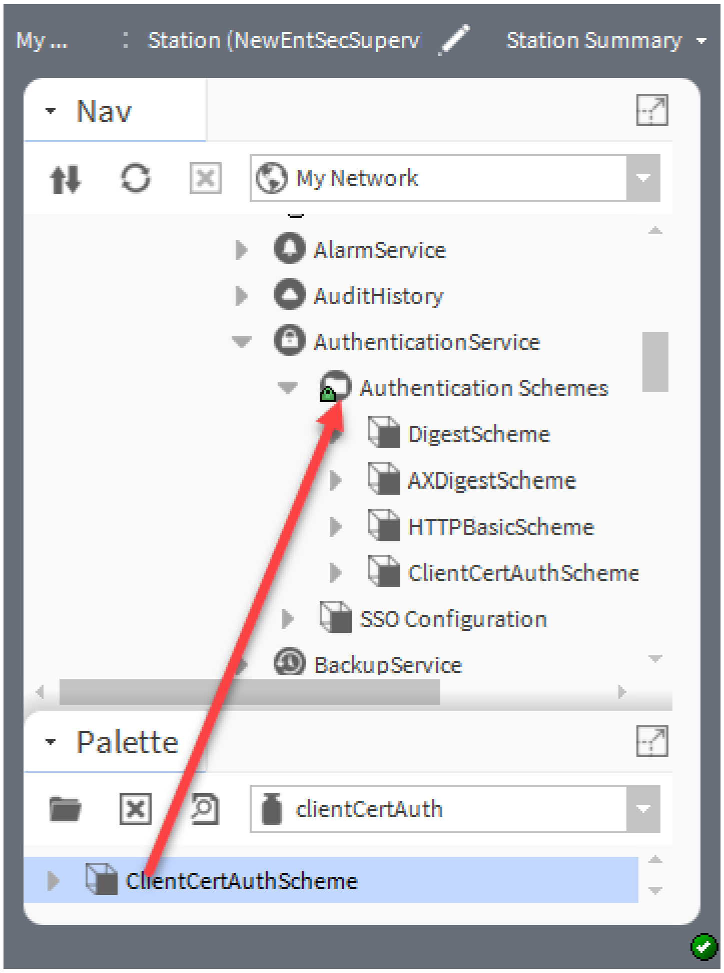
The next step sets up single sign-on in the **AuthenticationService**.

Setting up authentication

Client authentication verifies that a keypad user is authorized to connect to the security system. This user is not a person, rather it represents the Niagara Touch display.

Prerequisites:
You are working in Workbench connected to the station that manages the display device. The station has an AuthenticationService in the Services folder.

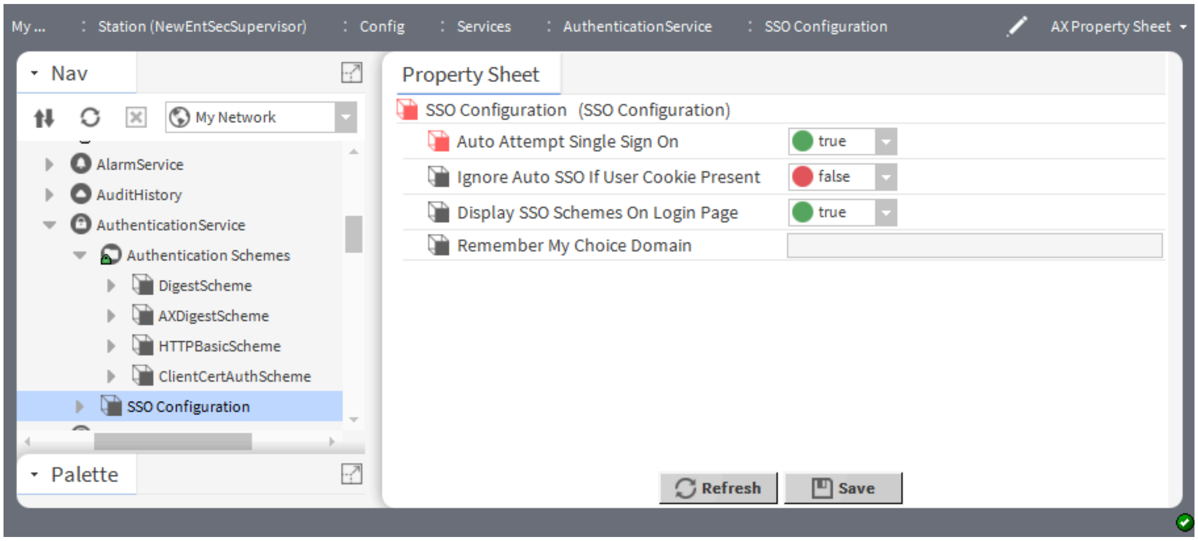
Step 1. Expand **Config** > **Services** > **AuthenticationService** > **AuthenticationSchemes**.
By default, this station comes with one **ClientCertAuthScheme**.



Step 2. If you need a second scheme, open the clientCertAuth palette and drag the **ClientCertAuthScheme** component from the palette to the **Authentication Schemes** node under the **AuthenticationService**.

Step 3. Double-click **SSO Configuration** (this component is at the same level as **Authentication Schemes** under the **AuthenticationService**).

The SSO Configuration **AX Property Sheet** opens.



SSO Configuration (SSO Configuration)

Auto Attempt Single Sign On	● true
Ignore Auto SSO If User Cookie Present	● false
Display SSO Schemes On Login Page	● true
Remember My Choice Domain	

Step 4. Set **`Auto Attempt Single Sign-On`** to `true`, confirm that **`Ignore Auto SSO if User Cookie Present`** is set to `false` and click **Save**.

Next steps

The next step associates the exported certificate with the display user.

Setting up a display user

This system user represents the Niagara Touch display, which is authorized to connect to the station and should be configured with the most restrictive role and permissions possible. This procedure creates this user and assigns the authentication certificate you created to this user. You will need a separate user for each display.

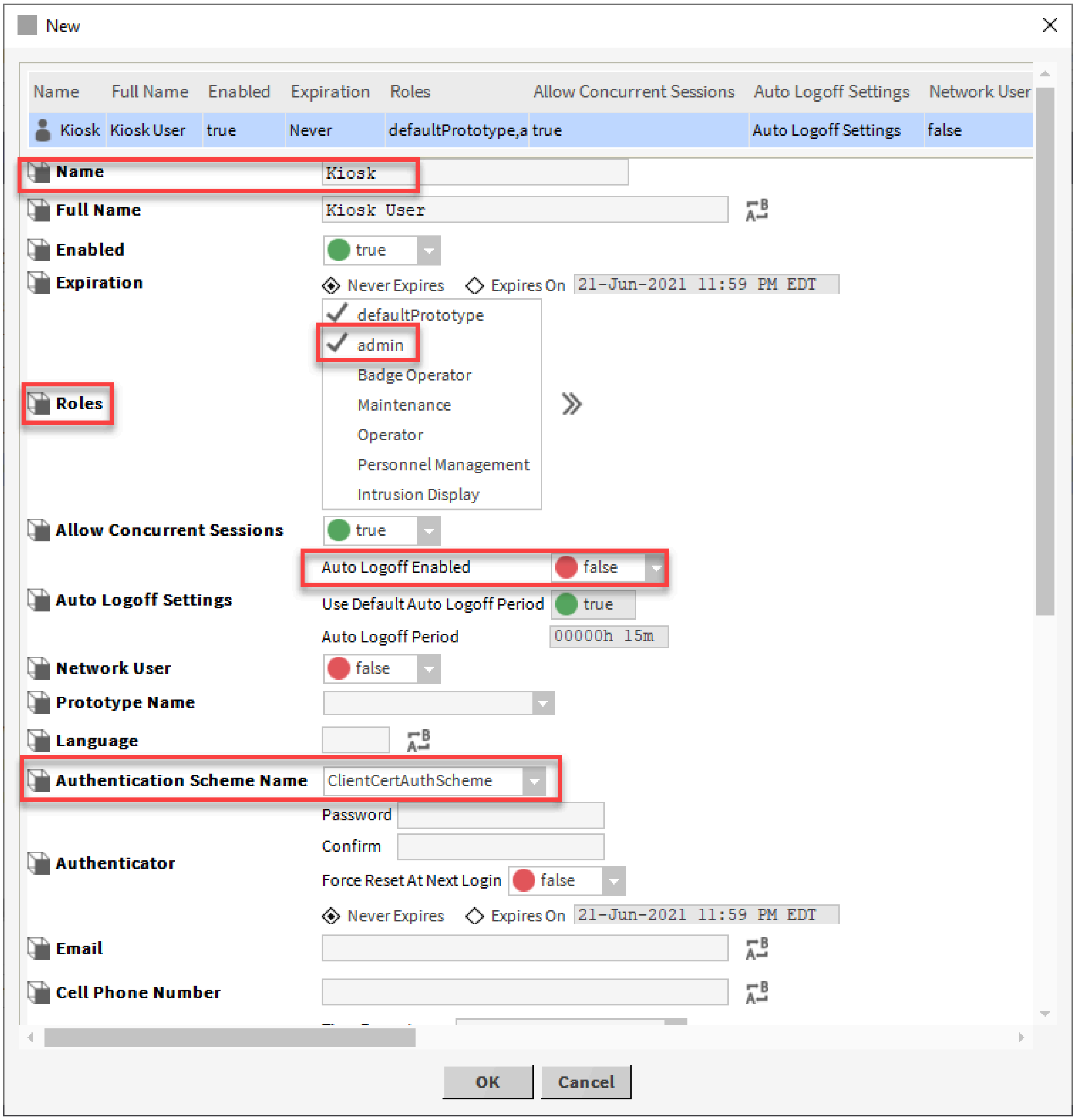
Prerequisites:

You are working in Workbench connected to the station that manages the intrusion zones.

Step 1. Expand **Config** > **Services** and double-click the **UserService**.
The **User Manager** opens.

Step 2. To create the user for the client certificate you created, click **New**, select the number of users to create and click **OK**.

The **New** view opens.



New

Name	Full Name	Enabled	Expiration	Roles	Allow Concurrent Sessions	Auto Logoff Settings	Network User
Kiosk	Kiosk User	true	Never	defaultPrototype,a	true	Auto Logoff Settings	false

Name Kiosk

Full Name Kiosk User

Enabled ● true

Expiration ◆ Never Expires ◇ Expires On 21-Jun-2021 11:59 PM EDT

Roles
- ✓ defaultPrototype
- ✓ admin
- Badge Operator
- Maintenance
- Operator
- Personnel Management
- Intrusion Display

Allow Concurrent Sessions ● true

Auto Logoff Settings
- Auto Logoff Enabled ● false
- Use Default Auto Logoff Period ● true
- Auto Logoff Period 00000h 15m

Network User ● false

Prototype Name

Language

Authentication Scheme Name ClientCertAuthScheme

Authenticator
- Password
- Confirm
- Force Reset At Next Login ● false
- ◆ Never Expires ◇ Expires On 21-Jun-2021 11:59 PM EDT

Email

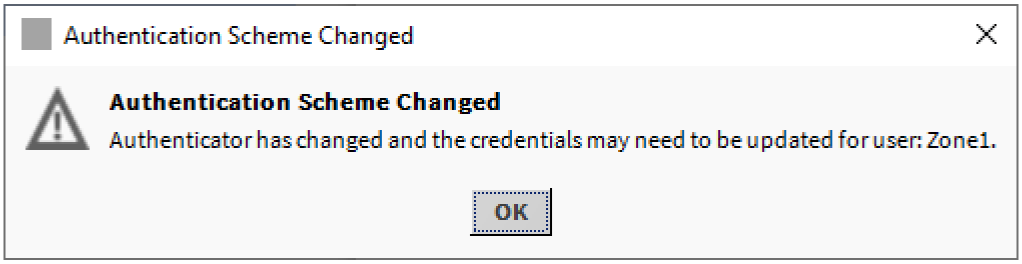
Cell Phone Number

Step 3. Enter values for at least these properties:

- **Name** can be the **Common Name** you used for the certificate.
- **Roles**, for now assign the admin role. You will change this later to the most restrictive role.
- Under **Auto Logoff Settings**, remove the check mark to select false for **Auto Logoff Enabled**.
- **Authentication Scheme**, set to ClientCertAuthScheme.

Step 4. To accept the changes and save the user, click **OK**.

The software alerts you that the credentials for the user need to be updated.



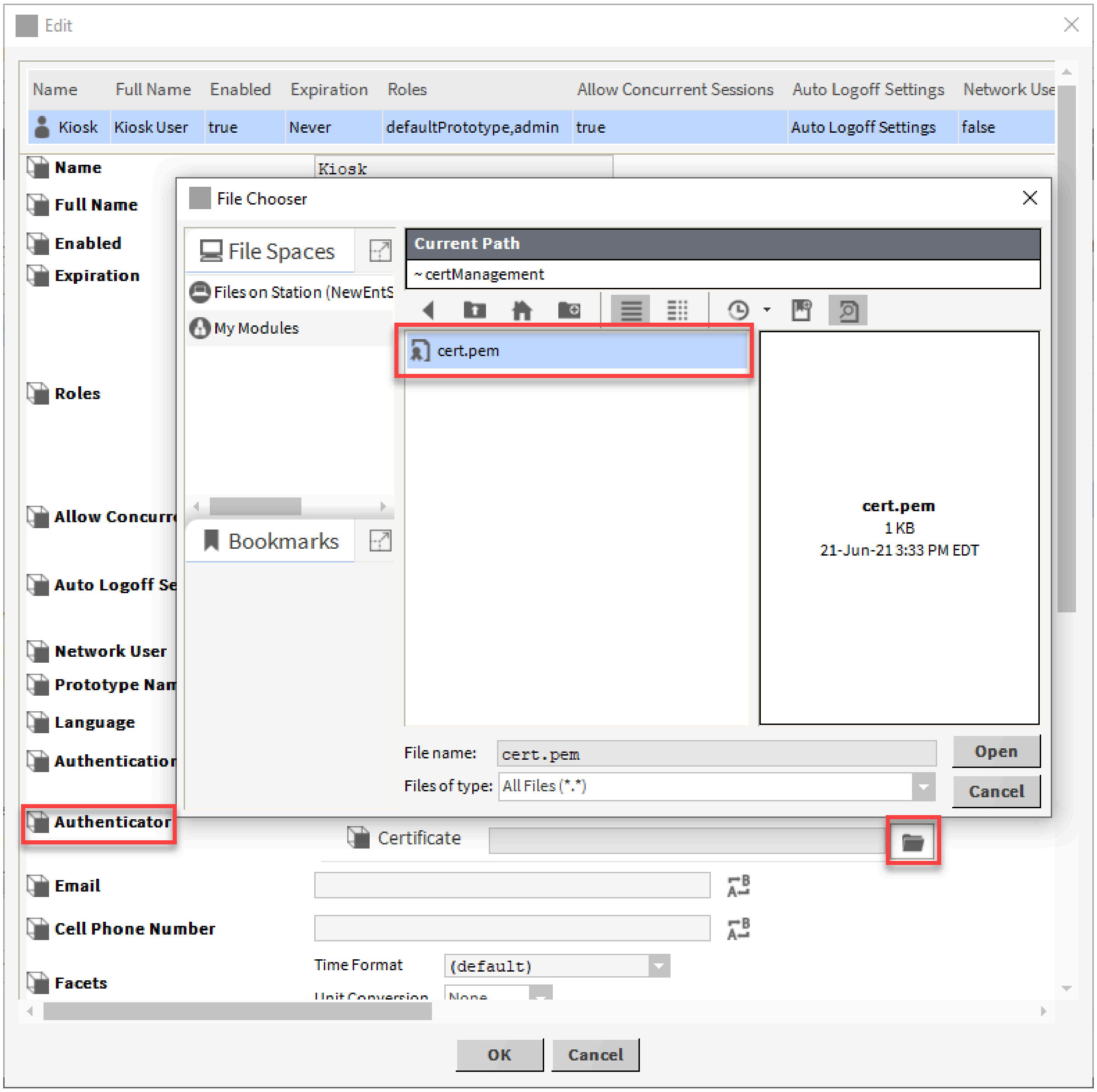
Authentication Scheme Changed

Authenticator has changed and the credentials may need to be updated for user: Zone1.

Step 5. To assign the certificate to this user, open the user again by double-clicking **UserService**, select the user you just created and click **Edit**.
The **Edit** window opens.

Step 6. Scroll down to **Authenticator** and under **Certificate**, click **Choose File**.

A **File Chooser** window opens.



Name	Full Name	Enabled	Expiration	Roles	Allow Concurrent Sessions	Auto Logoff Settings	Network Use
Kiosk	Kiosk User	true	Never	defaultPrototype,admin	true	Auto Logoff Settings	false

Name Kiosk

Current Path
~ certManagement

cert.pem
1 KB
21-Jun-21 3:33 PM EDT

File name: cert.pem

Files of type: All Files (*.*)

Time Format (default)

Unit Conversion None

Step 7. Navigate to the client certificate you created and, to assign the certificate to this user, select the certificate and click **Open**.
If you used the default location, double-click **User HomeCertManagement**.
The system advises you that the **FoxService** and **WebService** need to restart.

Step 8. To save the change you just made, click **OK**.

Next steps

Next, for Niagara 4.9 and earlier, you export the same certificate, but this time with its private key. Then, for all versions you add the certificate to the server socket’s TrustAnchor list. You will return to this user to configure more properties later.

Exporting the certificate with its private key (Niagara 4.9)

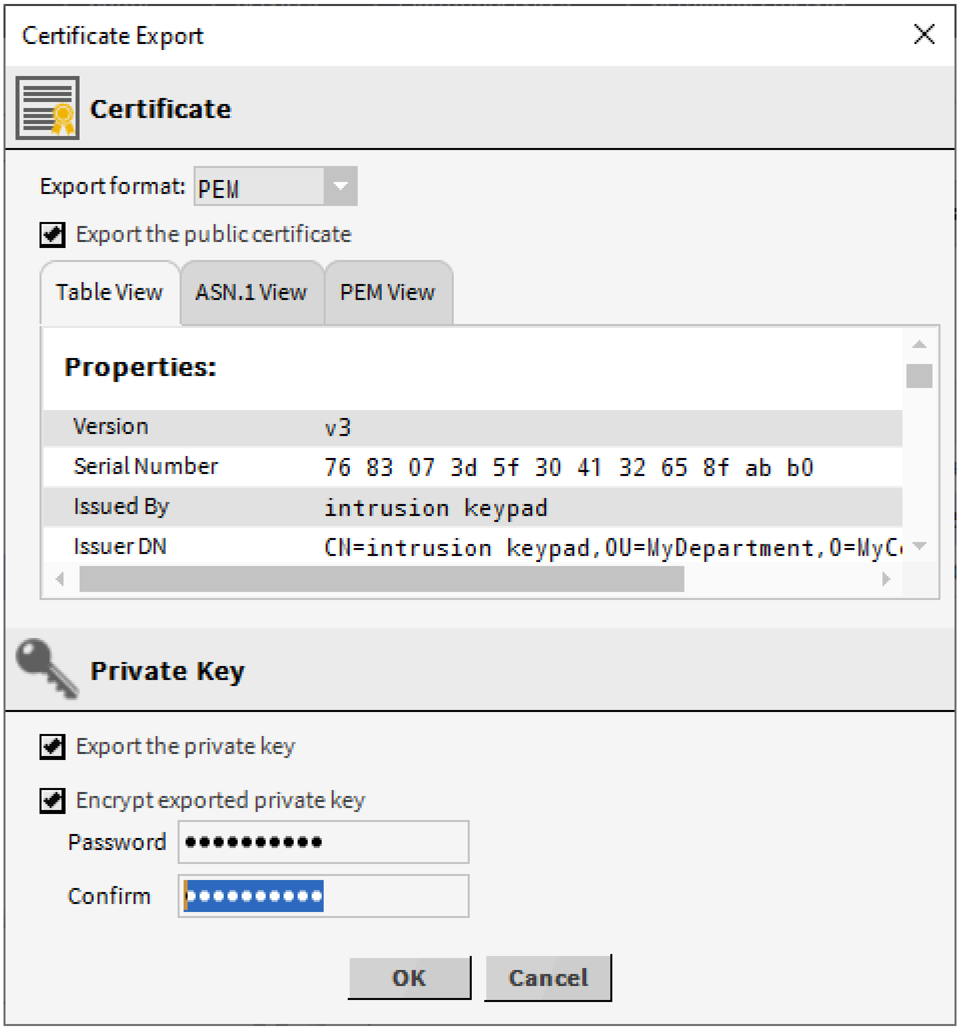
If you are using Niagara 4.9 you may export the display certificate with its private key. This provides the most robust security for data communication.

Prerequisites:
You are using Niagara 4.9 or earlier. You are working in Workbench running on a PC. You are connected to the station that manages the display device.

If you are using Niagara 4.10 or later you do not need to export the certificate with its private key. You can use the .pem file you exported to configure the **UserService**. OpenSSL does not support .pem files and private keys exported from Niagara 4.10.

NOTE: The private key of the server certificate validates the public key presented to the display by the client station. A server certificate without a private key is less secure than one with its private key. Without the encryption of the private key, a malicious user could install the certificate into devices that should not be allowed to make a connection. However, when a PIN is involved, as it is with arming and disarming an intrusion zone, the risk is low.

Step 1. To export the certificate with its private key, expand **Config** > **Services** > **PlatformServices**; double-click **CertManagerService**; in the **User Key Store**, select the certificate you created and click **Export**.
The **Certificate Export** window opens.



Export format: PEM

☑ Export the public certificate

Properties:

Version	v3
Serial Number	76 83 07 3d 5f 30 41 32 65 8f ab b0
Issued By	intrusion keypad
Issuer DN	CN=intrusion keypad,OU=MyDepartment,O=MyC

☑ Export the private key

☑ Encrypt exported private key

Password ●●●●●●●●●●●

Confirm ●●●●●●●●●●●

Step 2. Enable **`Export the private key`**, create and confirm a strong password to protect the key, record the password in a safe location and click **OK**.
A **File Chooser** window opens.

Step 3. Save the file in a location other than the location you used for the first save, for example, `C:\certs`.
Since you will use an OpenSSL command prompt to convert the .pem file to a .p12 file, a short path will make it easier to enter the commands.

Result
The next procedure downloads OpenSSL to create a .p12 certificate.

Preparing the .p12 server certificate

OpenSSL converts a .pem certificate file to a .p12 certificate file. The display recognizes this format.

Prerequisites:
You are working in Workbench running on a PC. You are connected to the station that manages the display device.

Step 1. Download the appropriate version of OpenSSL for Windows and install it.
Multiple sites provide pre-compiled executables. For example, you can download it from here: `https://slproweb.com/products/Win32OpenSSL.html`.

More information about OpenSSL is available here: `https://www.openssl.org/source/`

This YouTube video provides a tutorial for setting up OpenSSL: `https://www.youtube.com/watch?v=jSkQ27sTto0`

Step 2. Follow the instructions to install OpenSSL.

Step 3. Open an OpenSSL command prompt and change your directory to the folder that contains the certificate you exported, for example: `cd\certs`.

Step 4. To run the OpenSSL conversion from the command prompt, type this command and press **Enter**.

```
openssl pkcs12 -export -out cert.p12 -in <your cert> -inkey <your
cert>.pem
```

The output certificate name must be `cert.p12`.

OpenSSL prompts you to enter the pass phrase for the Niagara 4.9 (or earlier) certificate you exported with the private key.

Step 5. Do one of the following:

- For Niagara 4.9, enter the password you created when you exported the certificate with its private key.
- For Niagara 4.10, press **Enter**.

OpenSSL prompts you to create and confirm its password. Both certificates with and without an export private key require this .p12 password.

Step 6. Enter, verify and record this password in a safe place.
OpenSSL creates a new certificate with the .p12 extension and associated password.

Step 7. Confirm that the new certificate exists and move it to a secure location.
You do not want an unauthorized person to have access to this certificate.

Next steps
The next step is to install the .p12 certificate in the display.

Installing the .p12 certificate

The display requires the server certificate to make a secure connection to the station.

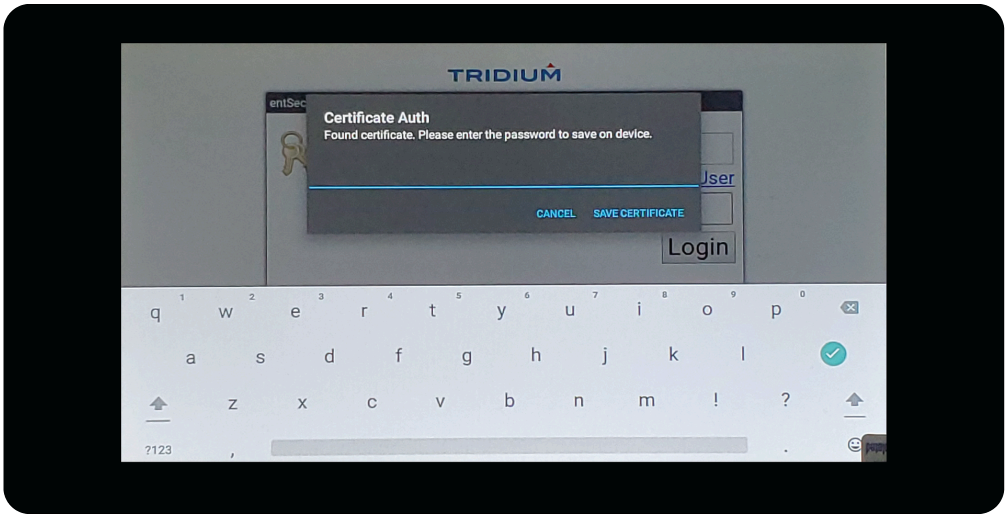
Prerequisites:
Your display is charged and ready to use. Your network router is within range so that the display can connect to it using WiFi.

Step 1. Save the .p12 certificate to a USB thumb drive or MicroSD card.
The USB adapter comes with the display unit.

Step 2. Use the adapter to connect the USB thumb drive to the display’s mini-USB connector or insert the MicroSD card.

Step 3. Turn on the display (the on/off button is the small button to the right of the mini–USB receptacle on one end of the display).
A start-up splash screen opens followed by a screen with this instruction: **TAP HERE FOR SETTINGS** as the device connects to your local area network.

Step 4. Tap **TAP HERE FOR SETTINGS.**



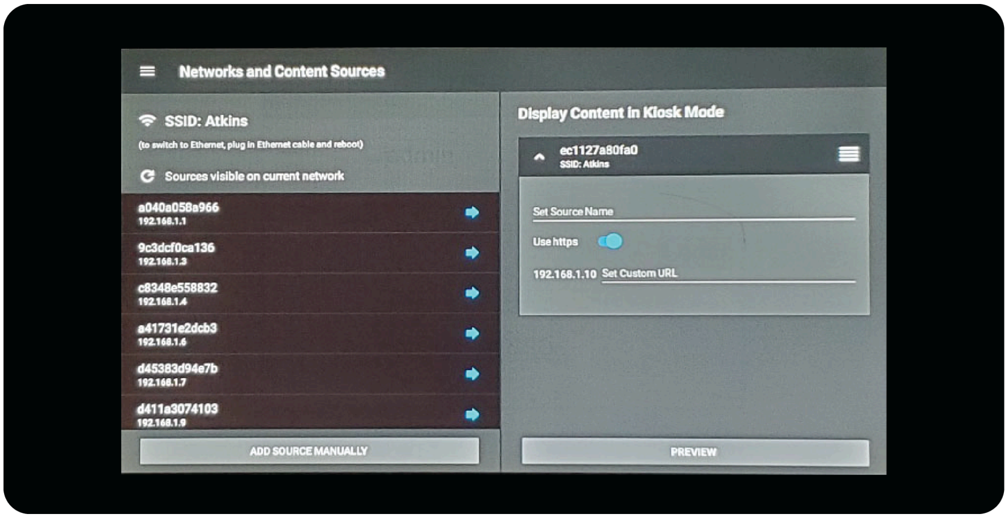
Certificate Auth
Found certificate. Please enter the password to save on device.

The display finds the certificate on the thumb drive or MicroSD card, imports it and opens the **Certificate Auth** window.

If, for any reason, you need to return to the first screen that reads, **TAP HERE FOR SETTINGS**, press the on/off button, and select `Restart`.

Step 5. Using the onscreen keypad, enter the password you created when you exported the certificate using OpenSSL and tap **SAVE CERTIFICATE.**

The **Networks and Content Sources** view opens.



SSID: Atkins
(to switch to Ethernet, plug in Ethernet cable and reboot)
Sources visible on current network

a040a058a966
192.168.1.1

9c3dcf0ca136
192.168.1.3

c8348e558832
192.168.1.4

a41731e2dcb3
192.168.1.6

d45383d94e7b
192.168.1.7

d411a3074103
192.168.1.9

Display Content in Kiosk Mode

ec1127a80fa0
SSID: Atkins

Set Source Name
Use https
192.168.1.10 Set Custom URL

On the left, under "Sources visible on current network" is the list of devices that are connected to your network.

Step 6. Using the IP address of the remote controller station, scroll down the list on the left, find the controller and tap the blue, right-pointing arrow.
The controller appears under the "Display Content in Kiosk Mode" list.

The display supports only one source at a time. If more than one source appears in the list on the right, swipe to the left over the source you do not need. This exposes a delete option (white X on a red square). Tap this X to delete the extra option.

Step 7. Expand the source by tapping the down arrow and tap to turn on **`Use https`**.
This enables secure communication between the display and controller station.

Step 8. To preview the connection, tap **PREVIEW**.

Step 9. Assuming the connection works as expected, tap **LAUNCH**.
The display connects to the controller station using certificate authentication.

Step10. In the browser, select `Log in with SSO` using the user you created in the station.
You do not need to input a password as the display recognizes the certificate you installed. The display automatically logs in using this user each time it reboots.

Configuration

Associating the display with its zone

The station that controls your intrusion zone(s) is the one to which your Niagara Touch display connects. This procedure uses the web UI.

Prerequisites:
You created your authentication certificate and have set up your display. You are working in the web UI and are connected to the station that manages your building's intrusion zones.

Step 1. If needed, set up one or more intrusion zones following the procedure earlier in this chapter.

Step 2. To add a display, navigate to **Controller Setup** menu, select **Intrusion Setup** > **Intrusion Displays** and click the Add button (⊕).
The Intrusion Display tab opens.

Step 3. Configure these properties:

Give the display a **`Display Name`**.

Change **`Smart Key Device`** to `none`.

Step 4. To add an intrusion PIN or PINs, select `true` for **`Arming Pin Required`**.

Step 5. To assign the intrusion zone to a display, click the Intrusion Zones tab, click the Assign Mode button (☑), select an unassigned zone and click the Assign button (⊕).

Step 6. To save these changes, click **Save**.
The system adds the display to the database, shows it the top of the view, and adds it as a component node under the **AlarmService**.

Step 7. Repeat these steps for each display.

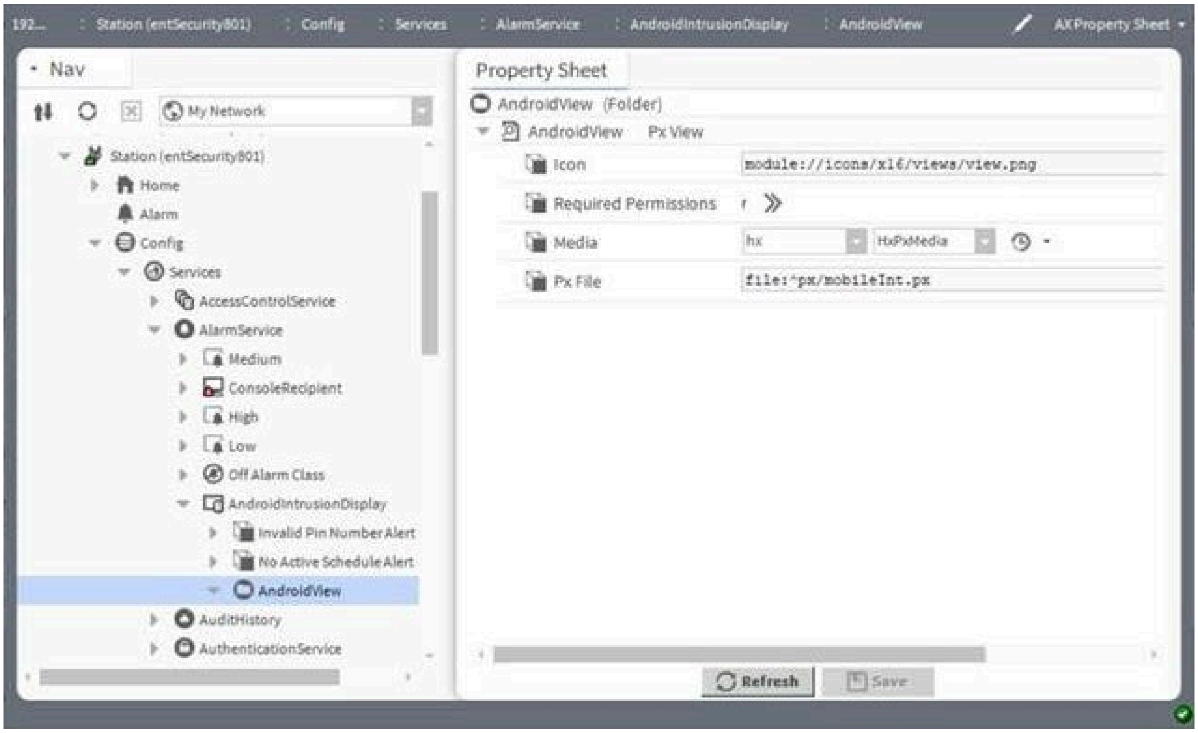
Next steps
The next step is to create the onscreen keypad.

Setting up the px view

You can create a Px view of an onscreen application and install it on the display.

Prerequisites:
You are working in Workbench connected to the station that controls the display.

Step 1. To configure properties, expand **Config** > **Services** > **AlarmService** and double-click **AndroidView.** The view’s **Property Sheet** opens.

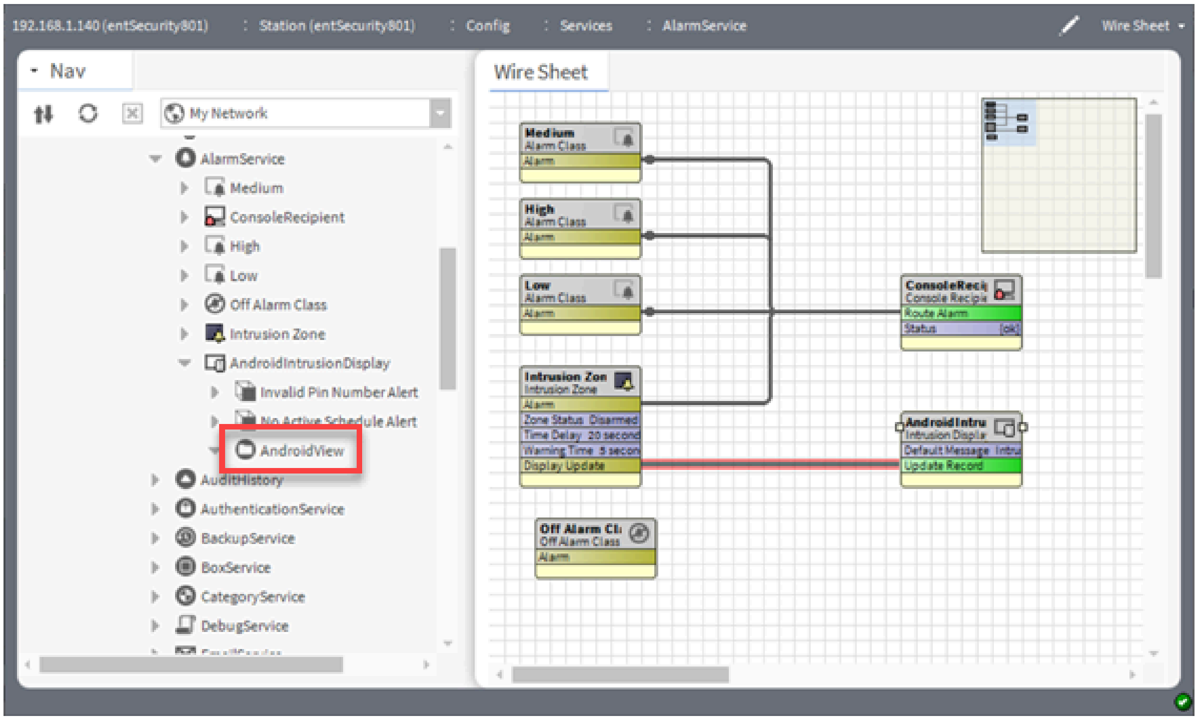


AndroidView (Folder)
AndroidView Px View
Icon `module://icons/x16/views/view.png`
Required Permissions r
Media hx HxPxMedia
Px File `file:^px/mobileInt.px`

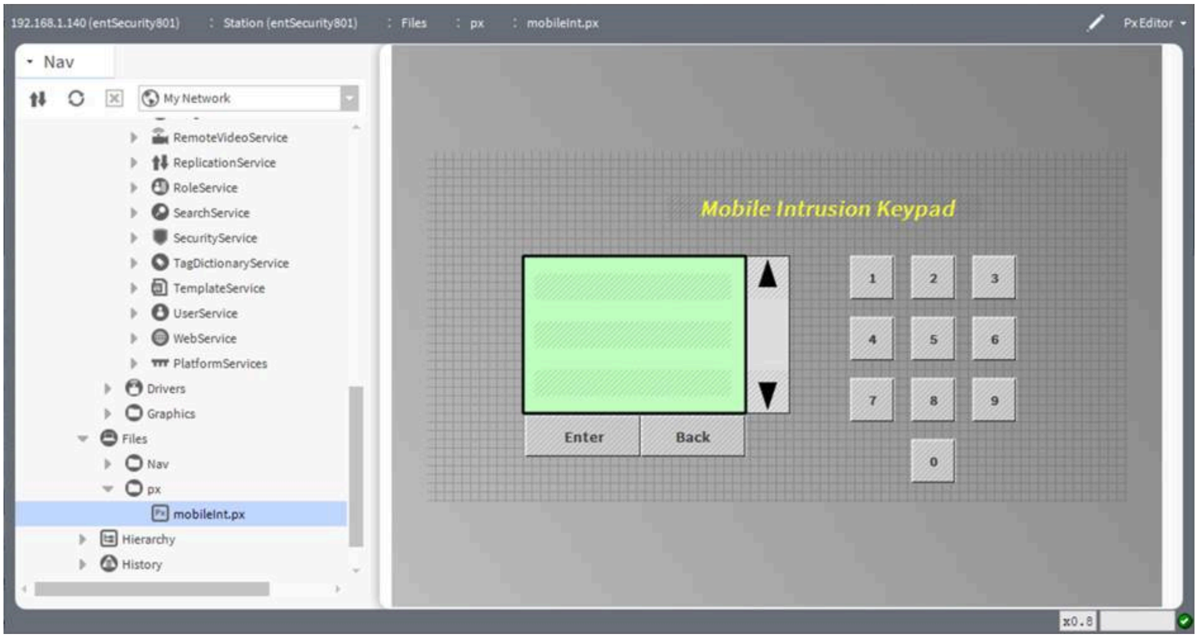
NOTE: This Px view uses relative ords.

Step 2. To customize data flow, right-click **AndroidView** and click **Views** > **Wire Sheet**.

The **Wire Sheet** view opens.



Step 3. To open the **Px Editor**, right-click **AndroidView** and click **Views** > **MobileInt**.
This displays the Px view.



Step 4. Test the arming and disarming function to make sure that the numeric keys function properly and that the station accepts your PIN.

Result
The next step is to set up a navigation file so that the keypad Px file opens on the display.

Setting up a navigation file

The onscreen Px view serves as the home page for the display user. When a person turns the display on, it defaults to this page. You need a separate .nav file for each display.

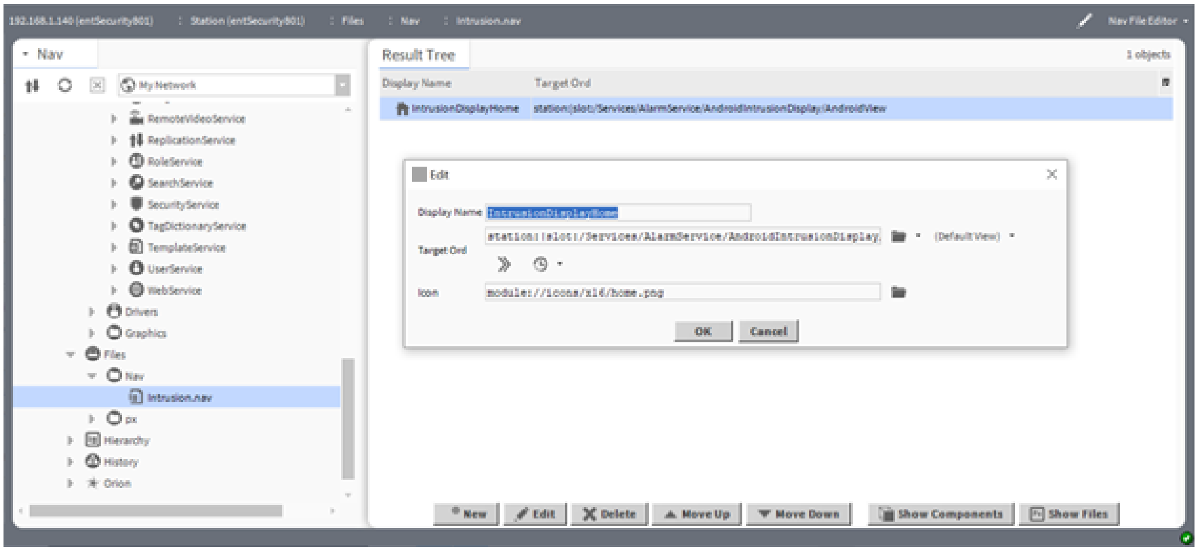
Prerequisites:
You are working in Workbench connected to the controller station.

Step 1. Create a folder under the station's **Files** node named **Nav**.
Nav files must reside under the **Files** node. They are not stored in the station database.

Step 2. To create a new .nav file, right-click the **Files** node and click **New** > **NewFile.nav**.
The **Name for New File** window opens.

Step 3. Give the .nav file a name, click **OK** and expand the **Files** node.

Step 4. To associate the .nav file with the onscreen display, double-click the file name, select the slot and click **Edit**.
The **Edit** window opens.



192.168.1.140 (entSecurity801) : Station (entSecurity801) : Files : Nav : Intrusion.nav

Display Name	Target Ord
IntrusionDisplayHome	station:|slot:/Services/AlarmService/AndroidIntrusionDisplay/AndroidView

Edit

Display Name: IntrusionDisplayHome

Target Ord: station:|slot:/Services/AlarmService/AndroidIntrusionDisplay (Default View)

Icon: module://icons/x16/home.png

Step 5. Click the folder icon and use the **File Ord Chooser** to select the location of the display folder.
In the example, this location is: `station:|slot:/Services/AlarmService/AndroidIntrusionDisplay/AndroidView`.

Result
The next procedure creates an display role.

Updating the role assigned to the display

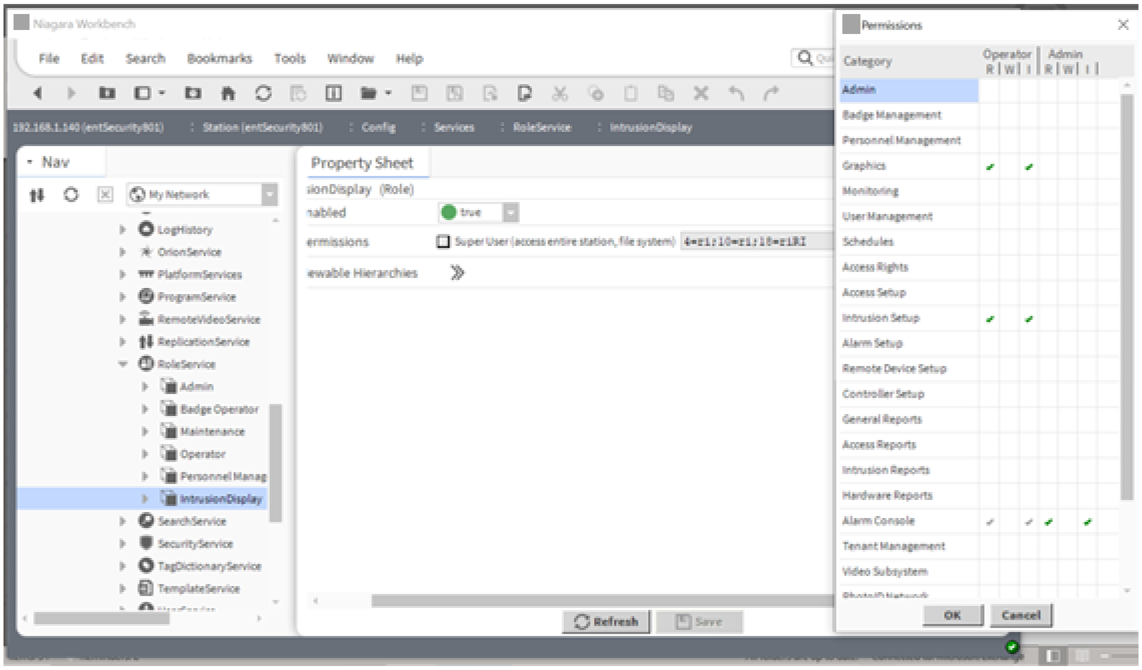
This special role limits the actions that a person can perform with the display to only arming and disarming an intrusion zone. Niagara 4.10 includes a default role for the display along with a Px view in its restore distribution file.

Prerequisites:
You are working in Workbench connected to the controller station that manages your building's intrusion zones.

Step 1. Expand **Config** > **Services** and double-click **RoleService**.
The **AX Role Manager** view opens.

Step 2. To edit the default role, select the role and click **Edit**.
The **Edit** window opens.

Step 3. In the Nav tree, double-click the role name.
The **AX Property Sheet** for the role opens.



Property Sheet

sionDisplay (Role)

nabled	● true
ermissions	□ Super User (access entire station, file system) 4=r1:10=r1:18=r1RI
ewable Hierarchies	»

Permissions

Category	Operator R	Operator W	Operator I	Admin R	Admin W	Admin I
Admin						
Badge Management						
Personnel Management						
Graphics	✓		✓			
Monitoring						
User Management						
Schedules						
Access Rights						
Access Setup						
Intrusion Setup	✓		✓			
Alarm Setup						
Remote Device Setup						
Controller Setup						
General Reports						
Access Reports						
Intrusion Reports						
Hardware Reports						
Alarm Console	✓		✓	✓		✓
Tenant Management						
Video Subsystem						

OK Cancel

Step 4. Confirm that `Operator` level read (R) and invoke (I) permissions are configured for two categories: `Graphics` and `Intrusion Setup`.

Step 5. Enable `Admin` level read and invoke permissions for `Alarm Console`, click **OK** and click **Save**.

Result
The next procedure updates the display user.

Updating the user assigned to the display

You already set up this user when you created and assigned the certificate to it. This procedure updates this user with additional information: role, .nav file and other information.

Prerequisites:
You are working in Workbench connected to your station that manages the display device.

Step 1. Expand **Config** > **Services** and double-click the **UserService**.
The **User Manager** opens.

Step 2. To edit the existing user, select it in the table and click **Edit**.
The **Edit** window opens.

Step 3. Configure these properties:

- For **Roles**, assign the name of the role you created, for example, `Intrusion Display`
- For **Nav File**, assign the name of the file you created, for example, `file:^Nav/Intrusion.nav`
- For **Allow Concurrent Sessions**, select `false`

Step 4. Configure the **Default Web Profile**, `HTML5 Hx Profile` as follows:

- Enable Hx Workbench View = Yes
- Enable Nav Tree Side Bar = No
- Enable Search Side Bar = No
- Enable Nav File Tree = No
- Enable Config Tree = No
- Enable Files Tree = No
- Enable Histories Tree = No
- Enable Hierarchies Tree = No
- Enable View Selection = No

Step 5. For the **Mobile Web Profile**, configure properties as follows:

- For **Mobile Nav File** enter the name of the file you created, for example, `file:^Nav/Intrusion.nav`.
- Set **Type** to `Handheld Hx Profile`.

Step 6. When you finish setting up these properties, click **OK**.

Result

The display should now be able to connect to your station. The role and permissions you configured for the display user are the minimum needed to operate the device. You can certainly add more permissions later. To ensure that your display always attempts to navigate to the correct station page, add a path to the url for your controller in the display setup of your station connection. Using the example of an intrusion keypad, the url for the display could be: `/ord/station:|slot:/Services/AlarmService/AndroidIntrusionDisplay/AndroidView`.

Configuring the intrusion display

These **AlarmService** properties control what appears on the display.

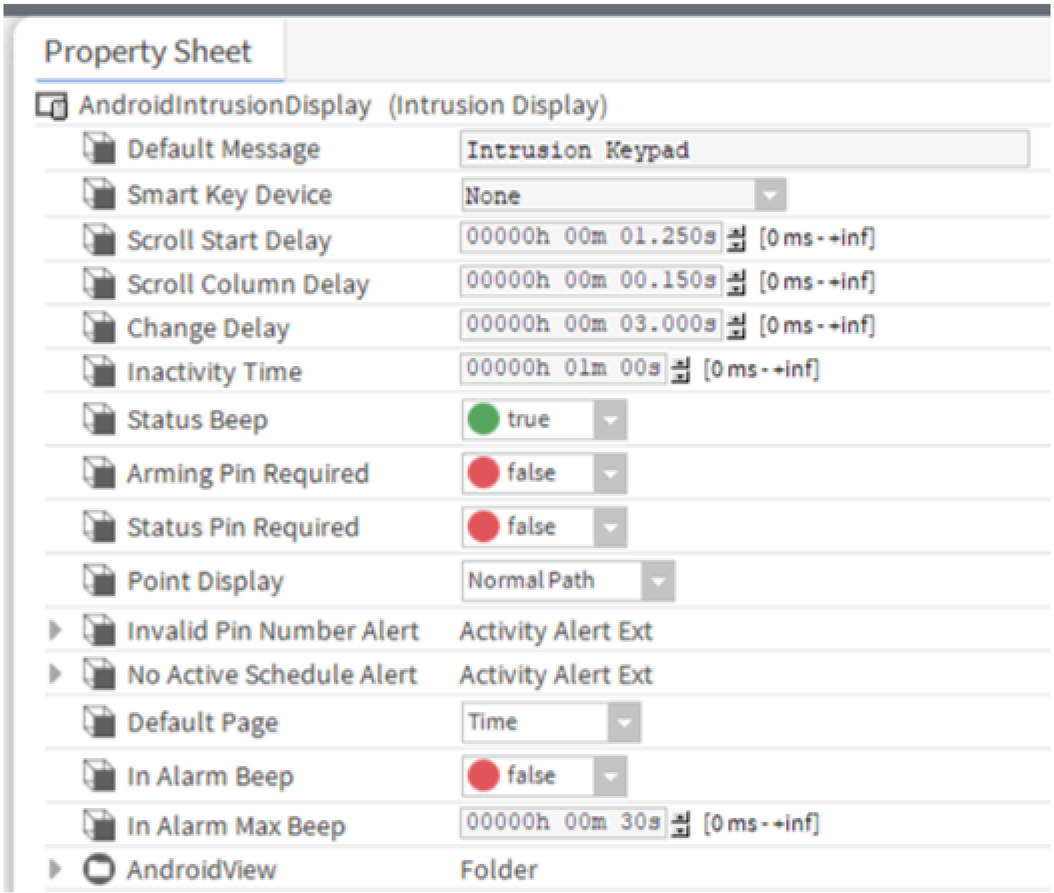
Prerequisites:

You are working in Workbench connected to your station that manages the intrusion zones.

Step 1. Expand **Config** > **Services** > **AlarmService**

Step 2. Double-click the **AndroidIntrusionDisplay** node.

The intrusion display’s **AX Property Sheet** opens.

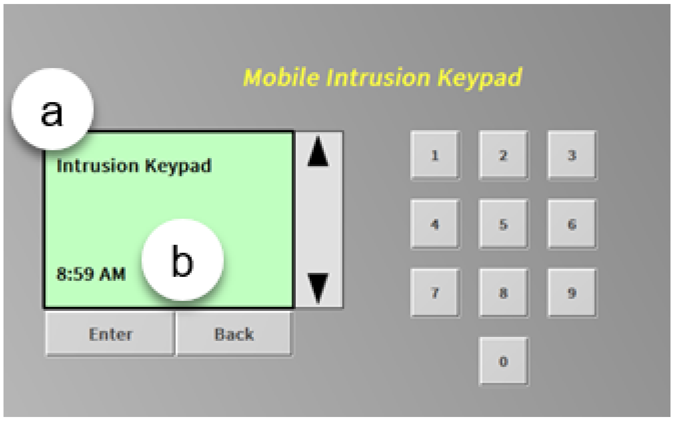


Property Sheet

AndroidIntrusionDisplay (Intrusion Display)

Default Message	Intrusion Keypad
Smart Key Device	None
Scroll Start Delay	00000h 00m 01.250s [0 ms - +inf]
Scroll Column Delay	00000h 00m 00.150s [0 ms - +inf]
Change Delay	00000h 00m 03.000s [0 ms - +inf]
Inactivity Time	00000h 01m 00s [0 ms - +inf]
Status Beep	● true
Arming Pin Required	● false
Status Pin Required	● false
Point Display	Normal Path
Invalid Pin Number Alert	Activity Alert Ext
No Active Schedule Alert	Activity Alert Ext
Default Page	Time
In Alarm Beep	● false
In Alarm Max Beep	00000h 00m 30s [0 ms - +inf]
AndroidView	Folder

Step 3. Set up the **`Default Message`**.
This message displays when **`Default Page`** is set to `Time`. This page displays after a period of inactivity.

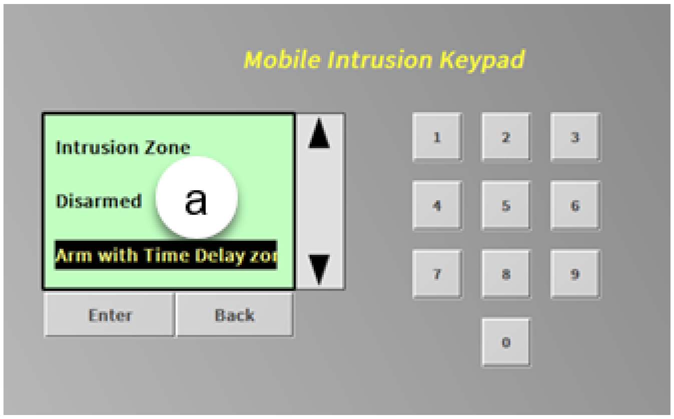


a. **`Default Message`**

b. **`Default Page`**

Step 4. Select `Summary` from the drop-down list for **`Default Page`**.

This page displays under the **Default Message** on the default screen. It can display the current time or the state of the intrusion zone(s) that are associated with the display. If your display is in a public area, you may not want to use the summary page as your default.



a. **Default Page**

Step 5. If a PIN is required to arm the system, set **Arming Pin Required** to `true`.
A PIN is always required to disarm the system.

Step 6. If a PIN is required to view the status of the system, set **Status Pin Required** to `true`.

Step 7. Select a value for **Point Display**.
Normal Path displays the station path to a point that is in alarm when performing an arming test or arm-with-time-delay-system. If the point exists in another station, the path displayed points to the remote station, for example: `entSecurity801.Input/Output Module.Sdi1`. If the point is in the local station, this property outputs `None`.

`Displays the Station Path to a Point`: displays the path to a point starting with the point reference when doing an arming test or arm-with-time-delay-system. For example: `Sdi1.Input/Output Module.entSecurity801`

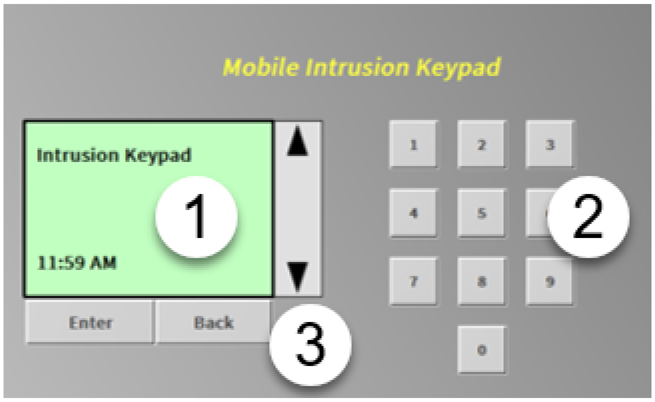
`None`: displays the local station path to a point that is in alarm when doing an arming test or arm-with-time-delay-system. For example, `entSecurity801.Input/Output Module.Sdi1`

The keypad interface

The onscreen keypad resembles a mechanical keypad. Its display window has a default view and a summary view.

The default display includes a timestamp.

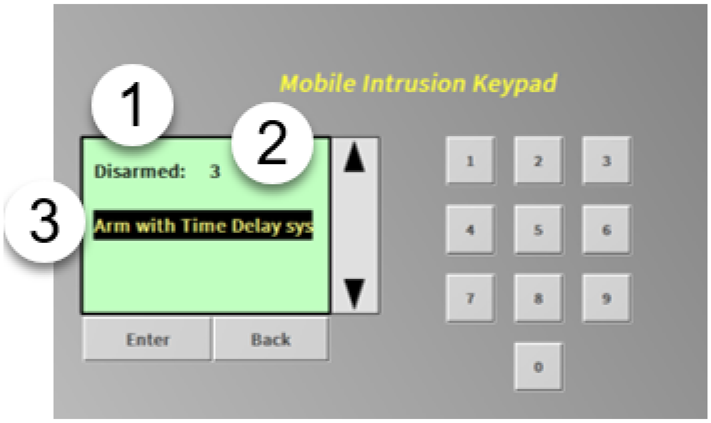
Figure 25. Intrusion keypad with default view



1. Display window with default information
2. Standard numeric keypad
3. **Enter** executes a selected action; **Back** returns to the previous view; the scroll bars navigate to additional zones.

The summary display shows the current state of the building, the number of zones and available action.

Figure 26. Intrusion keypad with summary view



1. Current state of the building
2. Number of zones in the building
3. Available action

For example, this summary indicates that the display is associated with three intrusion zones and all are currently disarmed.

You can arm all the zones at once or one at a time. To arm all zones simultaneously using a PIN, each zone must have the same PIN.

Arming a building

Several options are available for arming and disarming. These include preventing the arming of the building if any points are in alarm.

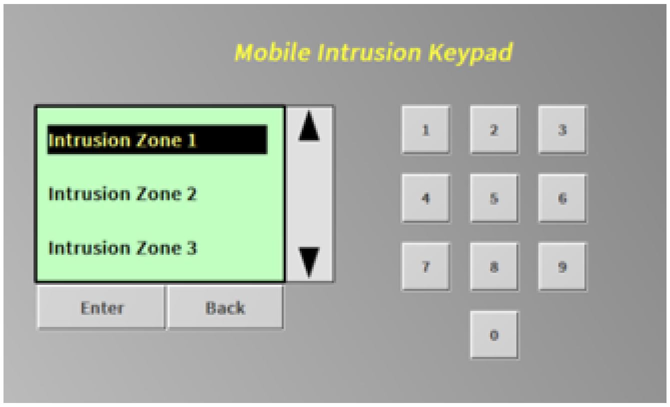
Prerequisites:
You have set up zones including required PINs.

Step 1. To test, before arming, if any points are in alarm, scroll down, select `Arming Test` and tap **Enter**.

Step 2. To select the zone to arm, scroll and select one of the following.

- To arm all zones at once, select `Arm system`.
- To arm zones one at a time, scroll up to the first line and select an intrusion zone.
- To arm with a time delay, select `Arm with Time Delay system`.
- To arm regardless of any points in alarm, select `Force Arm`.
- To arm regardless of any points in alarm as well as apply a time delay, select `Force Arm with Time Delay`.

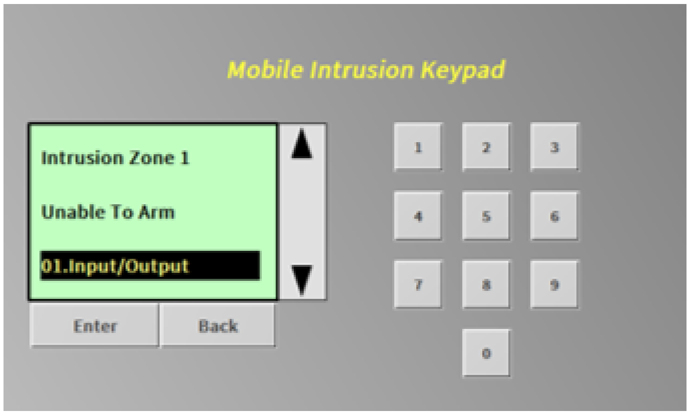
The display indicates your selection.



The screen capture shows arming a single zone.

Step 3. To arm the zone, tap **Enter**.

If you attempt to arm a building with a point in alarm, the display reports `Unable to Alarm`.

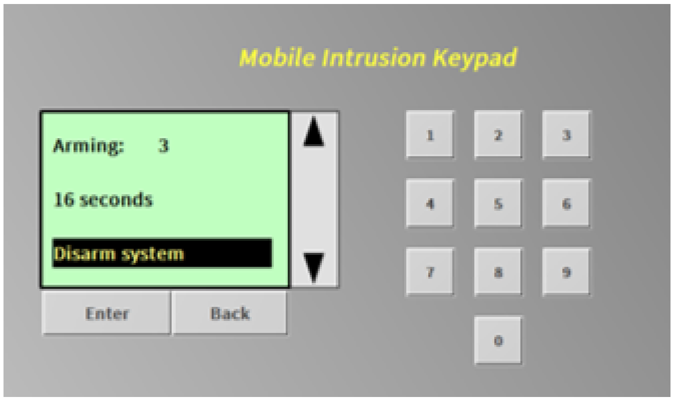


Intrusion Zone 1

Unable To Arm

01.Input/Output

If you selected `Arm with Time Delay`, the display includes a countdown timer.

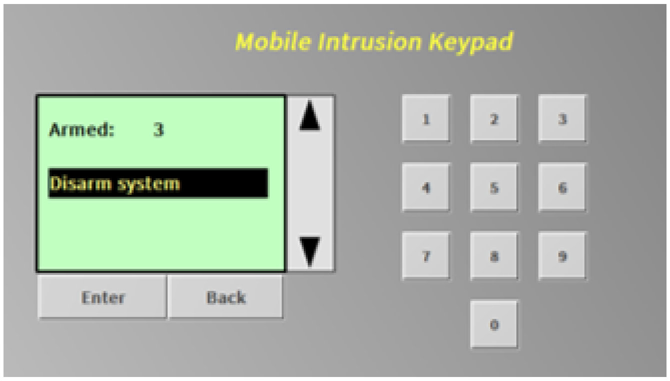


Arming: 3

16 seconds

Disarm system

After arming, the keypad displays the summary page with the option to disarm selected.



Armed: 3

Disarm system

Disarming a building

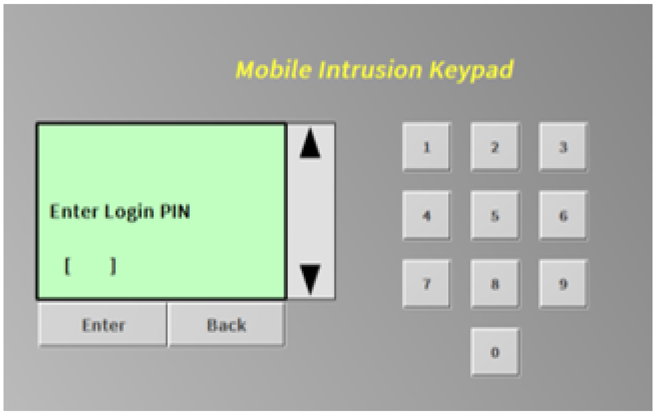
You may disarm all zones simultaneously or one at a time.

Prerequisites:
Zones have been armed. To disarm all zones at once, all zones have the same PIN.

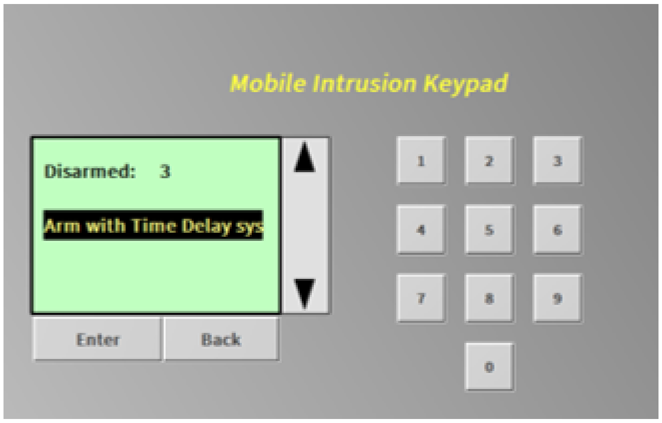
Step 1. Do one of the following and tap **Enter**:

- To disarm all zones simultaneously, select `Disarm system`.
- To disarm a single zone, scroll to `Disarm Armed zone`.

If a PIN is required, the keypad prompts you to enter the Login PIN.



Step 2. Use the keypad to supply the PIN and click **Enter**.
When the disarm command is successful, the keypad displays the summary view.



If the PIN is invalid, the keypad displays `PIN error` and prompts you to enter the PIN again.

SmartKey display/keypad

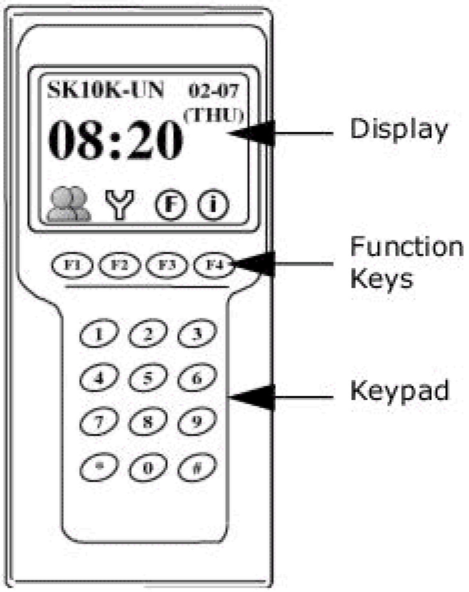
The SEC-INT-KP Remote Intrusion Display/Keypad (SmartKey device) provides a keypad and display screen for arming and disarming assigned intrusion zones.

The maximum number of SmartKey devices you can add or discover is six for each remote controller. If you add more than the maximum-allowed, the Status property for the extra SmartKey Devices displays `{fault} Exceeded device.limit of <n>` (where `<n>` is the maximum number of licensed SmartKey devices). Refer to the *Remote Intrusion Display/Keypad* installation sheet for installation and wiring instructions.

SmartKey device user interface

The SmartKey device user interface has three major parts:

Figure 27. SmartKey device

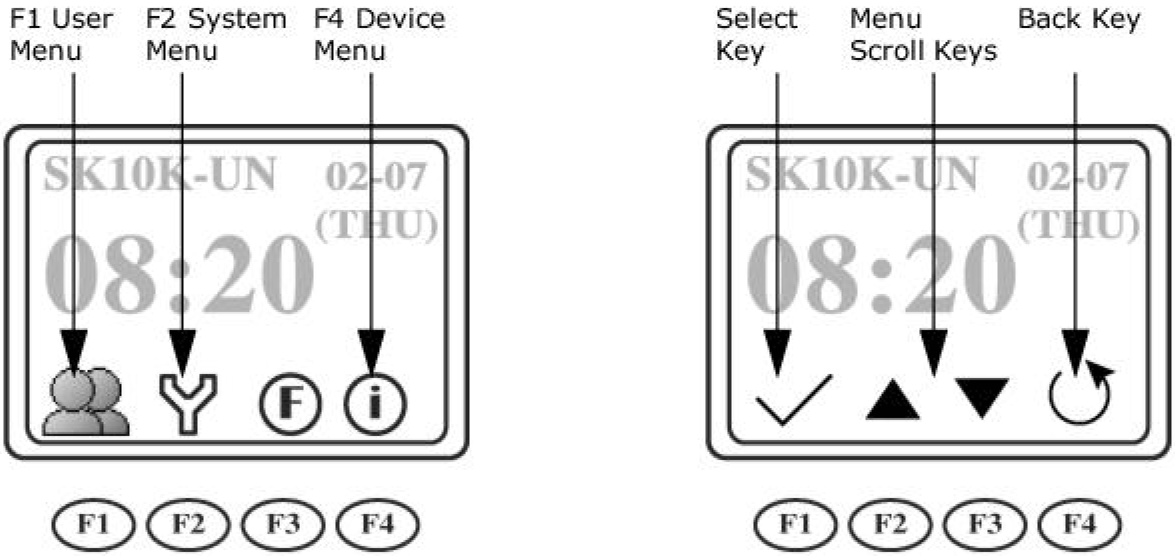


- Display: The top (upper area) of the display shows system information. The bottom area is reserved for two sets of function icons that work in conjunction with the function keys (F1-F4).
- Function Keys: These keys (F1-F4) open and navigate menus, and select menu items. Each function key corresponds to the menu function icon that appears directly above it on the display screen.
- Keypad: The twelve keys represent the numbers 0-9, asterisk (*) and pound (#) characters.

Function key controls

The four function keys (F1-F4) serve as selection keys for items that appear directly above them on the device display.

Figure 28. SmartKey device function keys and icons



Following is a description of each function key.

NOTE: Several of the menus require that you enter a login PIN to access them.

- F1 User Menu 👥

  When the User icon displays, pressing F1 key opens the Modify Logon PIN screen.

- F1 Select action ✓

  When the Select icon displays, pressing F1 key performs a selection action, similar to using an**Enter key** or **Ok** button.

- F2 System Menu Y

  When the System icon displays pressing the F2 key opens access to the System, Time, and Advanced… menus.

- F2 Scroll Up action ▲

  When the Scroll Up icon display, pressing the F2 key moves the selection indicator up one row each time you press the key.

- F3 Scroll Down action ▼

  When the Scroll down icon displays, pressing the F3 key moves the selection indicator down one row each time you press the key.

- F4 Device Menu ⓘ

  When the Device icon displays, pressing the F4 key opens the “Device” menu, which contains device ID and Firmware version information.

- F4 Back ↻

  When the Back icon displays, pressing the F4 key changes the display screen back to the previous screen.

Assigning a SmartKey PIN and ID

A unique ID identifies each SmartKey device on the network. Using the SmartKey device itself, you must assign this three-digit ID before you connect the device to the remote controller.

Prerequisites:
The SmartKey display/keypad has been installed and powered on.

The first time you use the SmartKey device, it prompts you to define a login PIN. Write down this PIN and keep it in a safe place.

CAUTION: If you lose this PIN, the SmartKey device must be sent back to the manufacturer.

Step 1. On the SmartKey device, press the **F2** key.
The Login screen opens.

Step 2. Enter the Login PIN number, press the **F1** key and select **System** menu from the display.
The **System** menu opens.

Step 3. Select Set **ID** and press the **F1** key.
The Input screen opens.

SmartKey intrusion keypads ship with a default ID (address) of 1. To connect more than one keypad, you must re-number them prior to discovery.

Step 4. Use the numeric keypad buttons to set a unique ID number (1-255) and press the **F1** key to save the entry.
The Operation Saved message appears temporarily to confirm that the ID number is set.

Step 5. Write down the ID number and location of each SmartKey device so you can easily identify SmartKey devices when setting up SmartKey devices in the Keypad Configuration view.

Discovering SmartKey devices

Discovery relies on the system to locate SmartKey devices connected to a remote controller.

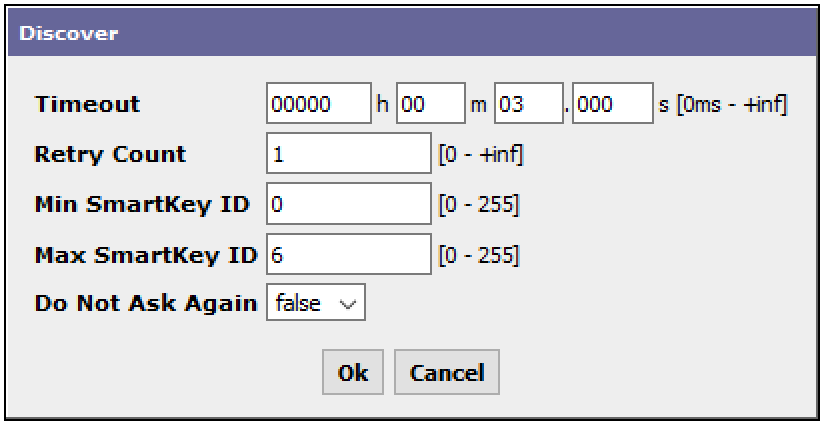
Prerequisites:
You have configured the PIN and ID (address) of the SmartKey display/keypad. Using the web UI, you are connected to the remote host controller to which the keypad is connected.

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.

Step 1. Under the **Controller Setup** menu, select **Remote Devices** > **Intrusion Displays/Keypads**.
The SmartKey Device Manager - Database view opens.

Step 2. Click the Discover button ( ).
The **Discover** window opens.



Discover

Timeout	00000 h 00 m 03 . 000 s [0ms - +inf]
Retry Count	1 [0 - +inf]
Min SmartKey ID	0 [0 - 255]
Max SmartKey ID	6 [0 - 255]
Do Not Ask Again	false

Step 3. To narrow the search, modify these properties and click **Ok**.
The discover job executes and displays found SmartKey devices in the Discovered pane.

Step 4. Select one or more discovered device(s), and click the Add button (⊕).
The system adds the device(s) to the Database pane.

Step 5. Name the device and click **Ok**.

Step 6. To update the database, click **Save**.

Adding and editing a SmartKey device

This procedure describes how to add Smart Key devices to the system database. You may add Smart Key devices while the device itself is off-line or online. Each SmartKey device has an ID, which you assign at the device. If the SmartKey ID has been assigned but you do not know it, and the device is currently online, use the discovery process to add the device instead of this manual process.

Prerequisites:
You are logged in to the remote station.

Step 1. Under the **Controller Setup** menu, select **Intrusion Setup** > **Intrusion Displays**.
The SmartKey Device Manager - Database view opens.

Step 2. Click the Add button (⊕).
The Intrusion Display tab opens.

Step 3. Enter an identifying **Display Name** for the device, select SmartKey Device from the **Smart Key Device** drop-down list.

Step 4. To require a PIN when the device is used to arm and disarm the intrusion zone, select true for **Arming Pin Required**.

Step 5. To assign the intrusion zone to the display/keyboard device, click the Intrusion Zones tab, click the Assign Mode button, select an unassigned zone, and click the Assign button (⊕).

Step 6. To save the record to the database, click **Save**.
One new device is added under the database at the top of the view.

Deleting a SmartKey device

This procedure explains how to delete SmartKey devices using the SmartKey Device Manager - Database view. You can also delete SmartKey devices from the Keypad Configuration view (under the SmartKey devices tab) by clicking the trash can icon).

Step 1. Under the **Controller Setup** menu, select **Remote Devices** > **Intrusion Displays/Keypads**.
The SmartKey Device Manager-Database view opens.

Step 2. Select the device to delete and click the Delete button (⊖).

Step 3. To reset the SmartKey device count, restart the station.

NOTE: Simply removing SmartKey devices from the database does not reset the SmartKey device count. You must restart the station.

Assigning a device to an intrusion zone

This procedure documents how to add a reader, keypad, or display to an intrusion zone. You can only add devices to intrusion zones when you are connected to the remote host station to which the device is connected. Devices are not visible and cannot be configured from remotely-grouped stations.

Prerequisites:
You are working in the remote host station to which the device is connected. The intrusion zone record in the local station exists.

Step 1. Click **Controller Setup** > **Intrusion Setup** > **Intrusion Zones**, and create a new zone or double-click an existing zone.
The Summary view for the display/keypad opens.

Step 2. Click the appropriate tab: Intrusion Displays for keypads and displays or Readers for card readers, and click the Assign Mode button (▤).
The Unassigned pane opens with a list of available devices.

Step 3. Click to select the device, and click the Assign button (⊕).
The system assigns the device to the intrusion zone.

Assigning an intrusion zone to a device

This procedure documents how to assign or update the assignment of an intrusion zone to a display and keypad.

Prerequisites:

You are working in a remote host controller station and have already created your intrusion zones.

Step 1. Click **Controller Setup** > **Intrusion Setup** > **Intrusion Displays**.

Step 2. Do one of the following:

- To create a new display/keypad, click Add (

  ⊕

).
- To edit an existing display/keypad, double-click on the display name entry in the table.

Step 3. Enter at least a **`Display Name`** and **`Default Message`**.

Step 4. To assign an intrusion zone to the display/keypad, click the Intrusion Zones tab.

Step 5. To locate the zone, click Assign Mode (▤).
The unassigned zones appear in the Unassigned pane.

Step 6. To complete the assignment, select the zone and click the Assign button (⊕).

Step 7. To save your configuration, click **Save**.

Arming and disarming an intrusion zone

How to arm and disarm depends on the hardware used to set up the zone. If the zone is not secure, it will not arm. This procedure uses the SmartKey display/keypad.

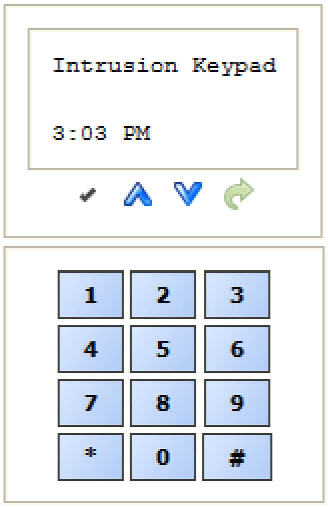
Prerequisites:
The access right assigned to your role permit you to arm and disarm.

Step 1. Ensure that all doors in the zone are secure.

Step 2. To arm a zone, do one of the following.

- If the zone is configured with a card reader, swipe your card at the reader.
- If the card reader has a keypad, enter the PIN.
- If the zone has an intrusion keypad, press the function key below the check mark.

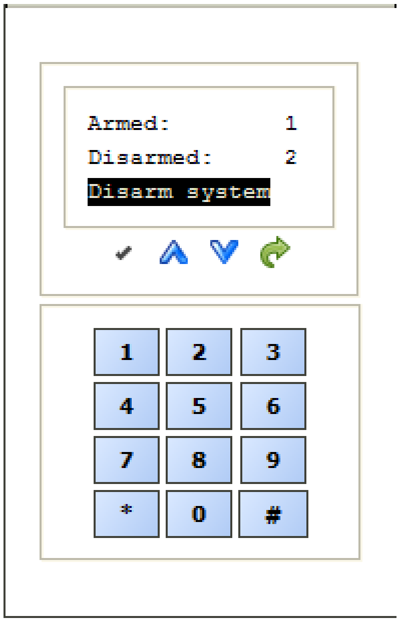
If you are using the intrusion keypad, the initial display looks like this:



Intrusion Keypad

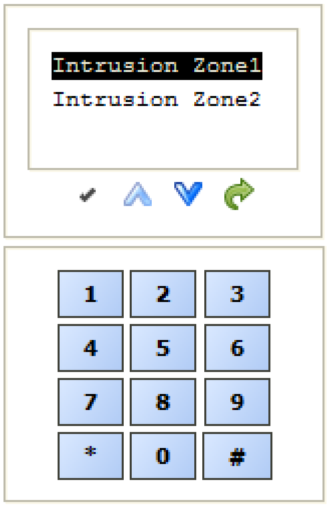
3:03 PM

Step 3. Use the **up** and **down** arrows to view additional information, such as system status, then touch the check mark.



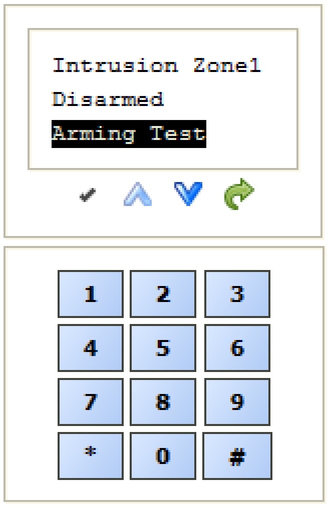
```
Armed:          1
Disarmed:       2
Disarm system
```

Step 4. Using the **up** and **down** arrows, scroll to the zone to arm or disarm, and press the check mark key to select the zone.



```
Intrusion Zone1
Intrusion Zone2
```

Step 5. Use the **up** and **down** arrows again to select the operation.



Intrusion Zone1
Disarmed
Arming Test

The operations are:

- `Arming Text` tests the zone to see if it is secure before attempting to arm.
- `Arm with Time Delay` arms the zone with a delay to allow the person to leave the area before the zone arms. If the zone is not secure, it will not arm. If you select this option, and `Arming Pin Required` is set to `false`, the arming process begins when you touch the check mark. The display beeps and counts down to armed. This allows the person to leave the area before the zone is armed.
- `Force Arm` arms the zone immediately. If the zone is not secure, it goes into alarm when it arms.
- `Force Arm with Time Delay` arms the zone with a delay. If the zone is not secure, it goes into alarm when it arms.

Step 6. To test the device, select `Alarm Test` and touch the check mark.
If the test fails, a description of the point in alarm scrolls across the bottom line of the display. If the test is successful, it displays Test Successful!

Step 7. After the test completes, touch the back arrow and select another option.

Step 8. You may arm, disarm and test an individual zone or multiple zones if all the zones are assigned the same PIN.
The action takes place when you touch the check mark or after you enter the PIN (if required). If a PIN is required, only the zones associated with the PIN are affected by the action.

Step 9. To use the PIN, enter it followed by #.

Assigning a card reader to an intrusion zone

This procedure sets up a single card reader without a keypad to use for arming and disarming an intrusion zone. Assigning a reader to a single zone is advised. If the reader is assigned to multiple zones, and one of the zones fails to arm, the person attempting to arm the building will not know which zone did not arm.

Prerequisites:
Your card reader has connections for LED and beeper control, and is connected to an R2R module on a host controller. Your PC is connected to the station of a remote host controller. The intrusion zone exists.

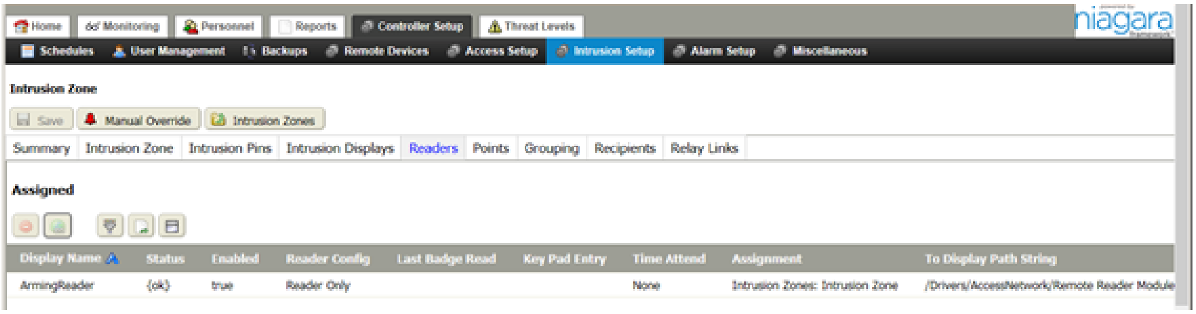
Add the reader at the module level. This reader may not be used to lock and unlock a door. Do not associate it with a door. The beeper and LED provide feedback to let the user know if the intrusion zone is armed or disarmed.

Step 1. To access the intrusion zone, click **Controller Setup** > **Intrusion Setup** > **Intrusion Zones**.
The Intrusion Zone view opens.

Step 2. Double-click the intrusion zone in the table.

Step 3. Click the Readers tab and click the Assign Mode button (⊟).
The system finds all the readers and populates the Unassigned pane.

Step 4. Select the reader in the Unassigned pane and click the Assign button (⊕).
The system moves the reader to the Newly Assigned pane.



Display Name	Status	Enabled	Reader Config	Last Badge Read	Key Pad Entry	Time Attend	Assignment	To Display Path String
ArmingReader	{ok}	true	Reader Only			None	Intrusion Zones: Intrusion Zone	/Drivers/AccessNetwork/Remote Reader Module

Step 5. To update the database with the newly-assigned card reader, click **Save**.

Step 6. To assign the reader to an existing access right, click **Personnel** > **Access Rights**, double-click the appropriate access right and click the Readers tab.
If needed, create an access right for the reader.

Step 7. To discover the reader, click the Assign Mode button (⊟), select the reader in the Unassigned pane, and click the Assign button (⊕).

Step 8. To arm and disarm the zone, present your badge at the reader.
Only people to whom the associated access right is assigned can use their badge to arm and disarm the zone.

If the zone is not secure, it will not arm. For example, if a door is propped open when the person tries to arm the zone, it will not arm. The person will need to find the problem and correct it before arming the zone.

Setting up a card reader with a keypad

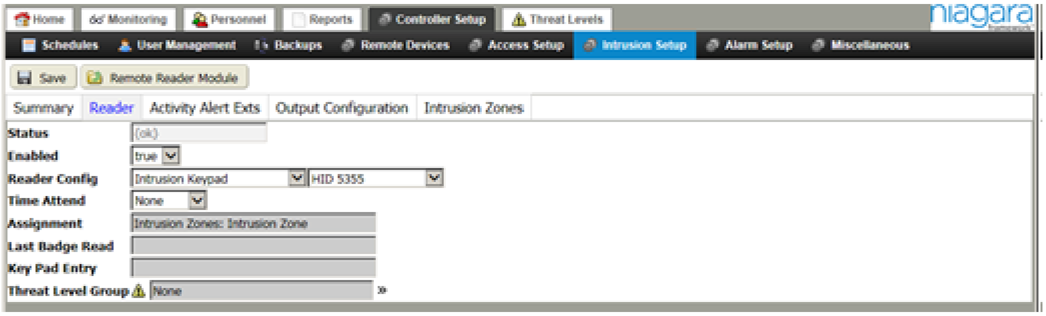
This procedure sets up a single card reader with a keypad to use for arming and disarming an intrusion zone. Assigning a reader to a single zone is advised. If the reader is assigned to multiple zones, and one of the zones fails to arm, the person attempting to arm the building will not know which zone did not arm.

Prerequisites:
Your card reader has connections for LED and beeper control, and is connected to an R2R module on a host controller. Your PC is connected to the station of a remote host controller.

Add the reader at the module level. This reader may not be used to lock and unlock a door. Do not associate it with a door. The beeper and LED provide feedback to let the user know if the intrusion zone is armed or disarmed.

Step 1. To add the reader to the database, click **Controller Setup** > **Remote Devices** > **Intrusion Displays/ Keypads**, click the Manage Devices button (⚙), to add, respond to the prompts.

Step 2. To assign the reader to the intrusion zone, click **Controller Setup** > **Intrusion Setup** > **Intrusion Zones**.



Status	(ok)
Enabled	true
Reader Config	Intrusion Keypad HID 5355
Time Attend	None
Assignment	Intrusion Zones: Intrusion Zone
Last Badge Read	
Key Pad Entry	
Threat Level Group ⚠	None »

Step 3. Add the reader to the intrusion zone.

Step 4. If needed add a PIN to the intrusion zone.

Step 5. To arm the zone, enter the PIN followed by #.
The system arms the zone after the delay period set up in the zone. The zone will not arm if it is not secure (a door is open).

Step 6. If the zone does not arm, clear the issue and try again.

Step 7. To disarm the zone, enter the PIN.

Chapter 12. Video installation

A network of video devices may include one or more Axis cameras, a Milestone DVR (Digital Video Recorder) and display device connected to the DVR or Maxpro cameras and an NVR (Network Video Recorder). The system provides the Axis, Milestone and Maxpro drivers. Each device has its own installation procedure, which is documented in materials provided by the manufacturer. This chapter segregates installation and configuration procedures based on the driver.

While these procedures use the web UI, you may prefer to use Workbench instead. Refer to the *Niagara Video Framework Guide* for Workbench procedures.

Browsers

HTML5 video rendering has been tested using Internet Explorer and Google Chrome.

Web Launcher and the Java applet

Niagara 4.9 supports HTML5 as well as the older Java-applet technology for rendering and playing back video clips. Video drivers, which support HTML5 (Milestone and Axis) do not require the Web Launcher (Web Start replacement) and Java applet, which run completely outside of a web browser.

These configurations require the Web Launcher and Java applet:

- Configurations that use the Maxpro video driver
- Configurations that use any video driver to play back older video clips that were rendered using the Java applet
- Configurations that use the Surveillance Viewer

TLS secure communication

TLS (Transport Layer Security) is a methodology for server authentication and data encryption. When TLS is enabled, all communication is automatically encrypted, including the data transferred from a camera to a station.

In addition to encryption, certificates provide device (server) authentication over a local area network in two ways:

- If you know that the self-signed certificate provided by a video device is valid, you can accept it the first time the station connects to the device and then manually approve it as an allowed host. Thereafter, no further action is required.
- More secure than using a self-signed certificate is to import a certificate into the video device that was signed by a CA (Certificate Authority) whose root certificate is in the station’s trust store. The first time the station connects to the device, authentication occurs automatically.

Over the Internet, an additional server certificate is required in the camera to authenticate the camera, as a server, to the browser that manages the transmission from the camera to the station. Again, you may accept and then approve a camera’s self-signed certificate, however, importing a signed server certificate into the camera is much more secure and should be your standard practice for securing all video devices when using the Internet.

A company may use a third-party CA, or serve as its own CA.

Security caveat

RTSP (Real Time Streaming Protocol) over TCP (Transmission Control Protocol), which is used for streaming media servers (video on demand and voice recording), is not secure. It does not use a TLS connection.

Video and port connections

When a configuration uses fox streaming to deliver video from a device, including a camera, DVR, NVR, and server (Axis, Maxpro, Milestone, XProtect), the controller station processes the incoming video and transmits it to users via the Web Service. This means that a device's network port can be different from the station's network port.

When a configuration does not use fox streaming, the station does not process the incoming video. Instead, the video stream transmits from the device to the user. This means that the video device must share the same network port as the station.

Requirements

To configure a video network, you need installed devices that are ready to be accessed, framework software, video drivers , additional licenses, one or more commissioned remote host controllers and signed server certificates.

Installed devices are ready to be accessed

All component devices (DVR, cameras, displays, NVR) must be physically installed, powered on, functioning correctly and ready to be accessed. For example, your camera(s), DVR, display(s), NVR must be connected to the network. Remote host controller must be on the same network as the video devices each controls.

For the a host station to access a device you need the following information:

- Device IP address and port number: These are required to set up UDP communications for the device.
- Device user name and password: Credentials are required for http access to devices for configuration, as specified by each individual driver.
- Appropriate ports open; the default are port 80 for the web, port 554 for control, port 9000 for data and port 9797 for motion detection.

Software and driver modules

This framework requires latest version of Niagara. The following general-purpose video driver jar files must be present in your installation's `modules` folder or already on the target station's controller.

- ndriver-rt.jar
- ndriver-wb.jar
- nvideo-rt.jar
- nvideo-wb.jar
- videoDriver-rt.jar
- videoDriver-wb.jar
- videoHx-rt.jar
- remoteVideo-rt.jar
- remoteVideo-wb.jar

You can view these modules in the `C:\Niagara\MySoftware-n.n.nn\modules` folder, where `MySoftware-n.n.nn` is your unique software installation folder.

You need one or more drivers for the specific manufacturer's equipment.

Licenses

Your license file must include an entry for the videoDriver feature, as well as a vendor-specific entry. Other device and point limits may exist in your license as properties associated with those features.

If your topology includes remote stations managed under the **NiagaraNetwork**, the Supervisor station must be licensed for the remote video feature.

Commissioned remote host controllers

Whether or not your network includes a Supervisor PC, each remote host controller must have been commissioned using NiagaraWorkbench.

Signed certificates

Each device (such as a camera) requires a server certificate signed by the private key of a root CA certificate. The root CA certificate with only its public key must be available in the station's System or User Trust Store. To authenticate a camera over the Internet, the root CA certificate must already be in the browser's trust store, or, if your company serves as its own CA, you must import the root CA certificate into the browser's trust store.

Video drivers default to secure communication. If a camera or other device does not support TLS, and the device must connect to the station, you may have to set **`Use Tls`** to `false` and change the device **`Http Port`** from `443` to `80`. Where to make these changes depends on the driver.

CAUTION: Do not disable secure communication unless you are setting up a device that does not support TLS. Disabling secure communication leaves your network vulnerable to a malicious attack.

About Axis network and camera configuration

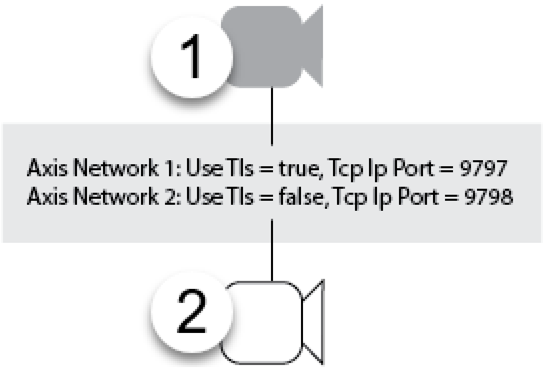
The properties and options that configure Axis camera-to-station communication provide flexibility and support for legacy cameras that lack a secure video stream as well as newer cameras that support TLS secure communication.

Axis networks

You can have two Axis networks: one to manage legacy cameras that do not support secure communication, and a second network to manage newer cameras that support secure communication. A single network cannot support both configurations.

Two properties play important roles in configuring these networks.

Figure 29. Station with two Axis networks


1
Axis Network 1: Use Tls = true, Tcp Ip Port = 9797
Axis Network 2: Use Tls = false, Tcp Ip Port = 9798
2

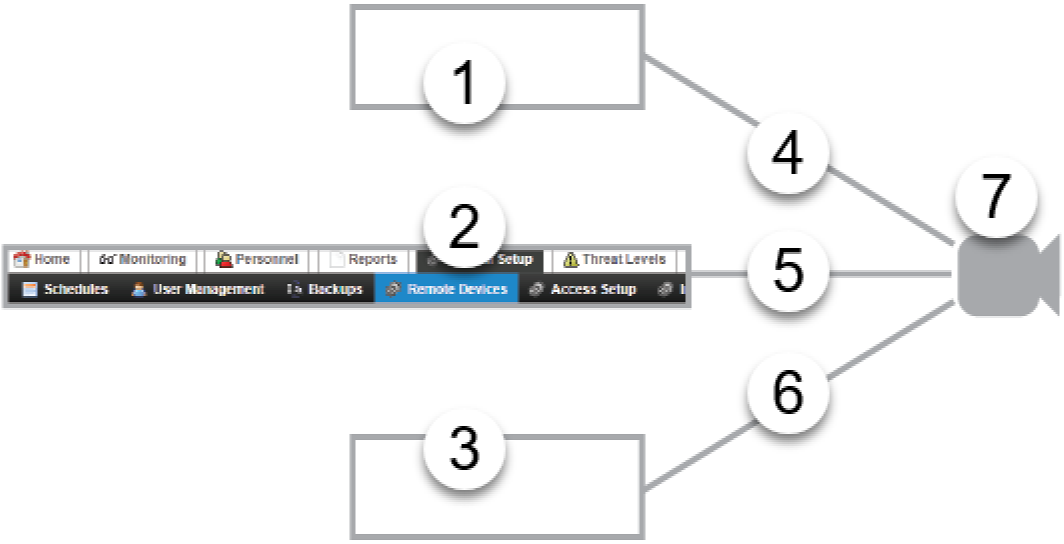
1. Camera(s) that support secure communication
2. Legacy camera(s) without secure communication

The **`Use Tls`** property on the Axis network tab (property sheet) enables and disables TLS security. The **`Tcp Ip Port`** must be unique for each network.

Axis camera communication channels

The camera properties configure the protocol, **`Web Port`** and CODEC used to communicate with the station. Three channels of communication connect to each video camera. Ideally, each should be secure.

Figure 30. Communication channels to and from a camera



1. Station—this channel delivers configuration properties and presets to the camera. These control how the camera operates.
2. Web UI—this channel receives the video stream from the camera and displays it in a browser.
3. Enterprise Security (Workbench)—this channel receives the video stream from the camera and displays it in a Surveillance Viewer.
4. Configuration data
5. Video stream
6. Video stream sent to Workbench

Newer cameras support TLS certificates for authenticating the camera as the server of video content and encrypting the video stream. Two protocols (one or the other) manage the video stream: HTTP or HTTPS (secure communication), and the more common RTSP (Real Time Streaming Protocol). Http and RTSP are not secure. The camera property that configures the protocol is **`Use Rtsp Stream`** (`true` = RTSP, `false` = Http or Https).

Communication security

The network property: **`Use Tls`**, and the camera property **`Use Rtsp Stream`** work together to configure secure channels when connected using a browser.

Properties		Channel protocols				
If Use Tls is …	**If Use Rtsp Stream is …**	**The configuration data channel uses …**	**HTML5 video streaming uses …**	**The video stream to the Web Launcher / Java applet (for Maxpro streaming) uses …**	**The video stream to Workbench uses …**	**Comments**
false	false	Http	Http	Http	Http	None of the channels are secure.
false	true	Http	Http	RTSP	RTSP	The camera's **`Web Port`** must be changed to 80. Its CODEC can remain at the default (MPEG, that is Ffmpeg_CODEC_ID_MPEG4).

Properties		Channel protocols				
If Use Tls is …	**If Use Rtsp Stream is …**	**The configuration data channel uses …**	**HTML5 video streaming uses …**	**The video stream to the Web Launcher / Java applet (for Maxpro streaming) uses …**	**The video stream to Workbench uses …**	**Comments**
true	true	Https	Https	RTSP	RTSP	Configuration data are secure but the video stream is not secure. The camera's **Web Port** can remain at the default: 443. Its CODEC should be changed to H264 (Ffmpeg_CODEC_ID_H264).
true	false	Https	Https	Https	Https	Configuration data are secure but the video stream is not secure unless you accept and approve the camera's self-signed certificate or install a server certificate in the camera that was signed by a root CA certificate in the browser's trust store. The Workbench video stream is secure. The camera's **Web Port** can remain at the default: 443. Its CODEC should be changed to MPEG4 (Ffmpeg_CODEC_ID_MPEG4).

A CODEC is a coder/decoder. The term refers to the method the camera uses to transmit a video stream.

More information about configuring Axis cameras for secure video streaming is available in the *Niagara Video Framework Guide*.

Installing an Axis video network (Web UI)

An Axis video network supports one or more Axis cameras. If some cameras support TLS (Transport Layer Security) and others do not, you will need two Axis video networks: one network with TLS enabled, and the other with TLS disabled.

Prerequisites:
The cameras are installed. The PC is connected to the camera network and running the web UI in a browser.

Step 1. Connect either to your Supervisor station (large installation) or to the single remote host station that controls the cameras (small installation).

Step 2. Click **Controller (System) Setup** > **Remote Devices** > **Remote Drivers.**
The Remote Drivers view opens.

Step 3. Click the Manage Drivers button (⚙), select `Add` and click **Ok**.

Step 4. Select the `Axis Video Network` from the drop-down list and click **Ok**.

Step 5. Optionally, give the network a unique name and click **Ok**.
The new Axis Network appears in the Network table.

Step 6. Double-click the newly-added network row in the table.
The Driver Manager view opens with the Axis Video Network tab selected.

Use Tls defaults to `true`, and **Tcp Ip Port** defaults to `9797`.

Step 7. To turn off TLS secure communication, change **`Use Tls`** to `false`.

CAUTION: Disabling TLS secure communication opens your installation to maliscious hacking. Do not disable this protection unless you know what you are doing, and, preferably, only if your network is not connected to the Internet.

Step 8. If this is the second Axis network you are installing, change **`Tcp Ip Port`** to 9798.
Each network requires a unique TCP/IP port number.

Step 9. Confirm that the network status is `{ok}`, and click **Save**.
If you have two networks, both network rows go into fault (turn yellow) until the software establishes each port. This can take a few seconds.

Adding (or editing) an Axis camera (Web UI)

Adding a camera may involve approving its certificate as well as configuring its communication properties. This procedure adds a camera manually. You can also discover cameras and edit their properties after adding them. Migrated installations list all existing cameras without the need to discover or manually add the cameras.

Prerequisites:
You are connected to the remote host station that controls the camera using the web UI. The Axis network has been set up, configured and its health reports `Ok`. For secure communication between camera and station, the camera supports TLS secure communication.

Step 1. From the main menu, click **Controller Setup** > **Remote Devices** > **Remote Drivers**.
The Remote Drivers view opens.

Step 2. Double-click on the Axis Video Network row in the table.
The Driver Manager view opens with the Axis Video Network tab selected.

Step 3. Click the Cameras tab.
The Camera Manager view opens.

This view displays a list of any existing cameras.

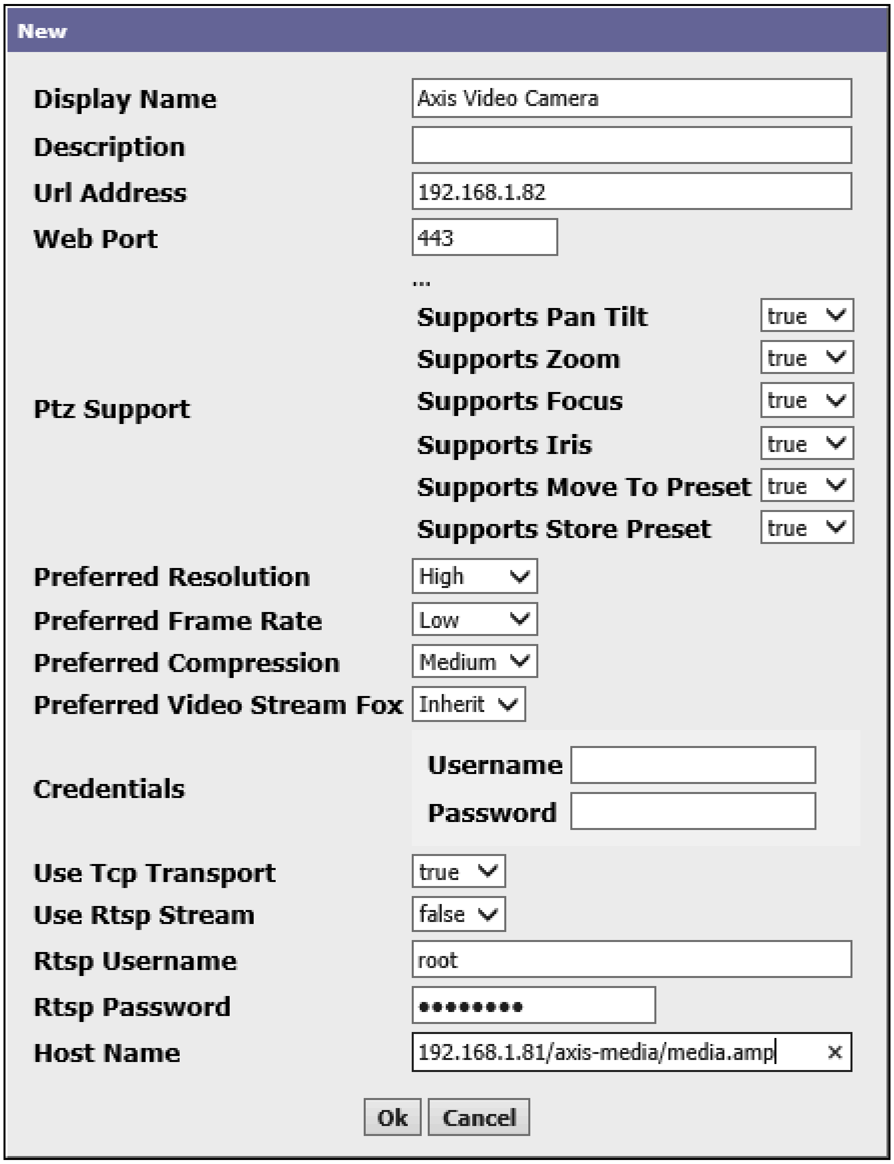
Step 4. Do one of the following:

- To edit the properties of an existing camera, double-click the camera row in the table or select the camera and click the Hyperlink button (

).
- To add an Axis camera manually, click the New button (

).

The **New** window opens.



New

Display Name	Axis Video Camera
Description	
Url Address	192.168.1.82
Web Port	443
	...
Ptz Support	Supports Pan Tilt: true Supports Zoom: true Supports Focus: true Supports Iris: true Supports Move To Preset: true Supports Store Preset: true
Preferred Resolution	High
Preferred Frame Rate	Low
Preferred Compression	Medium
Preferred Video Stream Fox	Inherit
Credentials	Username: Password:
Use Tcp Transport	true
Use Rtsp Stream	false
Rtsp Username	root
Rtsp Password	••••••••
Host Name	192.168.1.81/axis-media/media.amp

Step 5. Give the camera a **Display Name**, and optional **Description**; enter its **Url Address** (usually an IP address); and, to use secure Https streaming, click **Ok**.
A **Web Port** of 443 indicates that the communication channels default to secure communication. The camera must support TLS to communicate successfully.

If the station renders video from the camera using fox streaming, this port should be different from the station's port used to connect to the network. Otherwise, if the camera renders its own video and sends it to the user, this port should be the same as the port that connects the station to the network.

NOTE:

If **Use Rtsp Stream** is true, the channel will not connect because RTSP does not support secure communication from the camera to the station.

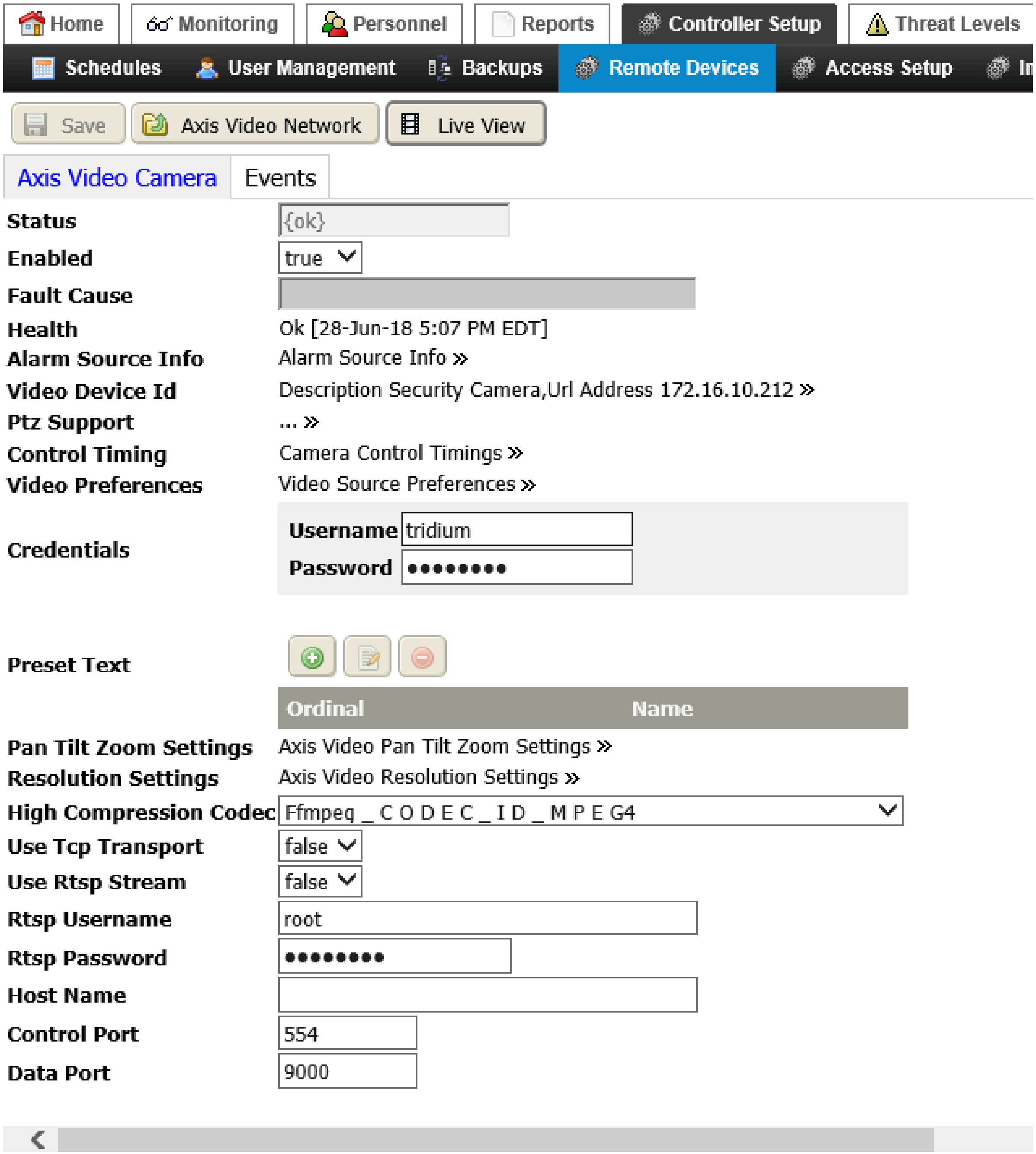
Step 6. To use RTSP streaming, set **Use Rtsp Stream** to true; define the credentials required by the RTSP (**Rtsp Username** and **Rtsp Password**); define the **Host Name** (<IP>/axis-media/media.amp); and click **Ok**.

This value defines a port to communicate data from a device that does not support secure communication.

The system saves the configuration to the station database.

Step 7. To view the camera properties, navigate back to **Controller Setup** > **Remote Devices** > **Remote Drivers** double-click the Axis video network row; click the Cameras tab; and double-click the camera row in the table.

The system opens the Axis Video Camera tab.



Status	{ok}
Enabled	true
Fault Cause	
Health	Ok [28-Jun-18 5:07 PM EDT]
Alarm Source Info	Alarm Source Info »
Video Device Id	Description Security Camera,Url Address 172.16.10.212 »
Ptz Support	... »
Control Timing	Camera Control Timings »
Video Preferences	Video Source Preferences »
Credentials	Username tridium Password ••••••••
Preset Text	Ordinal / Name
Pan Tilt Zoom Settings	Axis Video Pan Tilt Zoom Settings »
Resolution Settings	Axis Video Resolution Settings »
High Compression Codec	Ffmpeg _ C O D E C _ I D _ M P E G4
Use Tcp Transport	false
Use Rtsp Stream	false
Rtsp Username	root
Rtsp Password	••••••••
Host Name	
Control Port	554
Data Port	9000

Status should be `{ok}`.

Step 8. If **Status** is not `{ok}`, confirm that the **High Compression Codec** is appropriately configured for the camera, and, if necessary, change this property and click **Save**.

- For a secure Https:// connection between the camera and station, the CODEC should be: `MPEG4` (Ffmpeg_CODEC_ID_MPEG4).
- For an RTSP connection between the camera and station, the CODEC should be: `H264` (Ffmpeg_CODEC_ID_H264).

Discovering cameras (Web UI)

You can add cameras individually or use a discovery job to add cameras.

Prerequisites:
You are connected to the Supervisor station (large installation) or to the single remote host station that controls the cameras (small installation.)

Step 1. Click **Controller (System) Setup** > **Remote Devices** > **Remote Drivers.**
The Remote Drivers view opens.

Step 2. Click the Manage Drivers button (⚙), select `Add` and click **Ok.**
The Driver Manager view opens.

Step 3. Click the Cameras tab.
The Camera Manager view opens.

This view displays a list of any existing cameras.

Step 4. Click the Discover button ( ).
A discovery job runs. Some cameras will discover and others will not. If your camera does not discover after a minute or two, click on the New button (

🗋

) and add it manually.

Step 5. Double-click each camera and enter the **`Host Name`** for each and click **Save.**
The camera appears in the list under the Cameras tab.

Step 6. Ping the camera and observe if the status shows `{ok}` or `unacknowledged alarm`.

Step 7. If you have a PTZ camera with presets, double-click the camera and add or rename presets.

Step 8. Observe the ports listed under the camera and make sure that your firewall is configured with the needed ports open.
You will have issues with PTZ control and video motion if the required ports are blocked.

Approving a camera self-signed certificate (Web UI)

If your browser permits self-signed server certificates, this procedure guides you to compare the **`Issued By`** and **`Subject`** properties of this certificate before you manually approve the connection.

Prerequisites:
You do not have a server certificate for the camera that was signed by a valid root CA certificate.

Step 1. Accept the self-signed certificate and make a connection to the camera.

Step 2. To locate the certificate do one of the following:

- Using the web UI, navigate to **Controller (System) Setup** > **Remote Devices** > **Certificate Management.**
- Using Workbench navigate to **Station** > **Services** > **PlatformServices** > **CertManagement.**

The station opens the **Certificate Management** view.

Step 3. To acknowledge the security warning, click **Allow** and click the Allowed Hosts tab.

Step 4. To open the certificate, select it and click **View.**

The **Host Exemption** window opens.

Step 5. Confirm that the certificate's **`Issued By`** and **`Subject`** properties contain names you recognize, and click **Ok**.
For a self-signed certificate, these properties should be the same. They should contain the name of the camera manufacturer or other identifiable text.

CAUTION: If you do not recognize the value of these properties, you may need to investigate with the camera manufacturer. This certificate authenticates the camera as a valid video server. Approving a bogus certificate opens your system to a man-in-the-middle attack.

Step 6. Assuming that the certificate is valid, and, if the certificate has not been approved yet, click **Approve** and respond to the confirmation window by clicking **Yes**.
The web UI's Camera Manager view lists the camera.

Viewing the Axis camera video stream (Web UI)

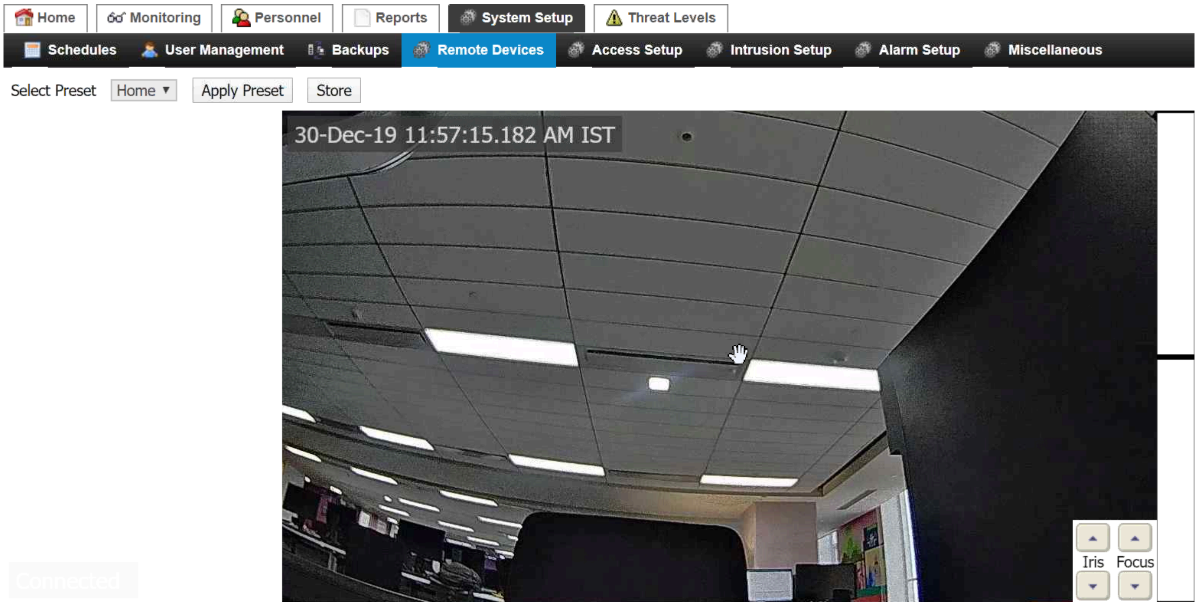
An Axis camera provides features for manipulating the HTML5 video stream.

Prerequisites:
The camera is installed and configured. The Axis Video Camera tab reports the camera's health as `Ok`.

Step 1. From the main menu, click **Controller Setup** > **Remote Devices** > **Remote Drivers**, double-click on the Axis network row in the Remote Drivers table, and click the Cameras tab.
The Camera Manager view opens.

Step 2. Double-click a camera row.
The view opens to the Axis Video Camera tab.

Step 3. Click the **Live View** button at the top of the view.
After a moment connecting, the video stream opens.



The first time you make the connection it takes a few seconds for the live view to open. If the framework reports "Connection timeout," just wait a little longer.

Step 4. To adjust the Iris and Focus, click the controls.

Result
An Axis camera can also appear in a Video Surveillance viewer.

Configuring an alarm

This procedure uses a Motion Detected event in a connected camera to trigger an alarm. The steps use both the web UI and Workbench interfaces.

Prerequisites:
All cameras have been discovered or added to the station.

Step 1. Click the Events tab and click the Discover button ( ).
The discovery job searches for events.

Step 2. Add Motion Detected to the database and double-click on Motion Detected.

Step 3. Click on the Alarm Setup tab and notice that the alarm has already been mapped back to the camera.

Step 4. Using Workbench, find a camera under the **AxisVideoNetwork** in your Supervisor station and, under the camera, the Motion Detected point.

Step 5. Delete the Alarm Settings extension.

Step 6. Open the alarm palette and drop a **BooleanChangeOfStateAlarmExt** on the point.

Step 7. Open the videoDriver palette and drop a **VideoAlarmExtParameters** component on the **BooleanChangeOfStateAlarmExt**.

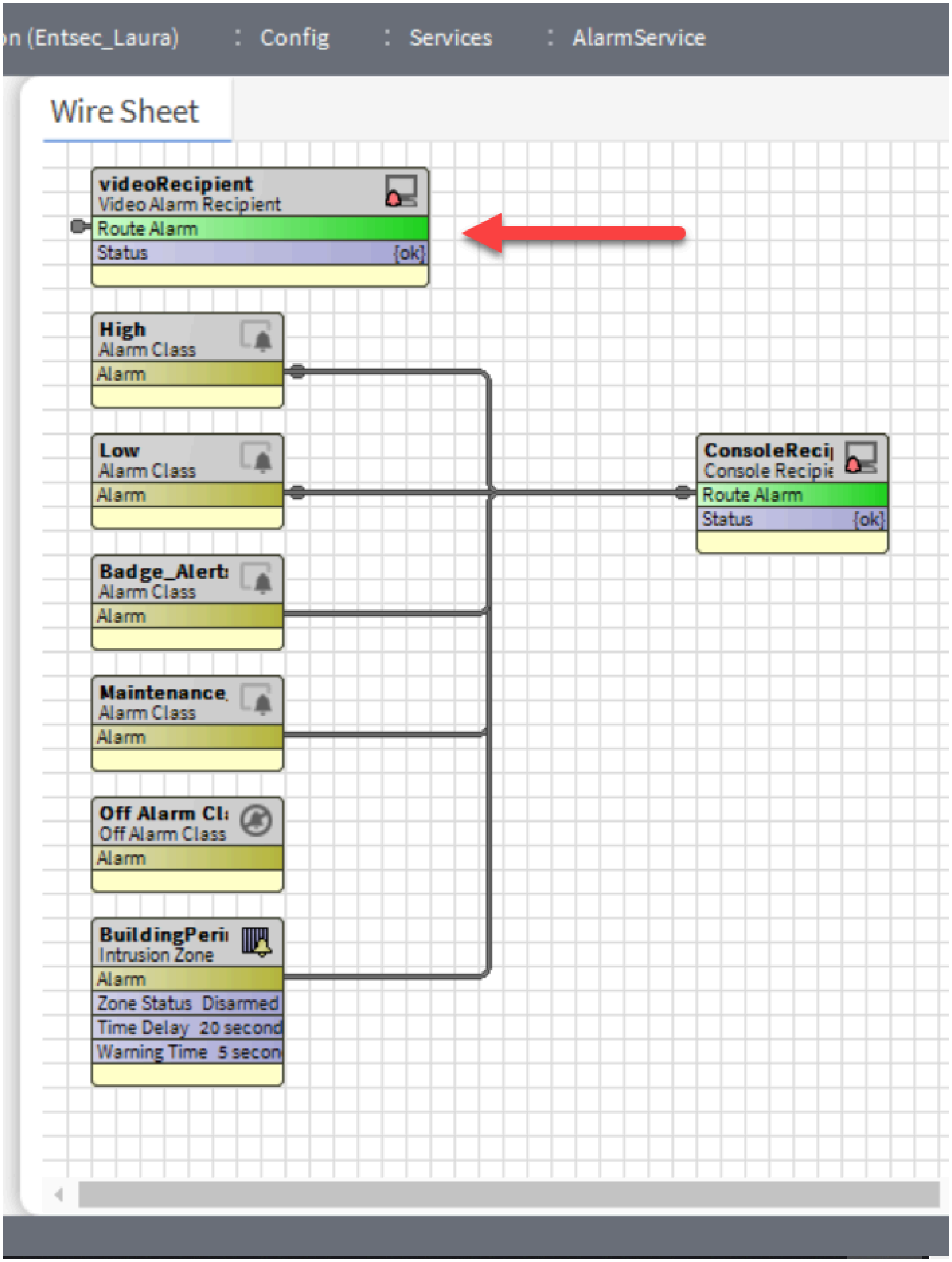
Step 8. Double-click on the alarm extension, scroll to the bottom of the view, click on the folder next to the `Camera Ord` property, select your camera and save your changes.

Step 9. Wave your hand in front of the camera.
The alarm console should report an alarm.

You can use this method to reference a camera to other alarms in your system and to play the associated video.

Step10. Expand **ConfigServices** and double-click the **AlarmService**.

Notice that a **videoRecipient** has been added to the **AlarmService**.



Enterprise Security adds this recipient automatically when you configure a video network. If you are using video in a standard station, you will need to add this recipient yourself. A **videoRecipient** is required to move a camera to a preset based on an alarm.

About Milestone driver configuration

The system supports three Milestone software products with two drivers: nmilestone and xprotect.

Milestone drivers and software products

The nmilestone driver supports the XProtect Professional product:

- XProtect Professional
- XProtect Enterprise (deprecated, but uses the same nmilestone.jar API)

The xprotect driver supports the XProtect Professional+ and XProtect Corporate products.

- XProtect Professional+
- XProtect Corporate

Interfaces

Two interfaces are available to add and configure these drivers in a station:

- Workbench
- Enterprise Security Web User Interface (web UI)

The *Niagara Enterprise Security Installation and Maintenance Guide* references both interfaces. The *Niagara Video Framework Guide* (this guide) references the Workbench interface exclusively.

Licensing

The milestone and xprotect drivers require a Milestone software license.

Driver naming conventions

The two drivers are referred to in different ways depending on where you are in Workbench:

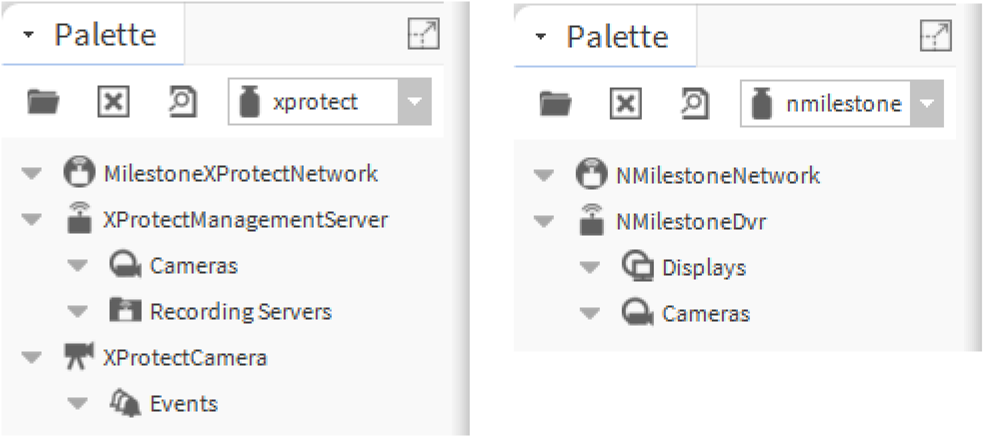
Table 25. Versions supported

Milestone Xprotect version	supported by
Xprotect 2020 R3 and earlier	Niagara 4.10u1 and earlier
Milestone Xprotect 2021 R1	Not supported

Palettes

Two palettes provide Milestone and XProtect components. These palettes require the Workbench interface.

Figure 31. Palettes and components



The xprotect driver provides these components:

- MilestoneXProtectNetwork sets up the network component.
- XProtectManagementServer connects to the Milestone management server, which may reside in a separate computer.
- Cameras is a folder for collecting one or more XProtect-compatible camera devices.
- Recording Servers is a folder for collecting recording servers.
- XProtectCamera provides camera configuration properties.
- Events is a folder for collecting events, such as motion detected.

The nmilestone driver provides these components.

- NMilestoneNetwork sets up the network component.
- NMilestoneDvr sets up a Milestone DVR.
- Displays is a folder for collecting one or more monitors to display video.
- Cameras is a folder for collecting one or more camera devices.

Port numbers

If Milestone and the station are installed on the same PC, the Milestone management server requires ports 80 and 443 for its internal processes. Before connecting, you must change the ports used by the WebService to 81 and 444 or relocate the management server to another computer that shares the network.

If you change the WebService ports and have connection problems, you may need to open them up in your firewall.

The nmilestone driver

This driver supports the Milestone Professional video management software program running in a stand-alone (single controller) or company-wide installation that includes at least one Supervisor PC.

Nmilestone features

- Automatic discovery of cameras
- PTZ operations: control and go-to presets
- Motion detection alarms and recording alarms
- Surveillance Viewer

- Alarm video playback
- Live video playback
- Switching between live and playback video
- Remote video connections
- Fox video streaming
- Graphics widgets

Tested models

The nmilestone driver has been tested with the Milestone XProtect Professional. Milestone XProtect Enterprise is deprecated, but uses the same API.

Requirements

- IP access between the DVR or camera and remote controller
- Appropriate open ports: the defaults are port 80 for the web (image server port), central port 1237, and upload events port 1234.

Compliance

- To create presets, use the Milestone application. This driver does not support preset creation. It does support the Move-to-Preset option.
- Milestone cameras do not support: Enable Detection and Disable Detection. Even if you add an Event Detection Control Ext, it will not work with a Milestone camera.
- This driver does not support Iris and Focus controls.
- Camera health continues to report `Ok` even after the camera is disconnected from the network. This is an issue with the Milestone application. Video is not streamed for a disconnected camera.

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

The xprotect driver

This driver supports Milestone's XProtect Corporate and XProtect Professional+ video management software running in a company-wide installation that includes at least one Supervisor PC.

Versions supported

Milestone Xprotect version	Supported by
Xprotect 2020 R3 and earlier	Niagara 4.10u1 and earlier
Milestone Xprotect 2021 R1	Not supported

xprotect features

Supported features include:

- Automatic discovery of cameras
- PTZ operations: control and go to presets
- Surveillance Viewer
- Live HTML5 video streaming
- Playback HTML5 video streaming
- Switching between live and playback video
- Motion detection alarms and recording video triggered by an alarm
- Alarm console video playback
- Remote video connections
- Fox video streaming
- Graphics widgets

- Support for a management server

Tested models

The Xprotect driver has been tested with the Milestone XProtect Corporate, XProtect Professional+, and the Xprotect Essentials+ and is compatible with the Xprotect Driver of Niagara. The integration steps remain unchanged.

Required files

This file in the `Niagara_Home\modules` folder: `xprotect-wb.jar`

NOTE: The previous module name for the xprotect driver was `xprotect-se.jar`. If you upgrade a system, do not copy this old file to the `module` folder. Running the software with both drivers introduces conflicts.

These files are in the `Niagara_Home\bin` folder:

- `VideoOS.Platform.dll`
- `VideoOS.Platform.SDK.dll`
- `xprotectBridgeService.exe`

Compliance

NOTE: For the purpose of configuring a camera, the xprotect driver must run in the Supervisor PC. Stand-alone systems, which have only one controller, do not support integrating a camera with the Milestone video management software. In a company-wide installation, the xprotect driver running in a controller provides alarm mapping (it resolves xprotect camera Ords that appear in the Supervisor’s alarm console). No other xprotect features work in a controller.

- The Xprotect SDK API does not support preset creation. The xprotect video driver supports only the Move to Preset option. To create presets, use the Milestone Corporate software.
- An action on the XProtect camera, called Get Preset List, must be invoked to read the list of presets from the Milestone Corporate software. Workbench provides this action, which takes immediate effect. Otherwise, getting presets from the camera occurs automatically on each camera ping.
- The XProtect SDK does not provide an API to add a camera programmatically to the management or recording servers. As a result, the xprotect driver does not support the add-net-camera option from Workbench. You must discover cameras to add them to a station.
- The XProtect SDK API does not support Iris and Focus controls. Consequently, the xprotect driver does not support the Iris and Focus operations from Workbench.
- The xprotect driver supports only Motion Detection Started and Motion Detection Stopped alarm conditions from the Milestone Corporate software.
- Since motion detection events are polled from a recording server, recording servers must be discovered and added to the management server component apart from cameras.

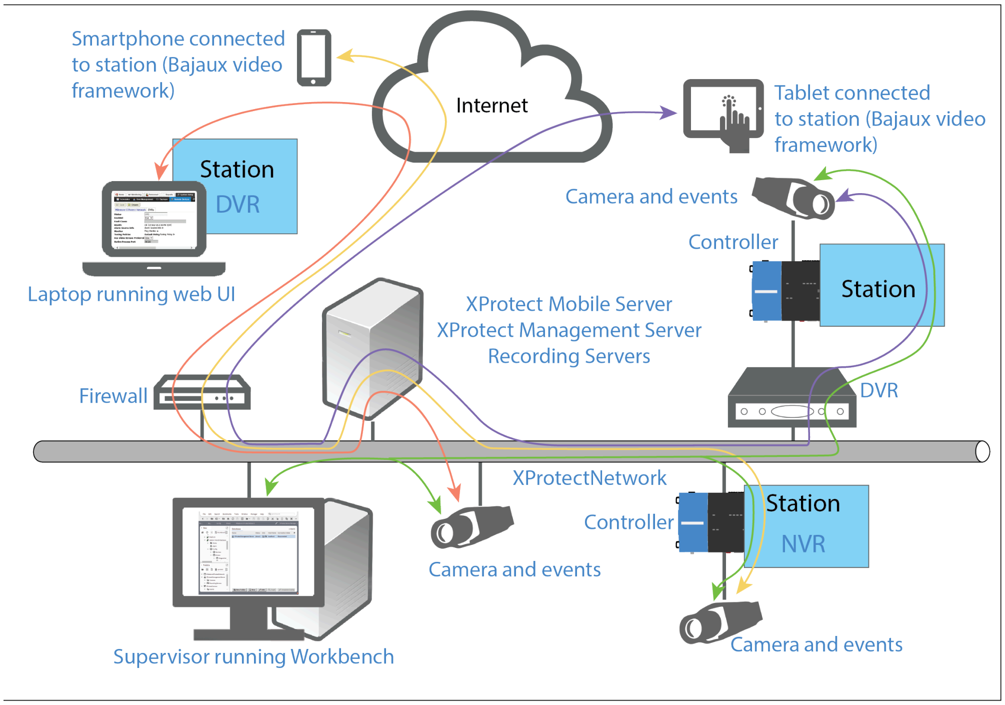
HTML5 streaming

The latest versions of Niagara support the video framework HTML5 streaming using the Milestone xprotect driver for video playback. The Surveillance Viewer continues to use the applet view (supported by Web Launcher), however, the playback viewer supports HTML5–rendered video clips. HTML5 streaming makes use of the MilestoneXprotectServer and XProtectMobileServer.

XProtect architecture

Milestone’s XProtect products offer comprehensive video performance for Niagara installations. In addition to licensing and configuring the drivers, additional software ensures connectivity on hand-held devices connected over the Internet.

Figure 32. XProtect architecture



The XProtectNetwork is the parent component. Its view, called the **X Protect Server Manager** supports one or more XProtect Management Servers.

An XProtect Management Server (usually located in a separate computer) configures access from a Supervisor station to all devices (cameras and recording servers) on the network. A **Host Name** identifies this computer on which the XProtect Management Server is running. When the authentication type is Windows, authorization properties identify the **Domain** name of the server (a separate IP address from that for the host computer) and provide credential authorization (username and password) to access the server. A **Hostname** (another IP address) and **Port** identify each Recording Server.

The XProtect Mobile Server supports access to cameras and recording servers from remote devices that connect to the video network through the Internet. All devices that use the web UI, including laptops/ computers, smartphones and tablets require the installation of the XProtect Mobile Server on the computer with the XProtect Management Server.

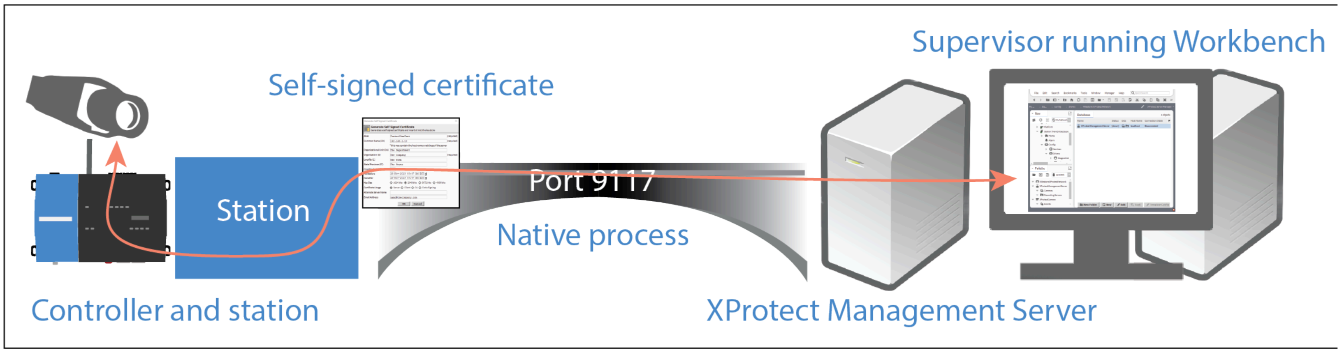
XProtect requirements

Secure communication requires a secure connection between all components, processes and browsers. XProtect products use an XProtectManagementServer to manage live video and store recorded video.

Native process protection

Behind the scenes a native process using port 9117 functions as a bridge between an XProtect management server and the station. Running on the local computer that houses the station, the native process starts when the xprotect driver starts and stops when the station shuts down.

Figure 33. XProtect connections



In Niagara, this process randomly assigned the port it used to connect without security to the station.

In Niagara, this connection requires a specific port through which only Niagara may make a secure connection from the station through the native process and on to the server. A certificate assigned to the port provides security for the native process. You must set up the `Native Process Port` and install the certificate.

Management and mobile servers

The MilestoneXProtectManagement server, which usually runs on a computer that is separate from the Supervisor PC, manages live video and stores recorded video.

The XProtect Mobile server supports mobile devices that use browsers to connect to the XProtect network over the Internet: computers, smartphones and tablets.

Before installing the xprotect driver:

- Use the Milestone XProtect VMS (Video Management System) Products System Installer, version 2019 R3 or later to install the XProtect software on a PC that is on the network other than your Supervisor PC.
- Ensure that the XProtect Mobile Server is installed and running on the Supervisor PC. This software provides the HTML5 solution for the video.

Camera certificates

Devices may always connect without security (`http://`), but to protect your data, all devices, including cameras, need to make only secure (`https://`) connections. Secure connections through a browser to remote cameras require TLS certificates. The Milestone Mobile server will not connect securely to a camera using even an approved self-signed server certificate. It requires that the camera have a certificate signed by a root CA certificate in the browser's trust store.

Adding a network (nmilestone or xprotect)

The Milestone networks support Milestone and XProtect surveillance hardware.

Prerequisites:
The station is licensed for one of two Milestone drivers: nmilestore or xprotect. You are running Workbench on a Supervisor PC or laptop.

Step 1. Open the platform and connect to the station.

NOTE: It can take a few seconds to a minute to establish communication with the station.

Step 2. In the station Nav tree, expand the **Config** folder and double-click the **Drivers** folder.
The **Driver Manager** view opens.

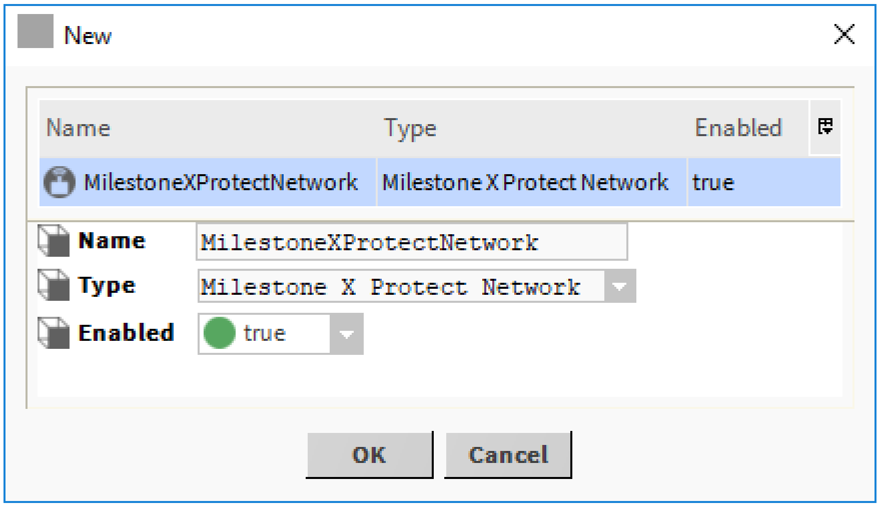
This view manages network video drivers.

Step 3. Do one of the following:

- To set up a network for the first time, drag the network component from the palette to the click **Drivers** folder or click the **New** button at the bottom of the view.
- To change properties, select the network name (activates the **Edit** button) and click **Edit**. This opens the **Edit** window, which provides access to most, but not all properties for editing.

If this is a new installation, the **New** window opens. Two Milestone networks are available: `NMilestoneNetwork` and `MilestoneXProtectNetwork`. Your Milestone installation requires one or the other, not both networks.

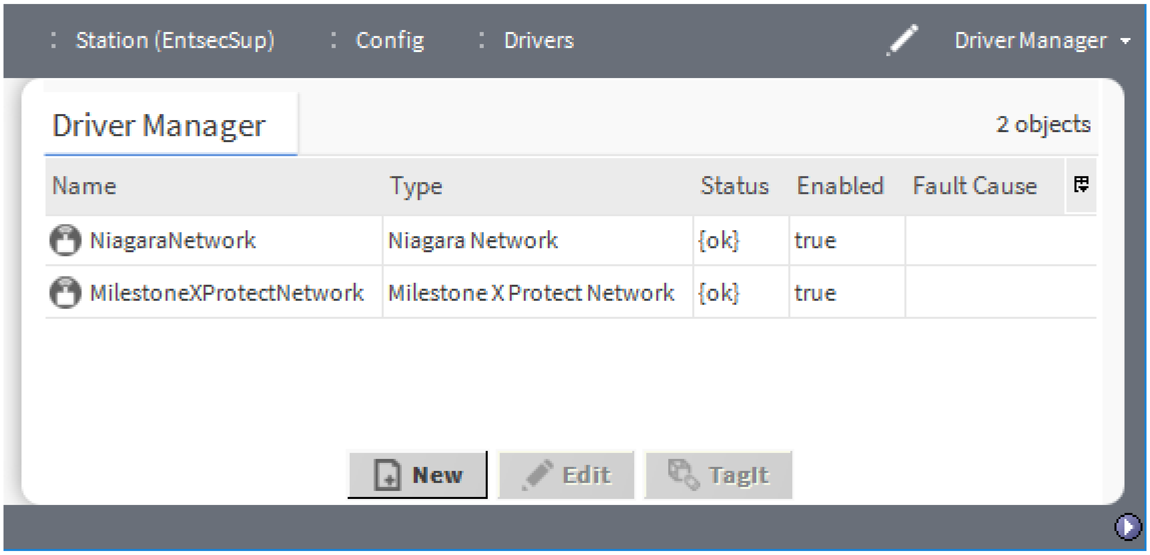
Step 4. To add the network, select it from the **`Type to Add`** list and click **Ok**.
A second **New** window opens.



Name	Type	Enabled
MilestoneXProtectNetwork	Milestone X Protect Network	true

Name MilestoneXProtectNetwork
Type Milestone X Protect Network
Enabled ● true

Step 5. Change the name and click **OK**.
The **Driver Manager** displays the added network.



Driver Manager

2 objects

Name	Type	Status	Enabled	Fault Cause
NiagaraNetwork	Niagara Network	{ok}	true	
MilestoneXProtectNetwork	Milestone X Protect Network	{ok}	true	

Step 6. To confirm that the network is ready, wait for the Status column to read `{Ok}`.

Next steps

If you installed a Milestone network supported by the nmilestone driver, you may add a DVR and discover cameras. Milestone XProtect networks require additional configuration.

Creating the XProtect management server

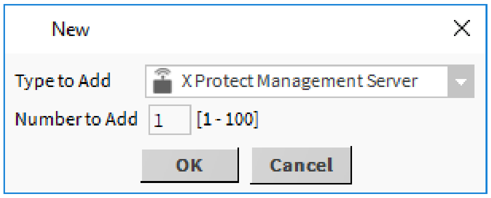
The XProtect management server supports access to a video network's NVR (Network Video Recorder) and cameras from a Supervisor PC or laptop. The XProtect Corporate product requires this management server to communicate with an NVR. This procedure sets up secure communication (Https) between the management server and station.

Prerequisites:
The XProtect management server is on line and ready to connect. Your PC or laptop is connected to the video network. You have admin privileges, are using Workbench, which is connected to a station with a MilestoneXProtectNetwork and the xprotect palette is open.

Step 1. To create the XProtect management server in the station, do one of the following:

- Drag an **XProtectManagementServer** component from the palette to the network component, double-click the new component and expand the **Connection** slot.
- Open the **X Protect Server Manager** view by double-clicking the **MilestoneXProtectNetwork** node in the Nav tree followed by clicking the **New** button at the bottom of the view.

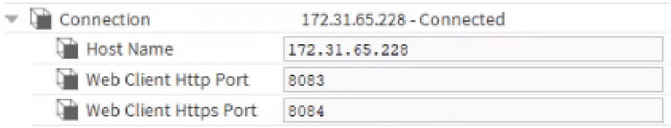
If you clicked the **New** button, the **New** window opens. If you expanded the **Connection** slot you see the connection properties.



New

Type to Add: X Protect Management Server

Number to Add: 1 [1 - 100]



Connection 172.31.65.228 - Connected

Host Name: 172.31.65.228

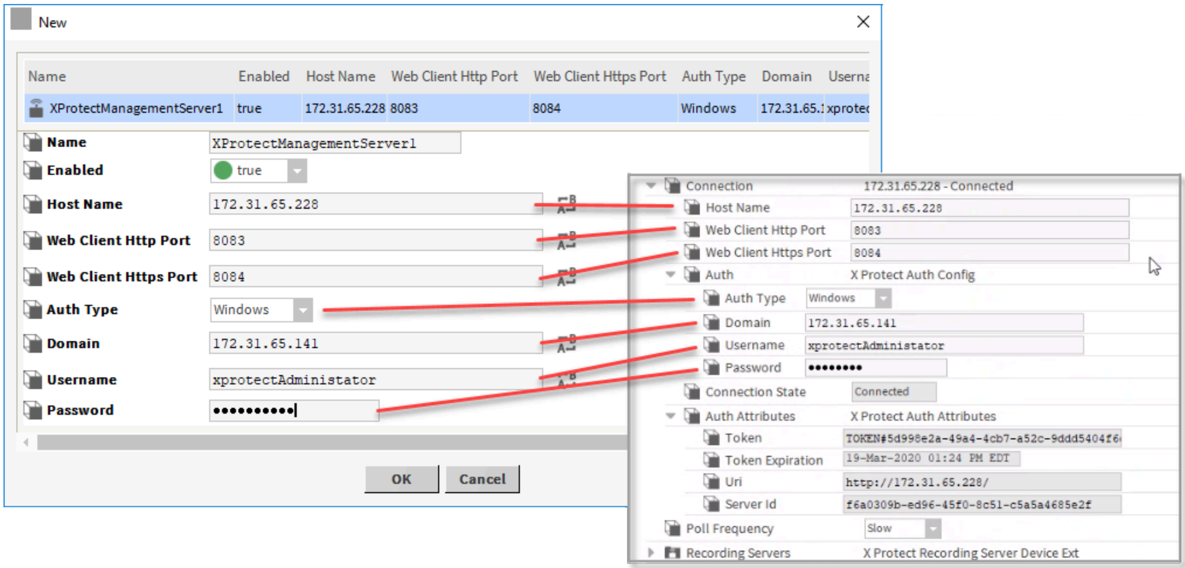
Web Client Http Port: 8083

Web Client Https Port: 8084

The **`Web Client Https Port`** must be different from the default.

Step 2. Optional: If you used the **New** button, you can change the name of the server and click **OK**.

A second **New** window opens.



Name	Enabled	Host Name	Web Client Http Port	Web Client Https Port	Auth Type	Domain	Userna
XProtectManagementServer1	true	172.31.65.228	8083	8084	Windows	172.31.65.1	xprotec

Name	XProtectManagementServer1
Enabled	true
Host Name	172.31.65.228
Web Client Http Port	8083
Web Client Https Port	8084
Auth Type	Windows
Domain	172.31.65.141
Username	xprotectAdministator
Password	●●●●●●●●●●

Connection	172.31.65.228 - Connected
Host Name	172.31.65.228
Web Client Http Port	8083
Web Client Https Port	8084
Auth	X Protect Auth Config
Auth Type	Windows
Domain	172.31.65.141
Username	xprotectAdministator
Password	●●●●●●●●
Connection State	Connected
Auth Attributes	X Protect Auth Attributes
Token	TOKEN#5d998e2a-49a4-4cb7-a52c-9ddd5404f6
Token Expiration	19-Mar-2020 01:24 PM EDT
Uri	http://172.31.65.228/
Server Id	f6a0309b-ed96-45f0-8c51-c5a5a4685e2f
Poll Frequency	Slow
Recording Servers	X Protect Recording Server Device Ext

The screen capture on the left represents the **New** window of the **MilestoneXProtectNetwork** component. The capture on the right shows the same properties after expanding the **XProtectManagementServer** > **Connection** component. These **Connection** properties enable communication between the management server and the station.

Step 3. For **Host Name** enter the IP address and for the **Web Client Https Port** enter the port number of the computer that hosts the management server.

Step 4. For the credentials, enter the **Username** and **Password** required by the Milestone corporate (management) server.

Step 5. For secure communication enter the **Web Client Https Port**.
If the management server uses fox streaming to deliver video, this port can be different from the port used by the platform/station to access the network. If the server does not use fox streaming, this port should be the same as the port that connects the platform/station to the network.

Step 6. To save the configuration, click **OK** or **Save**.
The framework attempts to connect to the server, but it fails because a secure connection via the native process bridge has yet to be established.

Configuring the mobile server

The web UI supports access to cameras and video streaming over the Internet. This access requires the installation and configuration of an XProtect Mobile Server in addition to the XProtect Management Server. When using the browser user interface, video streams via this server must be enabled and running.

Prerequisites:
This procedure assumes this is a new installation, and that you have installed in the trust store of each controller/station and camera, a certificate that was signed by a root CA certificate in the browser trust store.

If you recently downloaded and installed a Milestone X Protect Management Server, you also downloaded the XProtect Mobile Server installer.

Step 1. Install the XProtect Mobile Server on a separate PC.

Step 2. To edit this server's configuration file, use File Explorer to navigate to this path on your Windows computer:

Program Files\Milestone\Milestone Mobile Server

Step 3. Using a text editor, such as Notepad, open this file: `VideoOS.MobileServer.Service.exe.config`.

Step 4. Scroll down or search for this `HttpHeader` tag:

```
add key=”Access-Control-Allow-Origin” value=“*”/>*
```

This line indicates if the response can be shared with requesting code from the given origin. The asterisk (*) tells browsers to allow requesting code from any origin to access the resource. Another possibility is:

```
add key=”Access-Control-Allow-Origin” <origin>/>*
```

where you would replace `<origin>` with a single specific source: a hostname or constant IP address for a station that does not change.

Step 5. Save any changes you made and restart the XProtect Mobile Server.

Step 6. To verify that the mobile server is operational, use your browser to contact the server by entering the IP address and port number of the server’s PC:

`<ip address>:8081` or `https://<ip address>:8082`

These are the default ports for the XProtect Mobile Server.

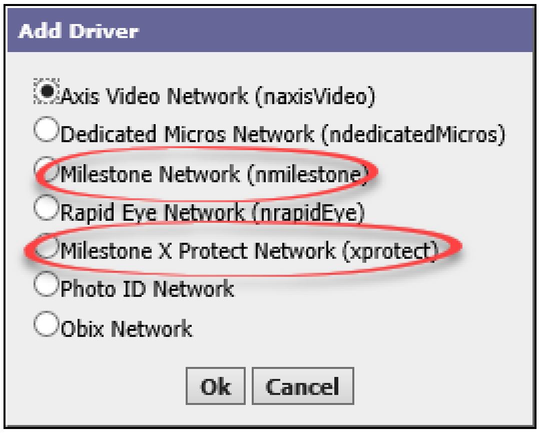
Using the web UI to install a Milestone network

Adding a network to a station is the first step for discovering cameras that are compatible with a Milestone system. While you can use the web UI to add a network, to ensure connectivity the preferred method for adding a network is to use Workbench, running it as an administrator.

Prerequisites:
The station is licensed for the nmilestone or xprotect driver. You are working in the web UI.

Step 1. From the main menu, click **Controller (System) Setup** > **Remote Devices** > **Remote Drivers**. The Remote Drivers view opens.

Step 2. Click the Manage Drivers button ( ), select the `Add` option and click **Ok**. The **Add Driver** window opens.



Add Driver

● Axis Video Network (naxisVideo)
○ Dedicated Micros Network (ndedicatedMicros)
○ Milestone Network (nmilestone)
○ Rapid Eye Network (nrapidEye)
○ Milestone X Protect Network (xprotect)
○ Photo ID Network
○ Obix Network

Step 3. Select the `Milestone` driver from the list and click **Ok**. The **Add Driver** window opens.

Step 4. Use the default driver name or change the name and click **Ok**.

Step 5. To check the network configuration, double-click the network row, confirm the configuration properties, and, if you change any, click **Save**.

The network status should report `{Ok}`.

Adding a Milestone DVR

A DVR (Digital Video Recorder) can include a camera and display.

Prerequisites:
You are connected to the remote host station. You are working in the web UI.

Step 1. From the main menu, click **Controller Setup** > **Remote Devices** > **Remote Drivers.**
The Remote Drivers view opens.

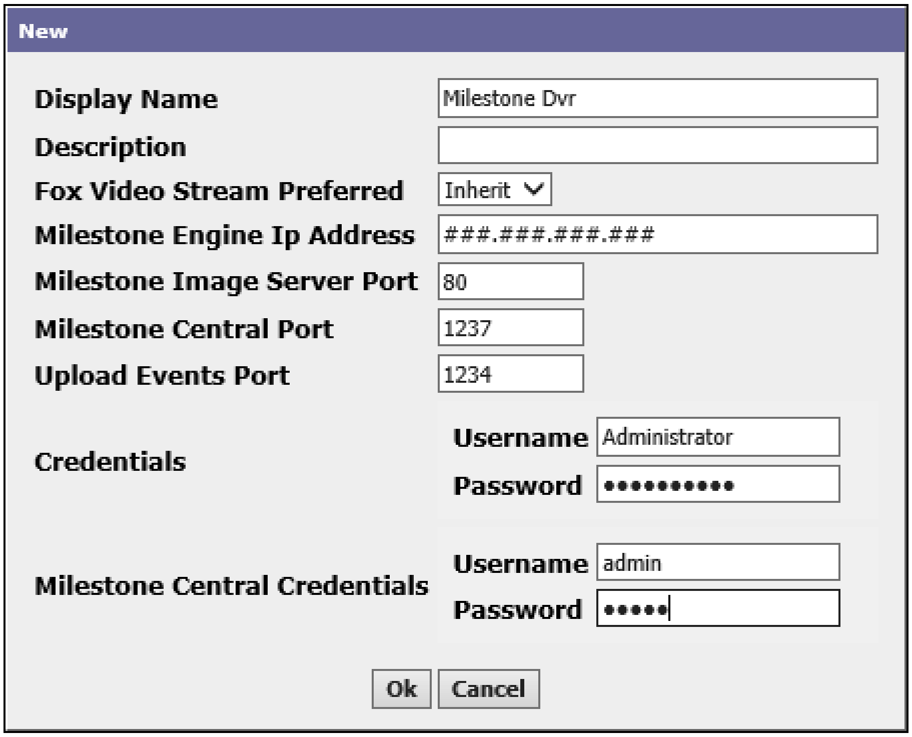
Step 2. Double-click on the `Milestone Network` row in the table.
The Driver Manager view opens with the Milestone Network tab selected.

Step 3. Click the DVRs tab.

Step 4. Do one of the following for the DVR:

- To edit the properties for an existing DVR, double-click the DVR row in the table or select the DVR and click the Edit button (
).
- To add a new DVR, click the **New** button (
).

For a new DVR, the **New** window opens.



New

Display Name	Milestone Dvr
Description	
Fox Video Stream Preferred	Inherit
Milestone Engine Ip Address	###.###.###.###
Milestone Image Server Port	80
Milestone Central Port	1237
Upload Events Port	1234
Credentials	Username: Administrator Password: ••••••••••
Milestone Central Credentials	Username: admin Password: •••••

Step 5. Enter at least these properties and click **Ok**:

- **`Milestone Engine Ip Address`** is the IP address for the DVR software.
- **`Credentials`** (**`Username`** and **`Password`**) are for accessing the DVR.
- **`Milestone Central Credentials`** (**`Username`** and **`Password`**) are for accessing the Milestone management server.

The **`Milestone Central Port`** connects the DVR to the network. If the DVR uses fox streaming to deliver video, this port can be different from the port used by the platform/station to access the network. If the DVR does not use fox streaming, this port should be the same as the port that connects the platform/station to the network.

Result

Adding a DVR adds the tabs (containers) for cameras and displays as well as adding the driver to the **Driver Manager** view.

Connecting a DVR to an XProtect server

An XProtect recording server provides IP video management software for large-scale, multi-site installations.

Prerequisites:

The driver has been added and configured. You are using the web UI.

Step 1. From the main menu, click **Controller Setup** > **Remote Devices** > **Remote Drivers.**
The Remote Drivers view opens.

Step 2. Double-click the **Milestone X Protect Network** row in the **Remote Drivers** table.

Step 3. Click the **DVRs** tab.
The **DVR** view opens.

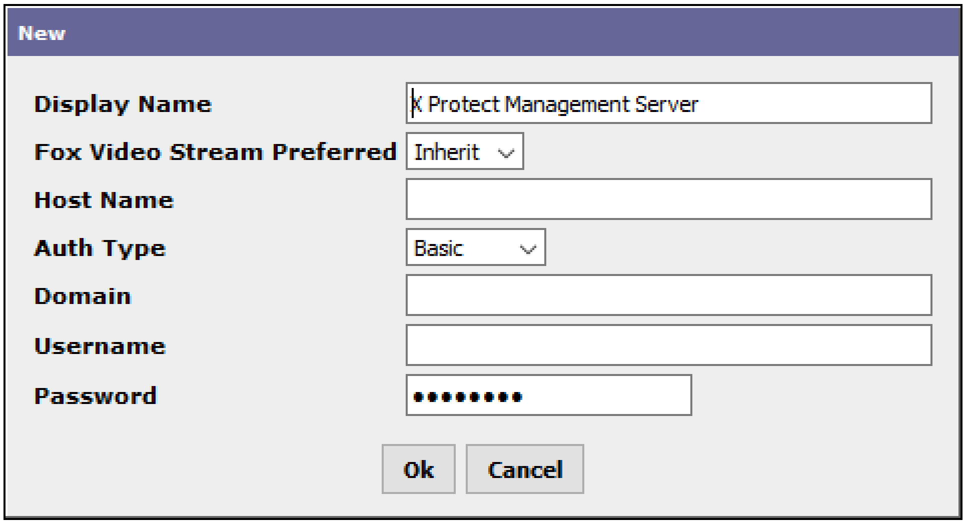
Step 4. Do one of the following:

- To edit the properties for an existing server connection, double-click the DVR row in the table or select the server row and click the Edit button (

).
- To connect a new DVR, click the **New** button (

).

The **New** window opens.

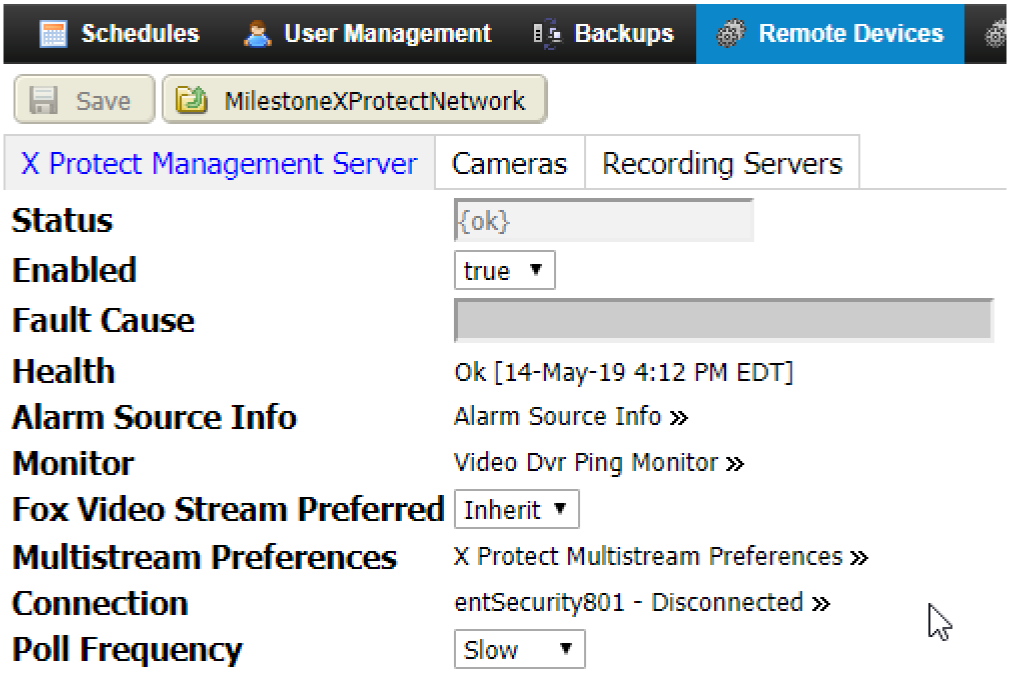


New

Display Name	X Protect Management Server
Fox Video Stream Preferred	Inherit
Host Name	
Auth Type	Basic
Domain	
Username	
Password	••••••••

Step 5. Enter the IP address for the remote controller in the **Host Name** property, select `Basic` or `Windows` for **Auth Type** and create supply credentials (**Username** and **Password**), and click **Ok**.

Step 6. Double-click the **X Protect Management Server** in the table.
The X Protect Management Server view opens with three tabs.



Status	{ok}
Enabled	true
Fault Cause	
Health	Ok [14-May-19 4:12 PM EDT]
Alarm Source Info	Alarm Source Info »
Monitor	Video Dvr Ping Monitor »
Fox Video Stream Preferred	Inherit
Multistream Preferences	X Protect Multistream Preferences »
Connection	entSecurity801 - Disconnected »
Poll Frequency	Slow

Notice that the **Connection** property shows "Connecting" and changes to "Connected."

Secure camera communication using a browser

A secure connection from a station to a camera connected to a DVR or NVR by means of a browser requires a server certificate in the camera that was signed by a root CA certificate in the browser's trust store.

If the server certificate in the camera is not signed by a recognized root CA certificate in the browser's trust store, you will need to connect using http:// to view video streams. This requirement is due to browser security.

NOTE: If you logged in to your station using https:// and you need to switch and log in with http:// instead, you must clear the browser cache to enable the login.

An https:// connection is always to be preferred. Before you discover cameras, make sure that each camera has a server certificate that was signed by a root CA certificate in the browser's trust store. The "System Security" chapter in this document explains how to generate server certificates and get them signed by a CA (Certificate Authority) as well as how to serve as your own CA.

Use the camera's configuration web page to install the signed server certificate in the camera.

Discovering cameras

This procedure is for discovering cameras when using the web UI.

Prerequisites:
The camera(s) is/are connected to a remote controller and are ready to discover. You are using the web UI and are connected to the station.

Step 1. From the main menu, click **Controller (System) Setup** > **Remote Devices** > **Remote Drivers.**
The Remote Drivers Manager view opens.

Step 2. Do one of the following:

- If you are using the nmilestone driver, double-click the `Milestone Network` row in the table and click the DVRs tab, and double-click a DVR row in the table.
- If you are using the xprotect driver, double-click the `X Protect Management Server` row in the table, click the DVRs tab, and double-click the `XProtectManagementServer` row in the table.

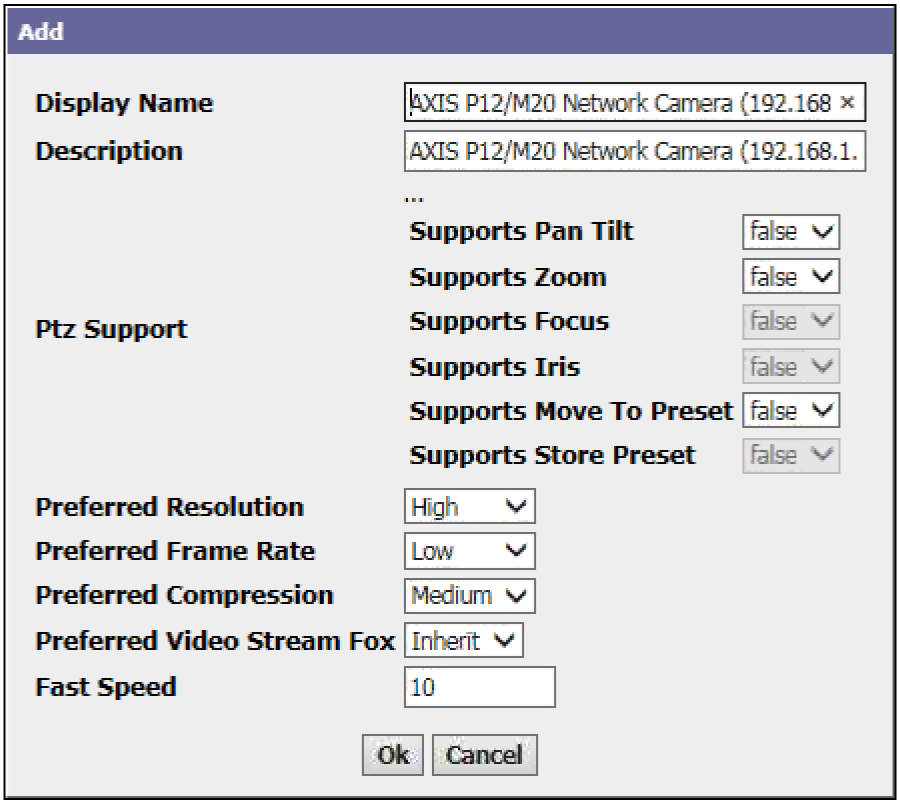
Step 3. Click the Cameras tab.

Step 4. Click the Discover button (🔍).
The system discovers the cameras.

Step 5. Select a camera in the Discovered pane, and click the Add button (⊕).
The system adds the discovered camera to the Database pane.

Step 6. To configure the camera, double-click its row in the table.

The **Add** camera window opens.



Display Name	AXIS P12/M20 Network Camera (192.168	
Description	AXIS P12/M20 Network Camera (192.168.1.	
	...	
Ptz Support	Supports Pan Tilt	false
	Supports Zoom	false
	Supports Focus	false
	Supports Iris	false
	Supports Move To Preset	false
	Supports Store Preset	false
Preferred Resolution	High	
Preferred Frame Rate	Low	
Preferred Compression	Medium	
Preferred Video Stream Fox	Inherit	
Fast Speed	10	

These properties depend on the camera. To understand the implications of making changes to camera properties, refer to the documentation for the camera.

Step 7. Check the configuration and click **Ok**.

Approving a camera self-signed certificate (Web UI)

If your browser permits self-signed server certificates, this procedure guides you to compare the `Issued By` and `Subject` properties of this certificate before you manually approve the connection.

Prerequisites:
You do not have a server certificate for the camera that was signed by a valid root CA certificate.

Step 1. Accept the self-signed certificate and make a connection to the camera.

Step 2. To locate the certificate do one of the following:

- Using the web UI, navigate to **Controller (System) Setup** > **Remote Devices** > **Certificate Management**.
- Using Workbench navigate to **Station** > **Services** > **PlatformServices** > **CertManagement**.

The station opens the **Certificate Management** view.

Step 3. To acknowledge the security warning, click **Allow** and click the Allowed Hosts tab.

Step 4. To open the certificate, select it and click **View**.
The **Host Exemption** window opens.

Step 5. Confirm that the certificate's `Issued By` and `Subject` properties contain names you recognize, and click **Ok**.

For a self-signed certificate, these properties should be the same. They should contain the name of the camera manufacturer or other identifiable text.

CAUTION: If you do not recognize the value of these properties, you may need to investigate with the camera manufacturer. This certificate authenticates the camera as a valid video server. Approving a bogus certificate opens your system to a man-in-the-middle attack.

Step 6. Assuming that the certificate is valid, and, if the certificate has not been approved yet, click **Approve** and respond to the confirmation window by clicking **Yes**.
The web UI's Camera Manager view lists the camera.

Discovering a recording server

A recording server is required to poll motion-detection events.

Prerequisites:
You have added the driver and X Protect Management Server. The X Protect Management Server tab on the **X Protect Management Server** view is open.

Step 1. Click the **Recording Servers** tab.

Step 2. Click the Discover button ( ).

Step 3. When the recording server(s) are discovered, click a server, and click the add button ( ).
The **Add** recording servers window opens.

Step 4. Make any changes to the `Display Name` and `Description` and click **Ok**.

Viewing live video

This procedure explains how to view a recorded video clip through the **Cameras** tab.

Prerequisites:
The xprotect driver and server have been added, cameras and recording servers found. The **X Protect Management Server** view is open.

Step 1. From the main menu, click **Controller Setup** > **Remote Devices** > **Remote Drivers**, double-click on the MilestoneXProtectNetwork row in the table, and click the DVRs tab.
The Server view opens.

Step 2. Double-click a server row and click the Cameras tab.
The view cameras opens.

Step 3. Click a camera row in the table.
The camera view opens with the X Protect Camera tab selected.

Step 4. Click the **Live View** button.
After a moment, the **live** view opens.

The first time you make the connection it may take a few seconds to open the live view.

Result
If you added a display, the resulting Surveillance Viewer lists the cameras displayed on the left side of the monitor.

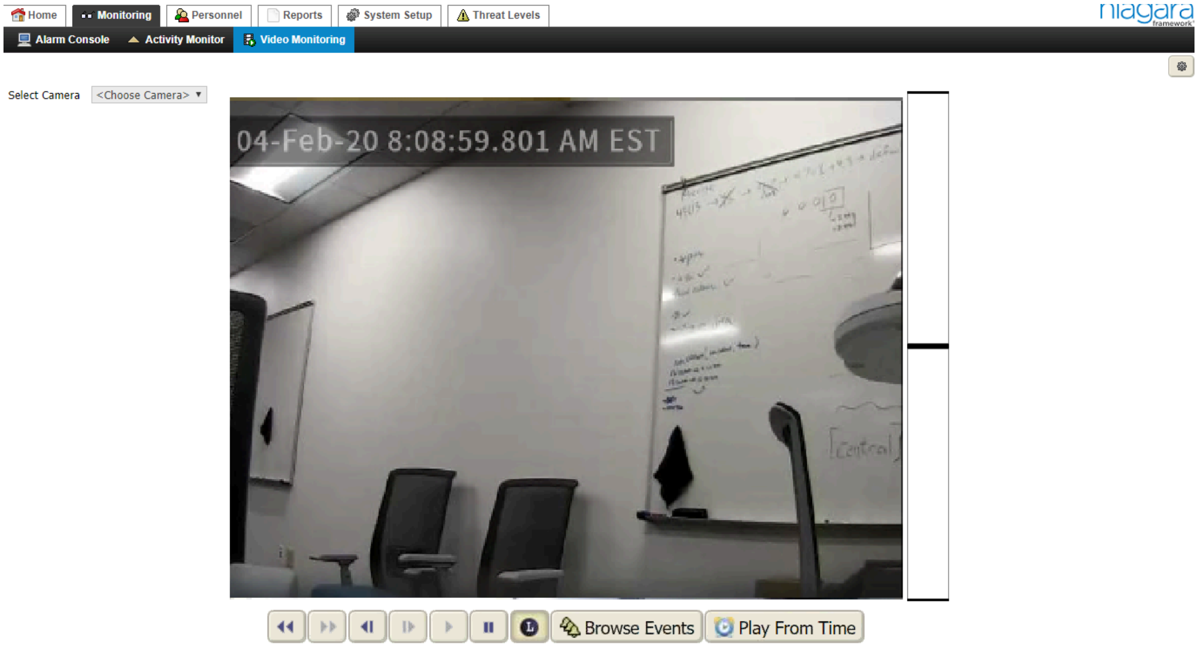
Playing back a recorded video

Using this procedure you can play back an HTML5–rendered video clip without leaving the alarm console recipient.

Prerequisites:
You have a Milestone DVR installed and configured. An alarm condition has been configured to report detected motion.

Step 1. On the main menu, click **Monitoring** > **Alarm Console**.
The **ConsoleRecipient - Snapshot** view opens.

Step 2. Click the **Playback View** button.
The most recently recorded video plays back.



Step 3. Do one of the following:

- To select a specific event for viewing, click the **Browser Events** button at the bottom of the window, select an event and click **View**.
- To start playback from a specific time, click **Play From Time**, select the time and click **OK**.

The saved video clip plays back.

Step 4. To return to the live view, click the Live button (Ⓛ).

Configuring motion-detected alarms

This procedure uses Workbench to set up and confirm HTML5 motion-detected alarms.

Prerequisites:
The xprotect driver and all video hardware is installed, discovered, configured and reporting a status of {ok}.

Step 1. Expand the video network down to the camera, double-click the **Events** node in the Nav tree and click the **Discover** button.

Step 2. To add the motion-detected event, select the discovered Motion Detected event type in the **Discovered** pane, click **Add** and **OK**.
The Motion Detected binary point moves to the **Database** pane.

Step 3. Open the alarm palette, expand the **Extensions** node, drag a BooleanChangeOfStateAlarmExt to the Motion Detected Boolean Point's Property Sheet, drop it on the component name and click **OK**.

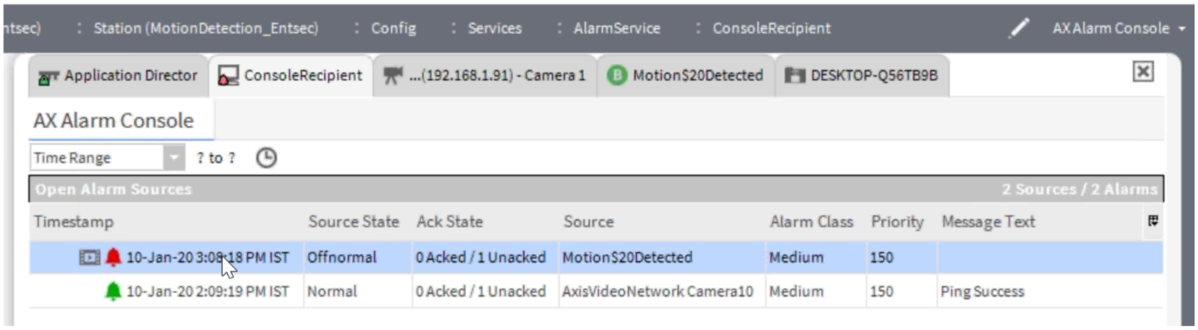
Step 4. Expand the extension, open the videoDriver palette, expand the **Alarm** node, drag a VideoAlarmExtParameters component to the BooleanChangeOfStateAlarmExt in the Property Sheet, drop it on the extension name and click **OK**.

Step 5. Scroll down to **`Meta Data`** and confirm that the Camera Ord has already been set.

Step 6. Scroll back up, double-click the **Recording Servers** node in the Nav tree, click **Discover**, add the recording server and ping it to ensure that it is connected and its **`Status`** reports `{ok}`.

Step 7. Create motion in front of the camera and confirm that the **`Out`** property changes to `true {alarm, unackedAlarm}`.
You may need to switch to the camera and ping the recording server again. The motion-detection recording may take some time.

Step 8. To confirm that the Alarm Console reports a motion-detected alarm, navigate to and expand the AlarmService in the Nav tree, double-click the ConsoleRecipient and confirm the alarm.



Timestamp	Source State	Ack State	Source	Alarm Class	Priority	Message Text
10-Jan-20 3:08:18 PM IST	Offnormal	0 Acked / 1 Unacked	Motion$20Detected	Medium	150	
10-Jan-20 2:09:19 PM IST	Normal	0 Acked / 1 Unacked	AxisVideoNetwork Camera10	Medium	150	Ping Success

Step 9. To confirm the alarm in the browser, log in to the system, click **Monitoring**.
The video icon (

) identifies the recorded clip associated with the motion-detection alarm.

Step10. To view the clip, use the check box to the left of the alarm row to select this alarm and click **Show Recurring** > **Review Video**.
The HTML5 video clip plays back.

About Maxpro network, camera and NVR configuration

The Maxpro driver supports both legacy devices that lack a secure video stream as well as newer cameras and NVRs that support TLS secure communication.

Through the web UI you can enable and disable a Maxpro network and configure its **`Alarm Source Info`**, **`Monitor`**, **`Tuning Policy`** and **`Fox Video Stream Preferred`** properties.

For video options in Workbench, refer to the *Niagara Video Framework Guide*.

Secure communication with video devices

By default, a Maxpro network provides TLS secure communication. If a camera or NVR on the Maxpro network does not support TLS, you will need to disable secure communication using Workbench and change the **`Http Port`** the device uses from 443 (secure) to 80 (not secure). You can change the **`Http Port`** using the web UI.

CAUTION: Be aware that the framework cannot prevent a flooding attack or other malicious activity if you must configure your devices without secure communication.

HTML5 streaming video

The Maxpro driver does not support HTML5 streaming. To support Maxpro devices, the browser requires the Web Launcher.

Installing a Maxpro network

Adding a network to a station is the first step for setting up a Maxpro video system.

Prerequisites:
The maxpro driver is licensed for this station and the driver's software modules are available.

Step 1. From the main menu, click **Controller (System) Setup** > **Remote Devices** > **Remote Drivers.**
The Remote Drivers view opens.

Step 2. Click the Manage Drivers button ( ), select the `Add` option and click **Ok.**
The **Add Driver** window opens.

Step 3. Select the `Maxpro` driver from the list and click **Ok.**
The **Add Driver** window opens.

Step 4. Use the default driver name or change the name and click **Ok.**

Step 5. To check the network configuration, double-click the network row, confirm the configuration properties, and, if you changed any, click **Save.**
The network status should report `{Ok}`.

Adding a Maxpro NVR

A Maxpro system with an NVR processes video data at the camera and streams it to the NVR.

Step 1. From the main menu, click **Controller Setup** > **Remote Devices** > **Remote Drivers.**
The Remote Drivers view opens.

Step 2. Double-click on the `Maxpro Network` row in the table.
The Driver Manager view opens with the Maxpro Network tab selected.

Step 3. Click the NVRs tab.

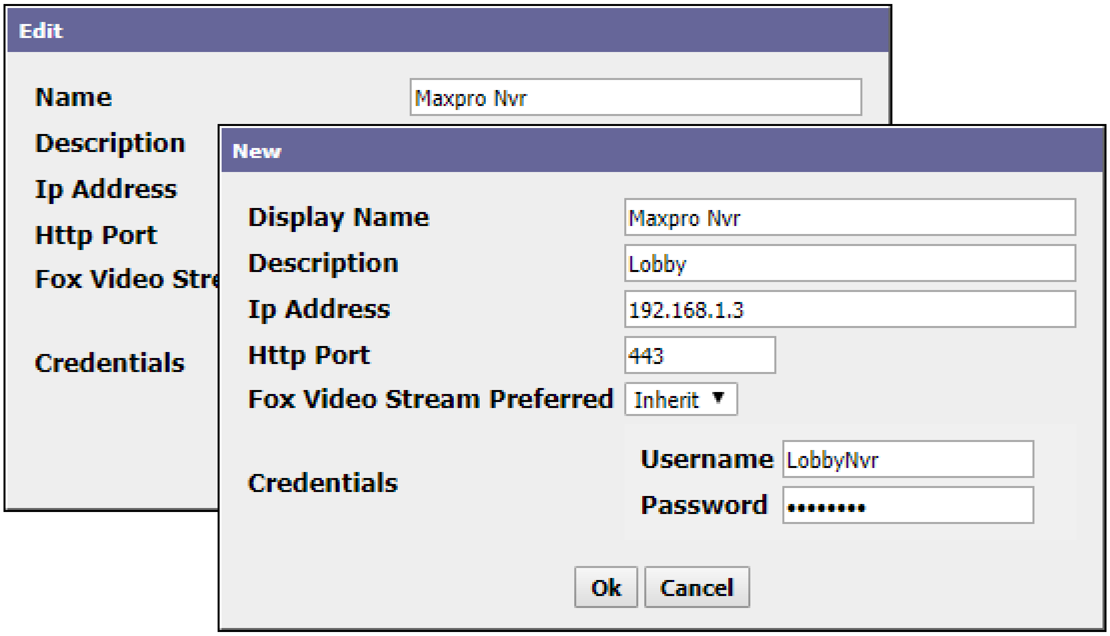
Step 4. Do one of the following:

- To edit the properties for an existing NVR, double-click the NVR row in the table or select the NVR and click the Edit button (

).
- To add a new NVR, click the NVRs tab.

Step 5. To continue adding a NVR, click the New button ( ), select the NVR from the drop-down list, name it, and click **OK.**

The **New** window opens.



Edit

Name: Maxpro Nvr

Description

Ip Address

Http Port

Fox Video Stre

Credentials

New

Display Name: Maxpro Nvr

Description: Lobby

Ip Address: 192.168.1.3

Http Port: 443

Fox Video Stream Preferred: Inherit ▼

Credentials: Username: LobbyNvr; Password: ••••••••

Step 6. Enter at least these properties and click **Ok**:

- **`Ip Address`** is the IP address for the NVR software.
- **`Credentials`** (**`Username`** and **`Password`**) are for accessing the NVR.

CAUTION: Do not change the **`Http Port`** to 80 unless you are setting up an NVR that does not support TLS secure communication. If port 80 is required, you must also turn off **`Use Tls`** using Workbench. Disabling secure communication leaves your Maxpro network vulnerable to a malicious attack.

If the NVR uses fox streaming to deliver video, the **`Http Port`** can be different from the port used by the platform/station to access the network. If the NVR does not use fox streaming, this port should be the same as the port that connects the platform/station to the network.

Result

Adding an NVR adds the tabs (containers) for cameras as well as adding the driver to the **Driver Manager** view.

Adding (or editing) a Maxpro camera

Adding a camera may involve approving its certificate as well as configuring its communication properties. This procedure adds a camera manually. Migrated installations list all existing cameras without the need to manually add the cameras.

Prerequisites:

You are connected to the remote host station that controls the camera using the web UI. The Maxpro network and NVR have been set up, configured and the health of each reports `Ok`. If the camera does not support TLS secure communication, you must have used Workbench to disable Use Tls and changed the Http Port address to 80. You cannot change these properties through the web UI.

Step 1. From the main menu, click **Controller Setup** > **Remote Devices** > **Remote Drivers.**
The Remote Drivers view opens.

Step 2. Double-click on the Maxpro Network row in the table.
The Driver Manager view opens with the Maxpro Network tab selected.

Step 3. Double-click on the Maxpro NVR row in the table.

The NVR Manager view opens with the Maxpro NVR tab selected.

Step 4. Click the Cameras tab.
The Camera Manager view opens.

This view displays a list of any existing cameras.

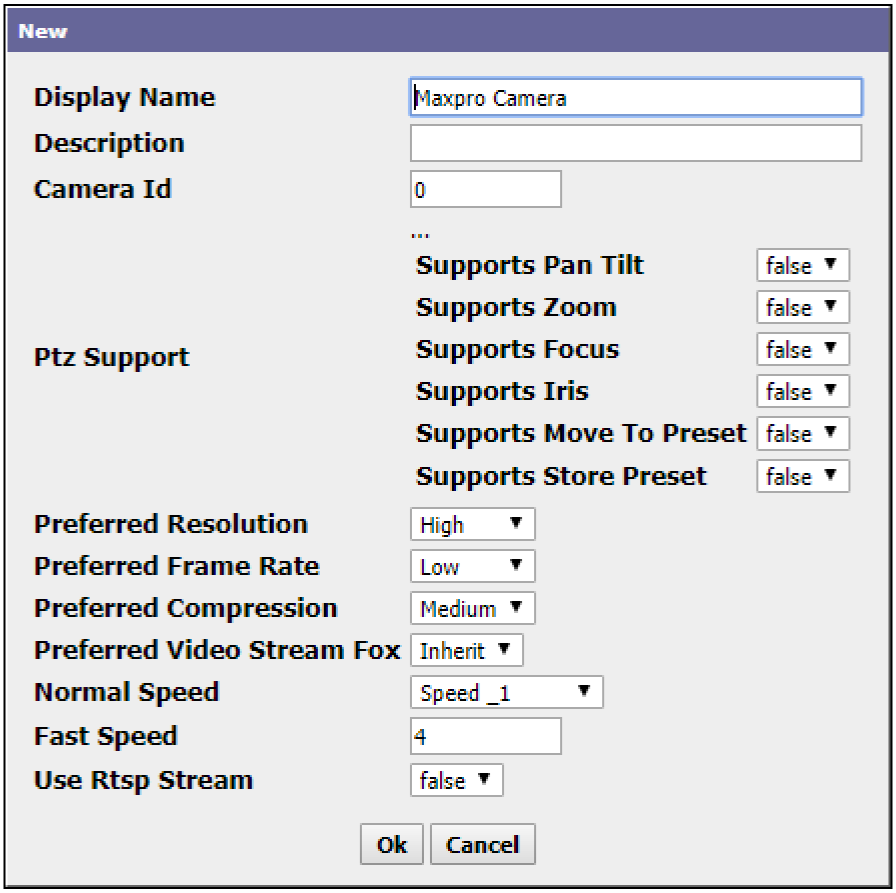
Step 5. Click the Discover button ( ) or do one of the following:

- To edit the properties of an existing camera, double-click the camera row in the table or select the camera and click the Hyperlink button (

).
- To manually add a Maxpro camera manually, click the New button (

).

The **New** window opens.



New

Display Name	Maxpro Camera	
Description		
Camera Id	0	
	...	
Ptz Support	Supports Pan Tilt	false ▼
	Supports Zoom	false ▼
	Supports Focus	false ▼
	Supports Iris	false ▼
	Supports Move To Preset	false ▼
	Supports Store Preset	false ▼
Preferred Resolution	High ▼	
Preferred Frame Rate	Low ▼	
Preferred Compression	Medium ▼	
Preferred Video Stream Fox	Inherit ▼	
Normal Speed	Speed _1 ▼	
Fast Speed	4	
Use Rtsp Stream	false ▼	

Step 6. Give the camera a **Display Name, and optional Description**; enter its **Camera ID** (usually an IP address).

The Maxpro driver supports TLS secure communication by default.

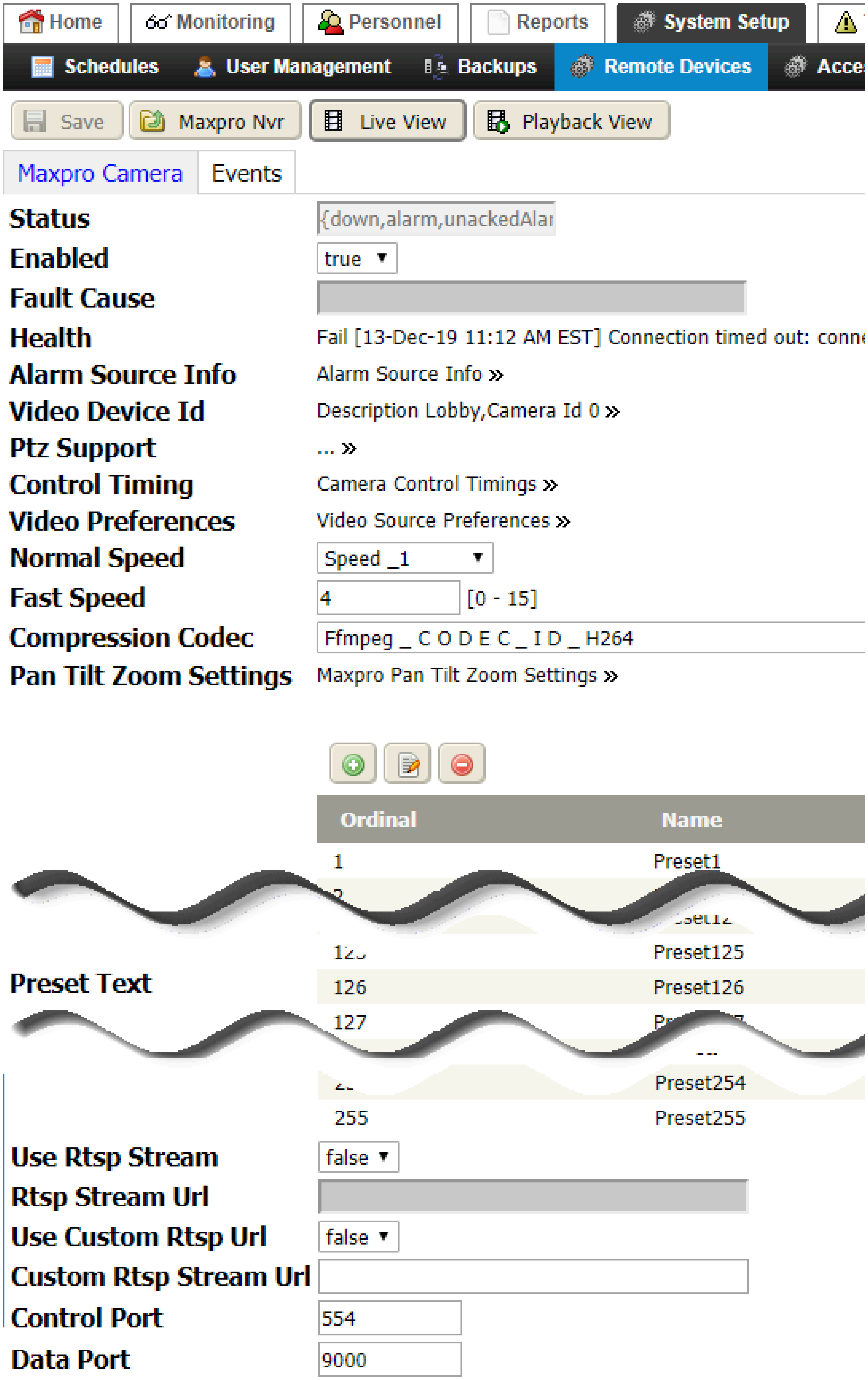
NOTE:

If your application requires RTSP and you change **`Use Rtsp Stream`** to `true`, the channel will not connect unless you already disabled TLS secure communication in Workbench.

Step 7. To use RTSP streaming, set **`Use Rtsp Stream`** to `true` and click **Ok**.
The system saves the configuration to the station database.

Step 8. Once the camera is set up, to view its properties, navigate back to **Controller Setup** > **Remote Devices** > **Remote Drivers** double-click the Maxpro Network row; double-click the NVR row, click the Cameras tab; and double-click the camera row in the table.

The system opens the Maxpro Camera tab.



Status	{down,alarm,unackedAlar
Enabled	true
Fault Cause	
Health	Fail [13-Dec-19 11:12 AM EST] Connection timed out: conne
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 »

Preset Text

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

Use Rtsp Stream	false
Rtsp Stream Url	
Use Custom Rtsp Url	false
Custom Rtsp Stream Url	
Control Port	554
Data Port	9000

Status should be `{ok}`.

Step 9. If **`Status`** is not `{ok}`, confirm that the **`Compression Codec`** is appropriately configured for the camera, and, if necessary, change this property and click **Save**.

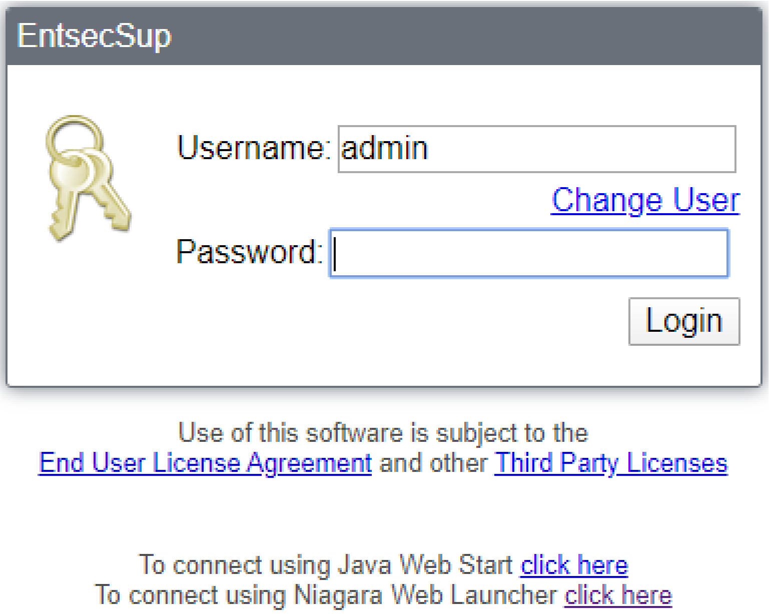
- For a secure Https connection between the camera and station, the CODEC should be: MPEG4 (Ffmpeg_CODEC_ID_MPEG4).
- For an RTSP connection between the camera and station, the CODEC should be: H264 (Ffmpeg_CODEC_ID_H264).

Playing back Maxpro-recorded video

The Maxpro driver does not support HTML5. Viewing videos recorded using the Maxpro driver requires the Web Launcher and Java applet. This goes for all the video-related views including live view, playback view, remote video views, and motion-detected video alarms.

Prerequisites:
You have one or more video clips recorded using the Maxpro driver.

Step 1. Open your browser and enter the station's IP address in the Address field at the top of the browser.
The Login window opens.



Username: admin

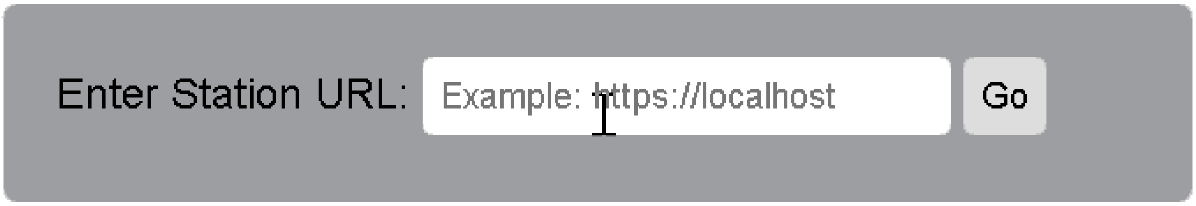
Password:

Use of this software is subject to the
End User License Agreement and other Third Party Licenses

To connect using Java Web Start click here
To connect using Niagara Web Launcher click here

Step 2. Click the link below the window that reads, "To connect using Niagara Web Launcher click here."

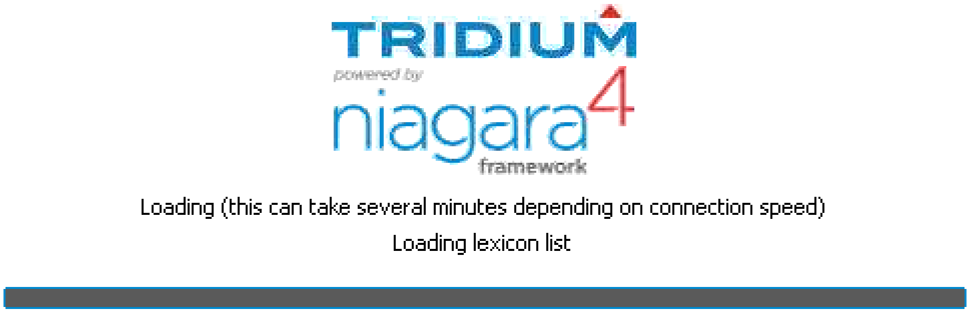
It may take a while for the Web Launcher to load and open a window for entering the station's URL.



If you see an error message, click the browser's back button.

Step 3. Enter the IP address in this box, click **Go**, enter the password in the login window and click **Login**.
The web UI opens supported by the Web Launcher.

Step 4. Click **Controller (System) Setup** > **Remote Devices** > **Remote Drivers**
The software opens the applet view followed by the video view.



Loading (this can take several minutes depending on connection speed)

Loading lexicon list

This works for both the Surveillance and Playback viewers.

Using the applet to play back applet-rendered videos

You may use the Niagara Web Launcher and Java applet to play back applet–rendered video clips associated with alarms.

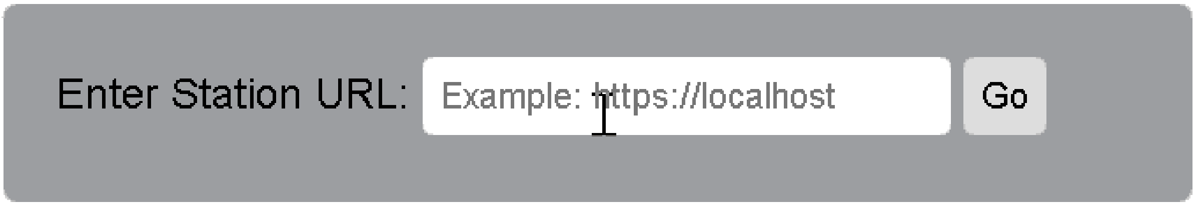
Prerequisites:
The applet–rendered video clip already exists.

The HTML5 Alarm Console is not available using Web Launcher.

Step 1. Open your browser and enter the station's IP address in the Address field at the top of the browser.
The Login window opens.

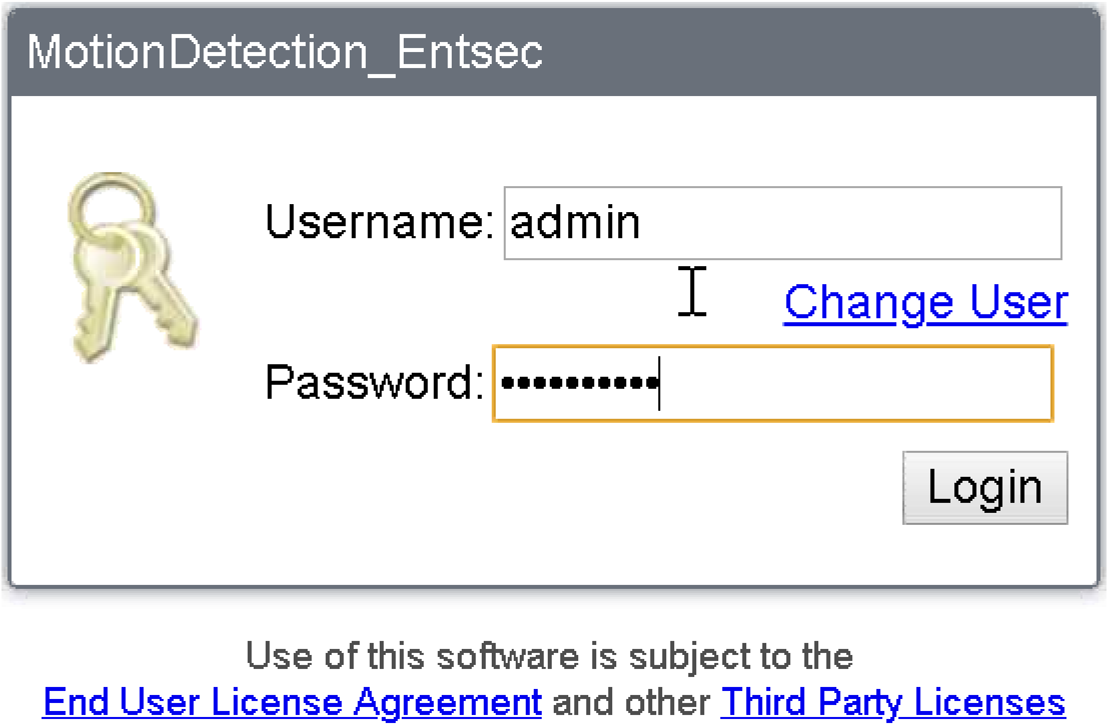
Step 2. Click the link below the window that reads, "To connect using Niagara Web Launcher click here."

It may take a while for the Niagara Web Launcher to load and open a window for entering the station’s URL.



If you see an error message, click the browser’s back button.

Step 3. Enter the station’s IP address in this box and click **Go**
A different login window opens.



Username: admin

Password: ••••••••••

Use of this software is subject to the End User License Agreement and other Third Party Licenses

Step 4. Enter the station password and click **Login**.
The web UI opens supported by the Web Launcher.

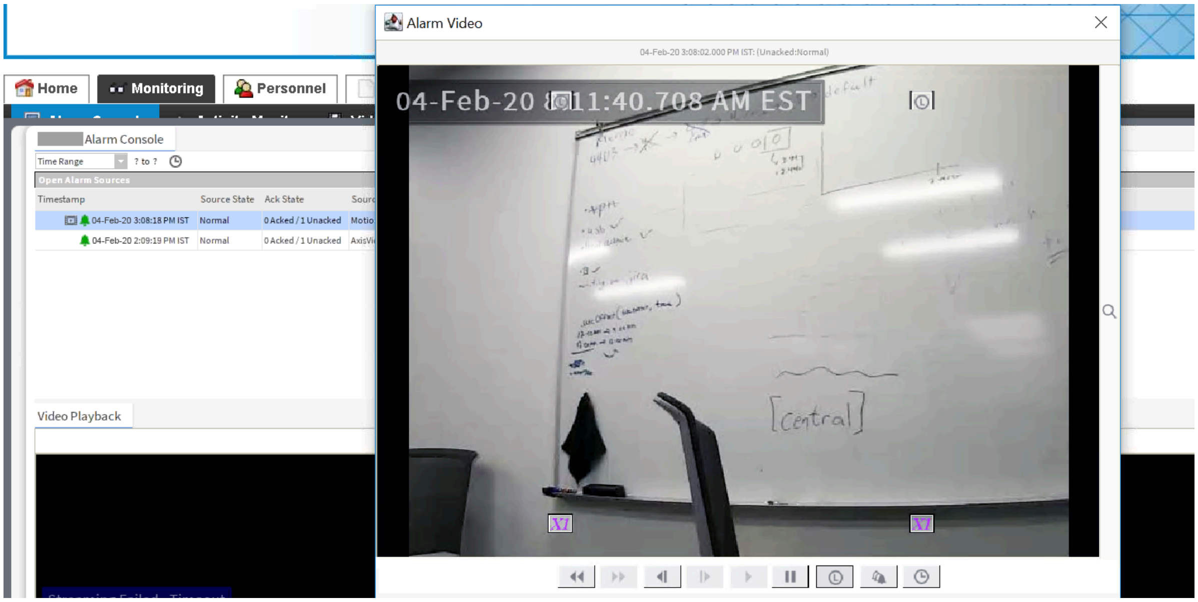
Step 5. Do one of the following:

- Click **Monitoring** > **Alarm Console**.
- Click **System Setup** > **Alarm Setup**, click **Alarm Consoles**, double-click the **ConsoleRecipient** row in the table, and click the **View Alarm Console** button.

The applet loads (this may take a bit of time) and opens its Alarm Console view. Both access methods load the same applet-based Alarm Console.

Step 6. Double-click the motion-detected alarm row in the table.

A pop-up window opens with the recorded video.



04-Feb-20 3:08:02.000 PM IST: (Unacked:Normal)

Timestamp	Source State	Ack State	Sourc
04-Feb-20 3:08:18 PM IST	Normal	0 Acked / 1 Unacked	Motio
04-Feb-20 2:09:19 PM IST	Normal	0 Acked / 1 Unacked	AxisVi

The screen capture shows the applet Alarm Console with an open video clip.

Chapter 13. 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.

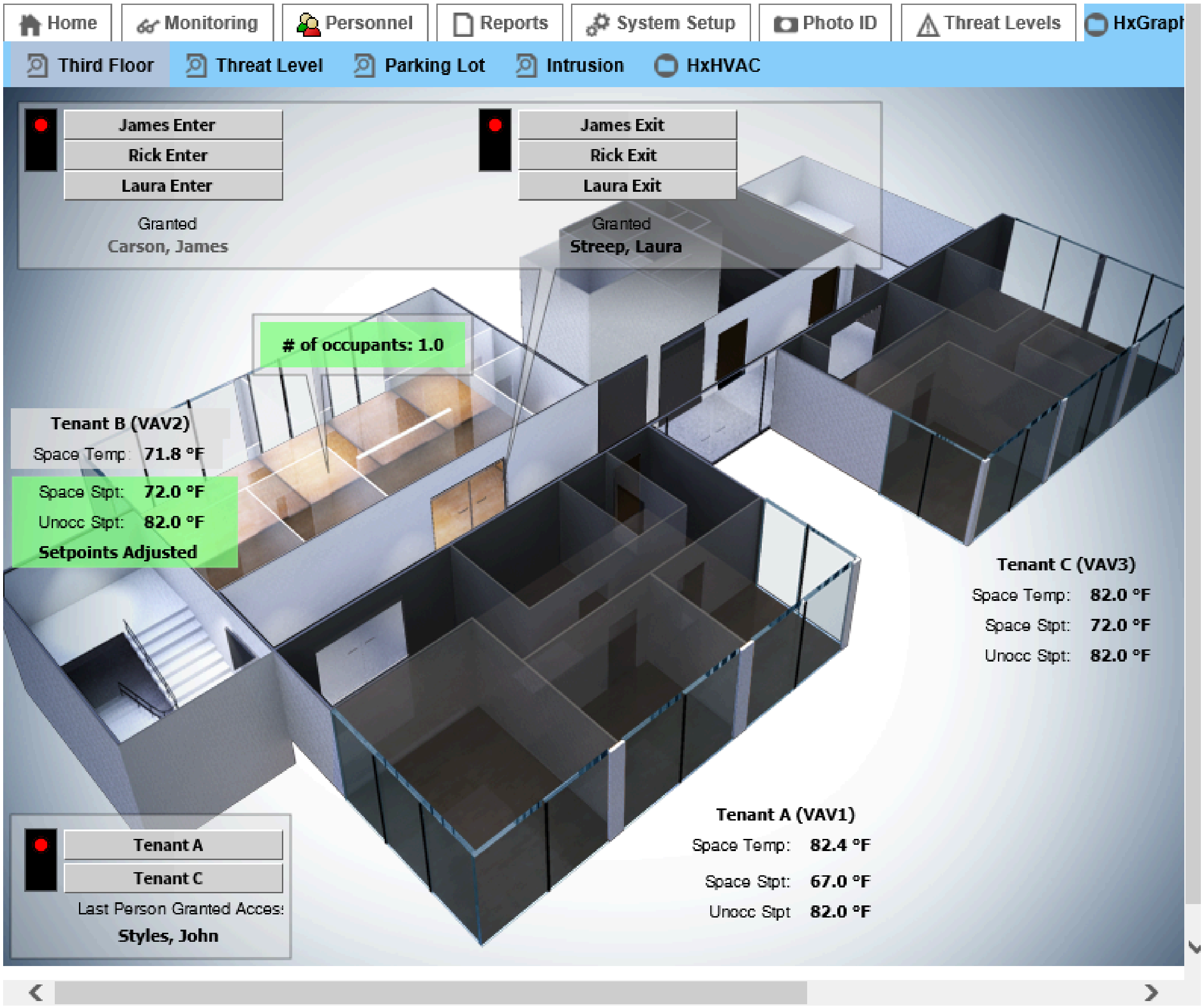
Consider carefully the basic capabilities and limitations of each technology. Obviously, a mobile phone is limited as to what it can usably display when compared to a graphic viewed in a web browser running on a computer. Keep this in mind, and test your views in all target media as you develop them.

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 34. A 3D image of a floor in a building



Granted
Carson, James

Granted
Streep, Laura

# of occupants: 1.0

Tenant B (VAV2)
Space Temp: 71.8 °F
Space Stpt: 72.0 °F
Unocc Stpt: 82.0 °F
Setpoints Adjusted

Tenant C (VAV3)
Space Temp: 82.0 °F
Space Stpt: 72.0 °F
Unocc Stpt: 82.0 °F

Tenant A (VAV1)
Space Temp: 82.4 °F
Space Stpt: 67.0 °F
Unocc Stpt 82.0 °F

Last Person Granted Acces:
Styles, John

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.

Creating a view using Workbench

While you can use the Graphic Editor, which is available in the web user interface (web UI), it is often preferable to create graphics using Workbench. This is especially true for more complex graphics. This procedure creates a graphic that can be accessed via user roles and, using Web Launcher, can be accessed from the web UI.

Prerequisites:
You are working in Workbench on a Supervisor PC

Step 1. Right-click the **Config** folder, click **New** > **Folder**, and give the folder a name, such as **Customized Views.**

Step 2. Create another folder within the **Customized Views** folder and name it for the view, such as Main Floor, Lobby, etc.

Step 3. Right-click the folder for the view and click **Views** > **New View**.
The **New Px View** window opens with the folder name as the default **`View Name`**.

As expected when using the Workbench interface, **`Target Media`** defaults to `WorkbenchPxMedia`. These media are designed for the Workbench interface. Since they do not work in a browser, they require Web Launcher when viewed in the web UI.

Step 4. Give the view a name, such as Main Floor, Lobby, etc. and click **OK**.
The software creates a `.px` file for the view and opens a blank canvas.

Step 5. Open the videoDriver palette, expand the **Px** folder and drag a widget to the Px Editor canvas.
The side bars populate.

- A bound Object Resolution Descriptor (ORD) connects the widget to a specific device slot (object).
- 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 widget type.

NOTE: Binding options that are dimmed indicate invalid options for the selected component.

Step 6. Configure options and click **OK**.
The Secondary view area displays properties and options that are related to the selected Source option.

Step 7. To bind additional widgets, repeat this procedure.

Step 8. To check how your view looks, click the Toggle View/Edit Mode: Hyperlink to Px Editor button (✎) or click the name of the view in the Nav tree.
This button toggles between the finished view and the Edit view.

Result

Refer to the *Niagara Graphics Guide* for more information about how to create and manipulate widgets.

Creating a new graphic view using the web UI

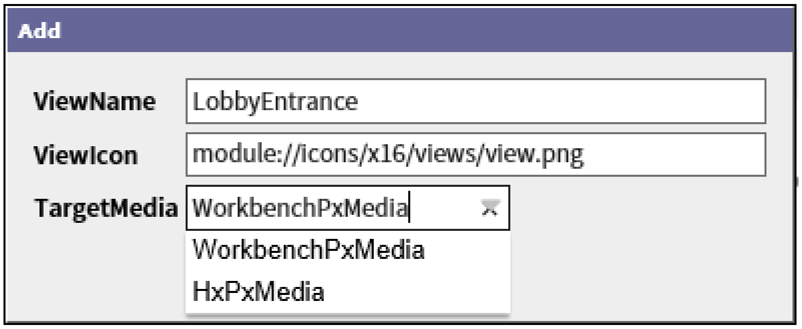
This procedure describes how to use the web UI to create a graphic view that displays current room (access zone) occupancy and temperature information.

Prerequisites:
You are working in the web UI. You have an appropriate graphic image to represent the building.

You can create graphics in many ways, depending on your resources, your skill level and what you are starting with. For example, if you already have a graphic page for building controls, you may add access information to an existing page. In other cases, you may create a new page from the start. One general process for creating a new graphic is outlined below with detailed steps following.

Step 1. Navigate to **Controller (System) Setup** > **Miscellaneous** > **Graphics** > **Graphics Management.**.

Step 2. Click the Add button (⊕).
The Add graphic window opens.



ViewName: LobbyEntrance

ViewIcon: module://icons/x16/views/view.png

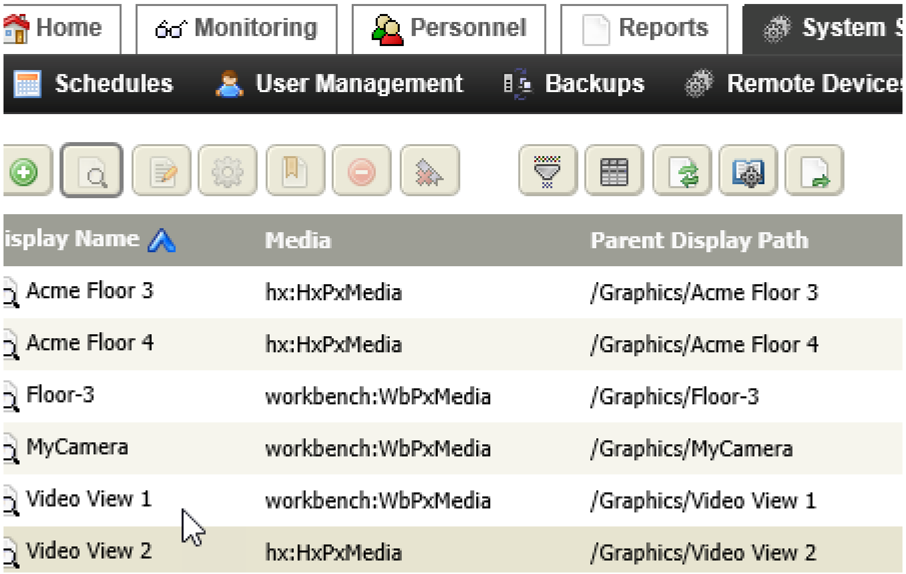
TargetMedia: WorkbenchPxMedia

`TargetMedia` defaults to `WorkbenchPxMedia`. These provide the richest visual experience, but may not be appropriate depending on the device (phone, tablet, computer).

`HxPxMedia` are designed for the web UI. 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.

Step 3. Give the graphic a name, select `HxPxMedia` for **`TargetMedia`**, and click **Ok**.

The system creates the graphic file in the station and displays the Graphics Management view with the new graphic page listed.

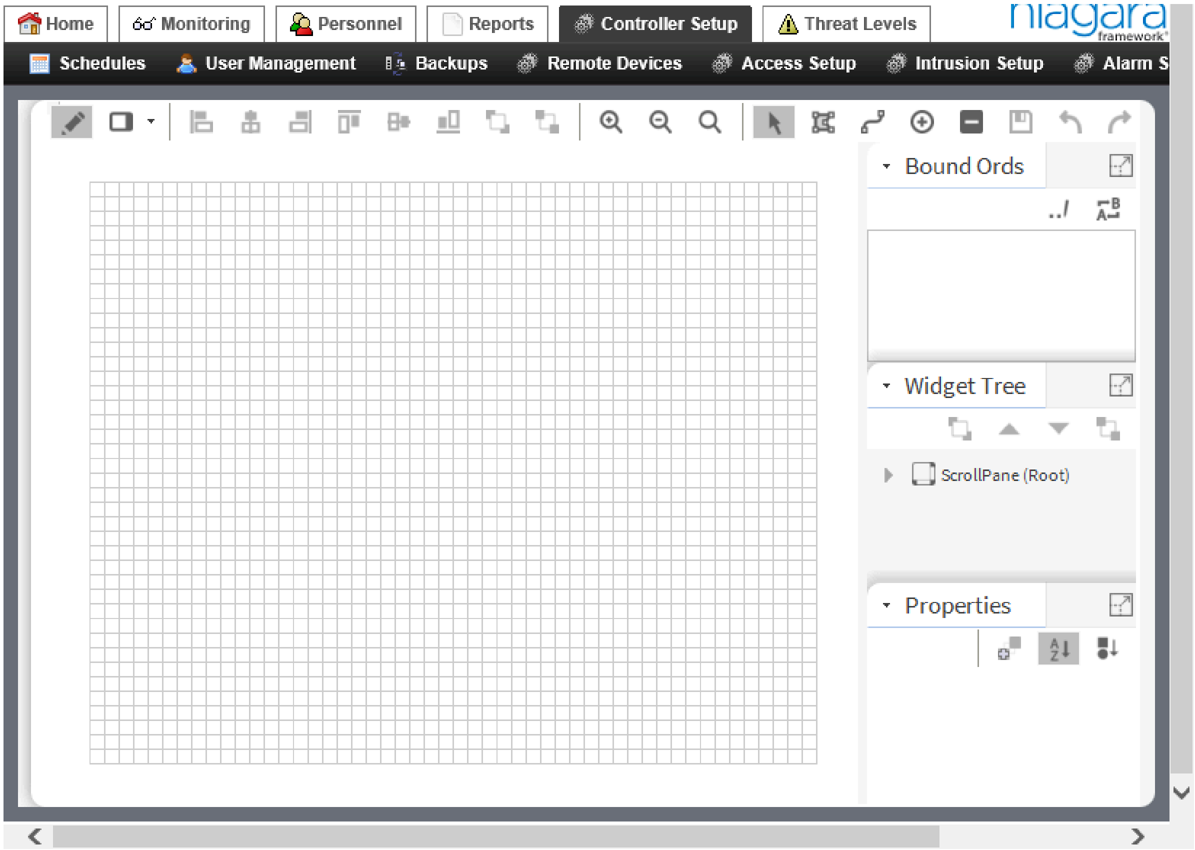


isplay Name	Media	Parent Display Path
Acme Floor 3	hx:HxPxMedia	/Graphics/Acme Floor 3
Acme Floor 4	hx:HxPxMedia	/Graphics/Acme Floor 4
Floor-3	workbench:WbPxMedia	/Graphics/Floor-3
MyCamera	workbench:WbPxMedia	/Graphics/MyCamera
Video View 1	workbench:WbPxMedia	/Graphics/Video View 1
Video View 2	hx:HxPxMedia	/Graphics/Video View 2

Step 4. Select the graphic you just created and click the Graphic Editor button (📝).
The browser may prompt you to continue even though the certificate presented by the station cannot be validated.

Step 5. Click **Continue**.

A blank Graphic Editor view opens.



The side bars configure:

- A bound Object Resolution Descriptor (ORD) connects the widget to a specific device slot (object).
- Properties populate based on the widget type.

Step 6. Add a background using an image that you have prepared previously — such as a floor plan.

a. Double-click in the middle of the CanvasPane to open the CanvasPane properties window.

b. In the CanvasPane properties window, use the background property field to select `Image` from the drop down option list and browse through the **Image Brush Editor** (use the `File Ord Chooser`) and **File Chooser** windows to select the desired image file, as shown below.

c. Click the **Open** button and then click **OK** to close all the windows and complete the insertion of the image on the graphic view.

The background image displays on the page.

Step 7. Add a widget.

If you selected `HxPxMedia` for **`Target Media`** and you attempt to drop a widget from the palette that requires the Web Launcher, the system displays, “Are you sure you want to create this widget?” Media Validation for “HxPx Media” found these problems:” A widget ORD follows.

Step 8. If you got the error message, click **Yes**.

The software creates the widget, but it works only in Workbench.

Result

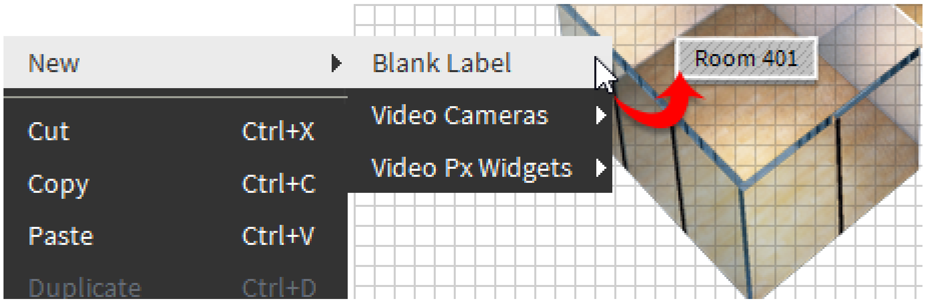
Refer to the *Niagara Graphics Guide* for more information about how to create and manipulate the graphics widgets.

Adding information to a graphic view

You can use labels to display information, such as images, static text, and dynamic information on your graphic page.

Prerequisites:
The graphic view is available from the web UI and the information to add is available to the station to which you are connected.

Step 1. Add a label by right-clicking on the canvas pane and selecting **New** > **Blank Label**. You can use the label properties palette to add text and formatting, as desired.
The image below shows static text used as a room label ("Room 401"). The label properties are edited to supply the text, a border and background shading.



Step 2. Add dynamic information (such as room temperature or occupancy count) to the graphic page by doing the following.

NOTE:

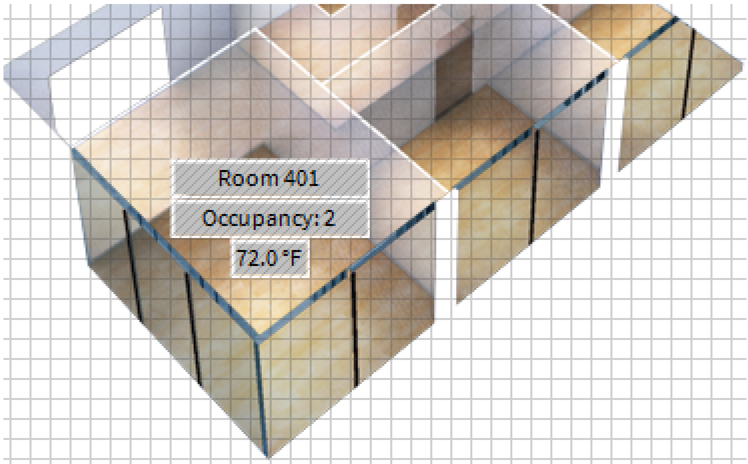
Adding dynamic information requires that you have information values (such as numeric point values) available in your station logic so that you can bind that information to a widget on the graphic view.

a. Add a new label, and then in the label's Properties window, click the Add Binding button ( ). Select `bajaui:Value Binding` in the ord property, then browse to connect the ord property to a desired control point in the station and click **OK**. With the ord connected, the value is now available to be assigned to the label text property field.
As an example, you may have some logic in your station that calculates room occupancy based on door entry and exit values. You can connect this field to the numeric point that has that information and display it in the label.

b. To display the bound value in the label, right-click inside the text property, choose **Animate** from the popup menu to display the **Animate** window, as shown below.

Use the BFormat field (Format) to designate the desired dynamic value and click **OK**.

The graphic now has a label and dynamic value that displays changing information such as occupancy or room temperature.

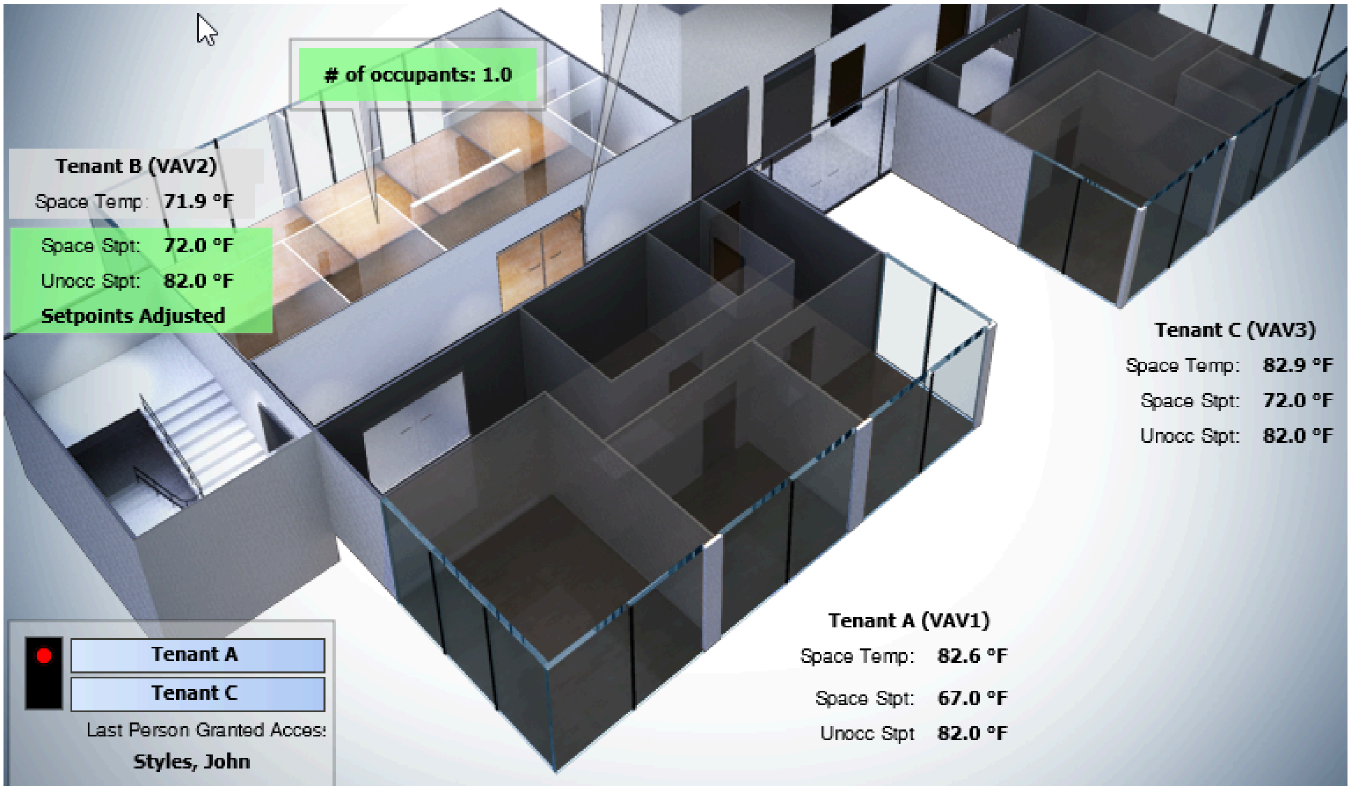


Step 3. To save your changes, click the Save button (💾) on the toolbar at the top of the view.

Result

The graphic page displays values with updates.

Following is an example of a page that has more information.



Adding video to a graphic

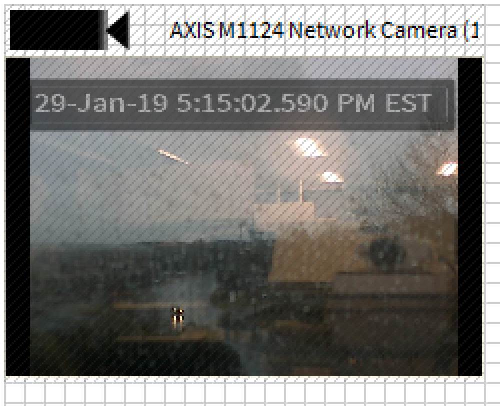
You can add live video or playback recorded video on a graphic page. This task describes how to add a live video camera to an existing graphic page.

Prerequisites:
You are working in the web UI. The graphic already exists.

Step 1. Navigate to **Controller (System) Setup** > **Miscellaneous** > **Graphics** > **Graphics Management**..
The Graphics Management view displays the list of graphics.

Step 2. Select the graphic and click the Graphic Editor button (📝).
The Graphic Editor view opens with the graphic in the editor.

Step 3. Right-click on the CanvasPane and select **New** > **Video Cameras** > **Your Video Camera.**
The video camera is added to the graphic.



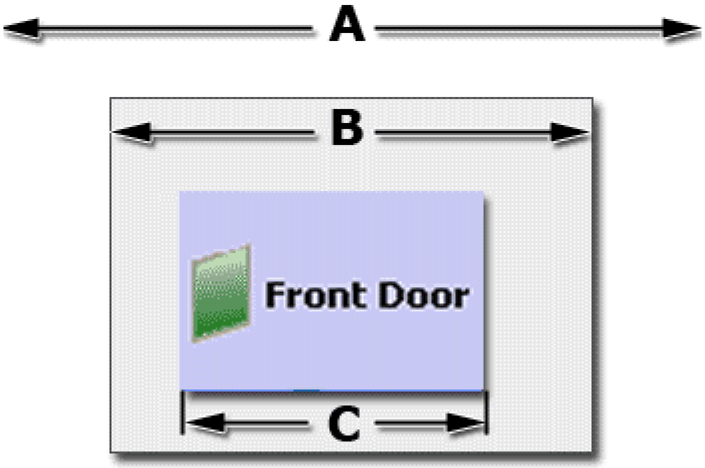
Step 4. To save your changes, click the Save button (💾).

Widget layout

Widgets are components that provide graphic visualizations. You use the Graphic Editor to define user interface functions for control and information display. An example of a widget is the label, which you can add to a graphic for the purpose of annotating the drawing.

NOTE: If either of the child objects is positioned outside of the view area of the parent, the system crops them and only the part within the parent is visible.

Figure 35. Front Door widget in context

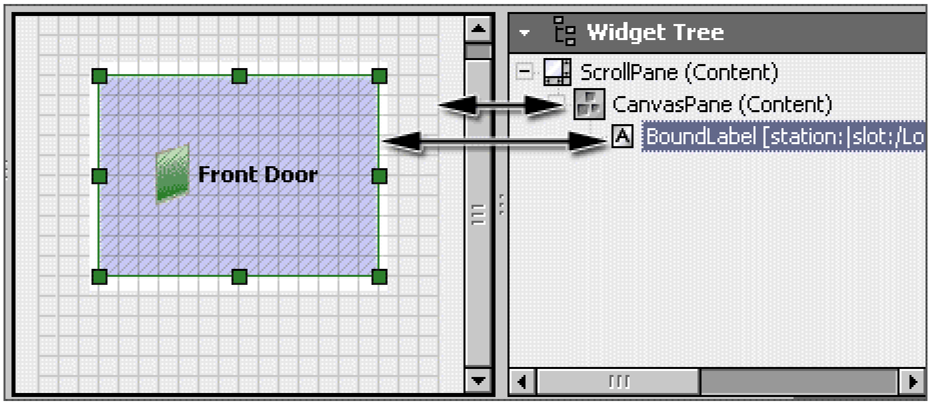


The screen capture shows a simple layout of a widget (C), held by the parent canvas (B) that is the child object of the scroll pane (A).

Widget panes

Some widgets are designed specifically to be container widgets that hold other widgets. These widgets are called panes.

Figure 36. Pane hierarchy in the widget tree



The screen capture shows the pane hierarchy in the widget tree and on the Graphic Editor canvas. Different types of panes provide different functions.

Table 26. Types of panes

Type of pane	Description
CanvasPane	This pane is used for absolute positioning.
BorderPane	This pane is used to wrap one widget and provide margin, border, and padding similar to the CSS box model.
ScrollPane	This pane supports a single child that may have a preferred size larger than the available bounds. The scroll pane provides a set of scroll bars for viewing areas of the child widget that go outside of its bounds.

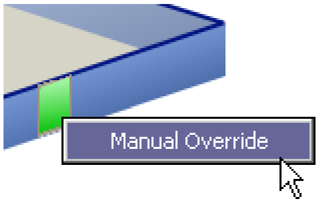
Widget painting

Painting refers to how widgets present themselves graphically (using: colors, transparencies, and so on), as well as cropping. Graphics are always translated so that the origin 0,0 is positioned at the top, left corner of the widget. The graphics crop (visible area) is set to the widget's size. Alpha and transparent pixels blend with the pixels already drawn.
The system draws widgets in property order with the first widget at the bottom, and the last widget on the top. Effective z-order is reverse of property order.

Widget commands

Widgets can include user commands that are commonly activated with buttons and menu actions. Menu commands are available and may be used on widgets.

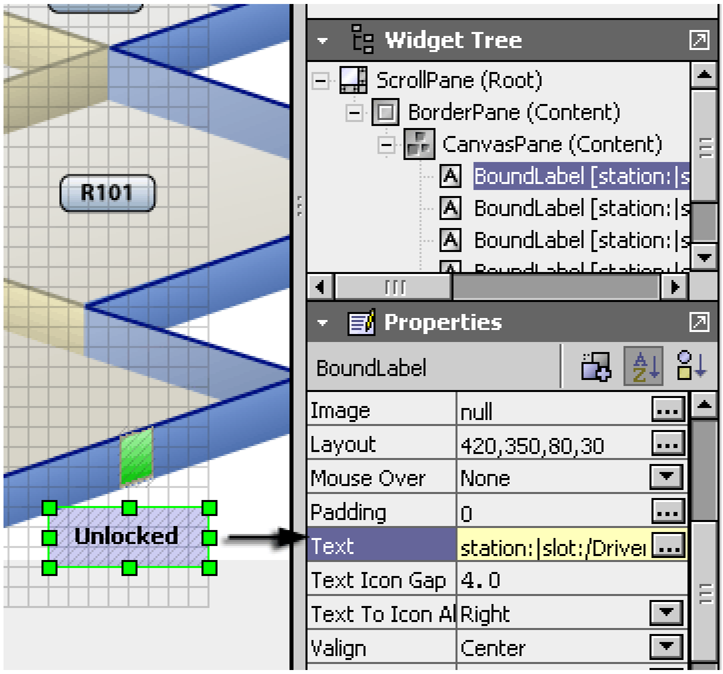
Figure 37. A widget command



Widget properties

Widget properties define many of the features, behaviors and appearance characteristics of widgets. By editing widget properties, you control how a widget behaves.

Figure 38. Widget properties



- ScrollPane (Root)
  - BorderPane (Content)
    - CanvasPane (Content)
      - BoundLabel [station:|s
      - BoundLabel [station:|s
      - BoundLabel [station:|s
      - BoundLabel [station:|s

Image	null
Layout	420,350,80,30
Mouse Over	None
Padding	0
Text	station:|slot:/Driver
Text Icon Gap	4.0
Text To Icon Al	Right
Valign	Center

The screen capture shows the properties in the side bar for a bound label. In this example, the text property of the label is bound to the `slot:/Drivers/AccessNetwork/baseReader/points/door1/strike/out/value` value, as shown in the text property. The binding of this value allows the dynamic presentation of the door strike in the Graphic view.

In the Graphic Editor view, you edit widget properties using the properties side bar or **Properties** window and their secondary windows. Properties that appear with the ellipses open secondary windows, which provide additional properties and options. These windows open when you click the property.

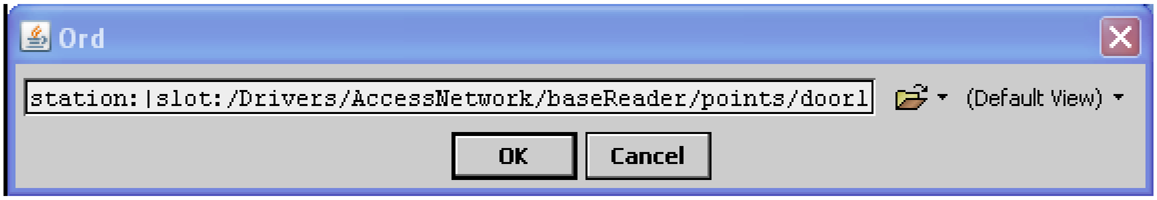
Animated graphics

Animated graphics are graphics whose values update in real-time. A graphic can be as simple as a single word of text (ON) or a number (72), or it can be an animated image (door opening). Widgets are animated by binding their properties to a legitimate data source.
For example, you connect numeric values to widget properties that use numeric values, and you connect binary values to objects that use binary values. By animating the properties of a widget, you control the text appearance of the image, as well as change a widget's location on the page, and even its visibility.

Data binding

An ORD (Object Resolution Descriptor) establishes the connection between a widget and an object. The ORD is the universal identifier used throughout the system. The ORD unifies and standardizes access to all information. Designed to combine different naming systems into a single string, it has the advantage of being parsable by a host of public APIs (Application Program Interfaces).
A single binding consists of a single widget-object relationship. A binding's ORD property identifies the location of the object that updates and animates the widget.

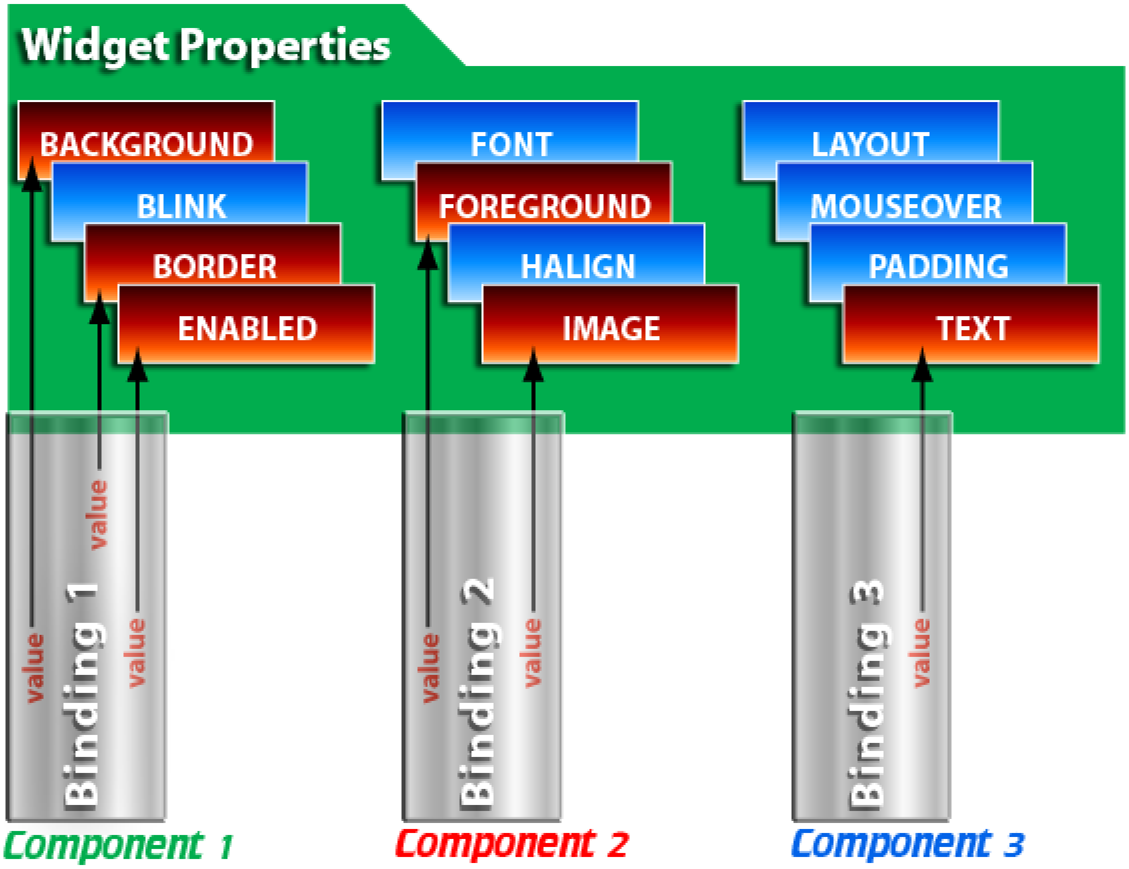
Figure 39. Widget data binding


Ord
station:|slot:/Drivers/AccessNetwork/baseReader/points/door1
(Default View)
OK
Cancel

The screen capture shows a value binding to a text label widget as viewed in the **Ord** window of a binding.

The most common type of binding, the value binding, provides some of the typical functions that are associated with building real-time information for presentation as both text and graphics. This includes support for mouse-over and right-click actions. Additionally, it provides a mechanism to animate any property of its parent widget using converters that convert the target object into property values.

Figure 40. Widget with three bindings

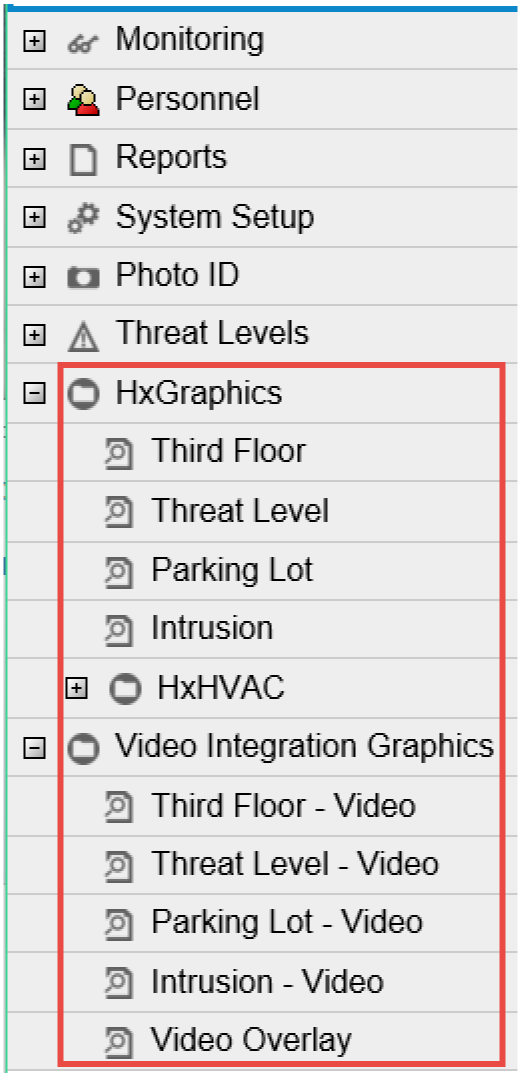


The screen capture illustrates the `object-to-widget` property binding concept. In this example, a widget has three separate data bindings. This means that each binding is coming from a different object and, therefore, each binding has a different ORD that defines its binding. Each binding provides access to an object's values so that they may be used, as required, to animate the widget properties.

Graphic views in the system menu

As the menu structure is a hierarchy with parent nodes and subordinate child nodes, you may create a nav (navigation) group for graphics and assign child graphics to it. You may also add graphics to an existing node in the navigation tree.

Graphics appear in the web UI menu.

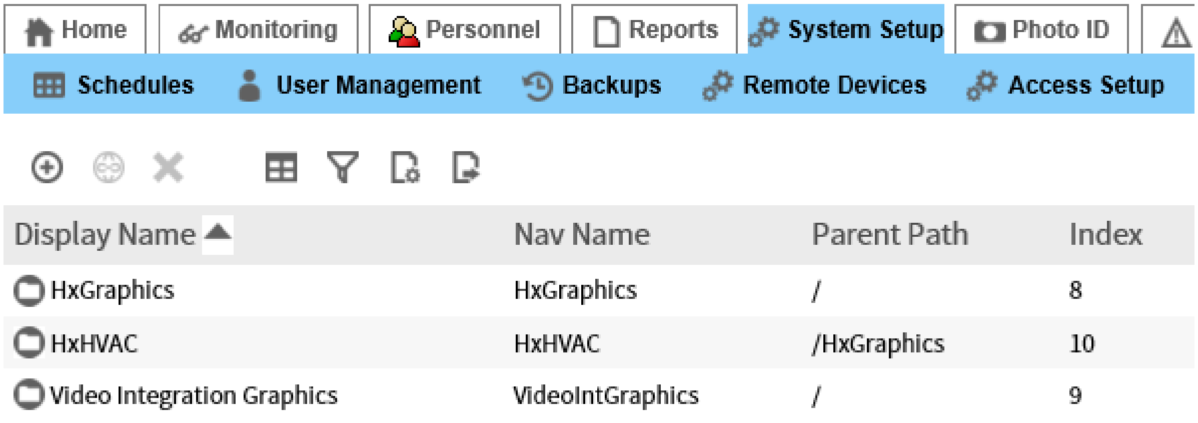


Creating (and editing) a navigation group

A nav group displays in the menu under its assigned parent.

Step 1. From the main menu click **Controller (System) Setup** > **Miscellaneous**, expand the **Graphics** menu and click **Navigation Groups**.

The Navigation Groups view opens.



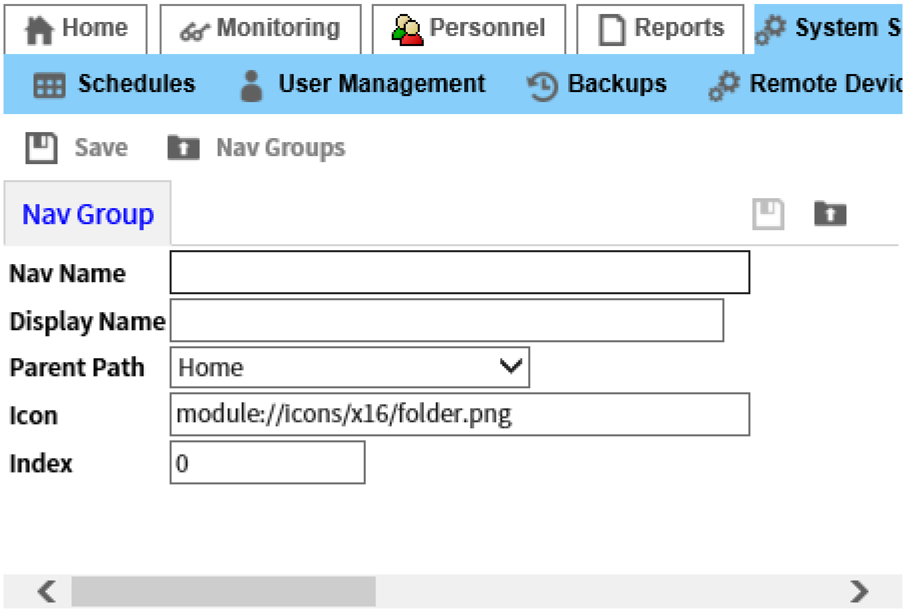
Display Name ▲	Nav Name	Parent Path	Index
HxGraphics	HxGraphics	/	8
HxHVAC	HxHVAC	/HxGraphics	10
Video Integration Graphics	VideoIntGraphics	/	9

This view displays a table of all the navigation groups that are available on the local station.

Step 2. Do one of the following:

- To add a nav group, click the Add button (⊕).
- To edit an existing group, select the group row in the table and click the Hyperlink button (🌐).

If adding, the Add New Nav Group view opens.



Nav Name	
Display Name	
Parent Path	Home
Icon	module://icons/x16/folder.png
Index	0

If editing, the system populates the properties displayed on the single tab below the **Save** button and a Navigation Groups link. The **`Display Name`** property defines how the nav group appears in the navigation tree. The **`Index`** property defines where the nav group appears in the menu hierarchy. A 0 or 1 places the nav group first.

Step 3. Fill in or edit the properties and click the **Save** button at the top of the view.

NOTE: A Nav Group does not display in the menu until a child menu item is assigned to it.

Adding a graphic view to the navigation tree

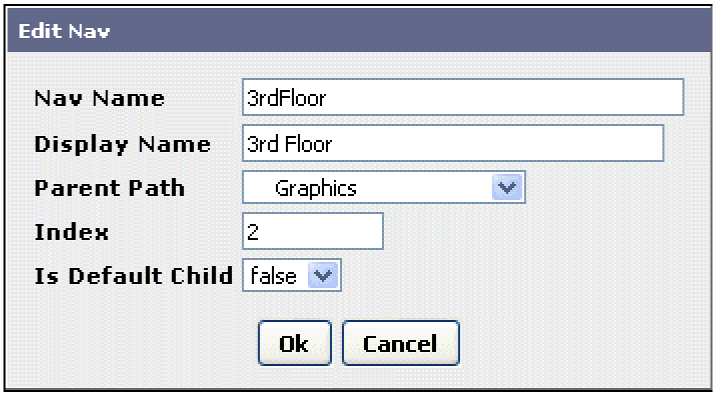
A small graphic in the navigation tree provides a visual representation of the node.

Prerequisites:
The graphic exists.

Step 1. From the main menu click **Controller (System) Setup** > **Miscellaneous**, expand the **Graphics** menu and click **Graphics Management**.
The Graphics view opens.

Step 2. Select the graphic row in the table and click the Edit Nav button ( ).

The **Edit Nav window** opens.



Edit Nav

Nav Name	3rdFloor
Display Name	3rd Floor
Parent Path	Graphics
Index	2
Is Default Child	false

The `Display Name` property defines how the graphic appears in the navigation tree. The `Index` property defines where the graphic appears in the sub-menu hierarchy. A 0 or 1 places the graphic first.

Step 3. Fill in the properties and click **Ok**.

Designing a reusable graphic

Graphic files that are used in multiple views on a local station or even possibly for use across different stations, may supply an absolute value from a target device in a specific remote station, or a relative value from a device within the current station. A relative path causes a Graphic file to resolve data bindings to identically named components that reside in different locations, thus making one graphic file usable in many views. Refer to the *Niagara Graphics Guide* for more information.

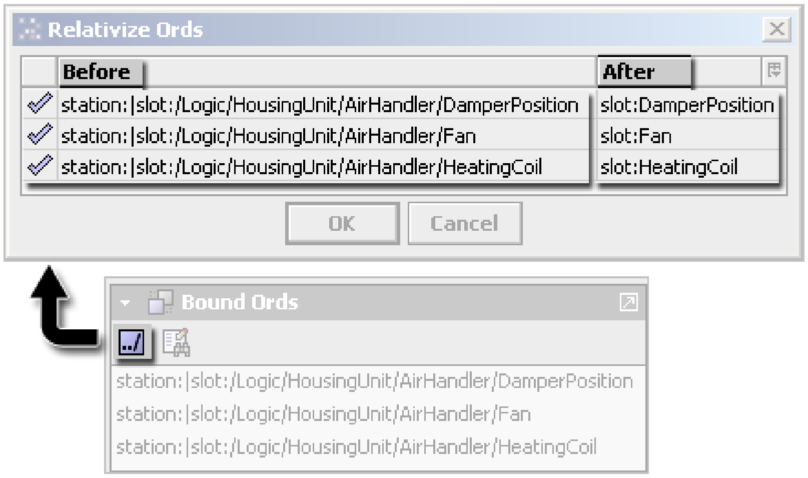
Prerequisites:
You have configured the same device names identically in multiple locations. The graphic to reuse is open in the Graphic Editor.

Step 1. Select the device widget.

Step 2. Open the Widget Tree side bar and double-click the object in the Widget Tree or on the canvas.

Step 3. Select the BoundLabel under the Canvas Pane in the Widget Tree.

Step 4. Click **Relativize ORDs**.



Relativize Ords

	Before	After
✓	station:|slot:/Logic/HousingUnit/AirHandler/DamperPosition	slot:DamperPosition
✓	station:|slot:/Logic/HousingUnit/AirHandler/Fan	slot:Fan
✓	station:|slot:/Logic/HousingUnit/AirHandler/HeatingCoil	slot:HeatingCoil

station:|slot:/Logic/HousingUnit/AirHandler/DamperPosition
station:|slot:/Logic/HousingUnit/AirHandler/Fan
station:|slot:/Logic/HousingUnit/AirHandler/HeatingCoil

The **Relativize Ords window** opens.

Step 5. Change the absolute Ord (Before) to a relative Ord (After).

Chapter 14. Maintenance

This chapter contains additional configuration procedures, as well as procedures for updating software, replacing the Supervisor PC and replacing controllers. It concludes with a troubleshooting section that provides some steps to follow when things are not working right.

All topics are available in the *Niagara Community Resource Center*. Through this site you can also comment on these topics. The technical documentation team welcomes your suggestions for improving these procedures with your real-world experiences.

Changing the admin password

The admin user has access to the entire system. Changing the password for this user on a frequent and regular basis is a powerful best practice for maintaining a secure system. This procedure uses the web UI.

Prerequisites:
You are logged in to the station with admin privileges. This procedure documents a task performed in both the Supervisor PC and remote controller stations using the system's browser interface. The alternative Supervisor station command is in parenthesis.

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

Step 2. In the **`New Password`** property, type a new strong password.

Step 3. To confirm that you typed the name correctly, type the new password again in the **`Confirm New Password`** property, and click Save.
If the two values match, the system implements the change.

Step 4. To return to the home view, click Home.

Result

TIP: Your system should be set up with more than one user that has admin rights in case someone loses the admin password.

Changing the system passphrase

The system passphrase protects sensitive information stored in file systems, and on the SD card in each controller, and encrypts portable files, such as backups and station copies. You should define a strong system passphrase. If you skipped configuring this phrase during installation, this procedure documents how to set it up now.

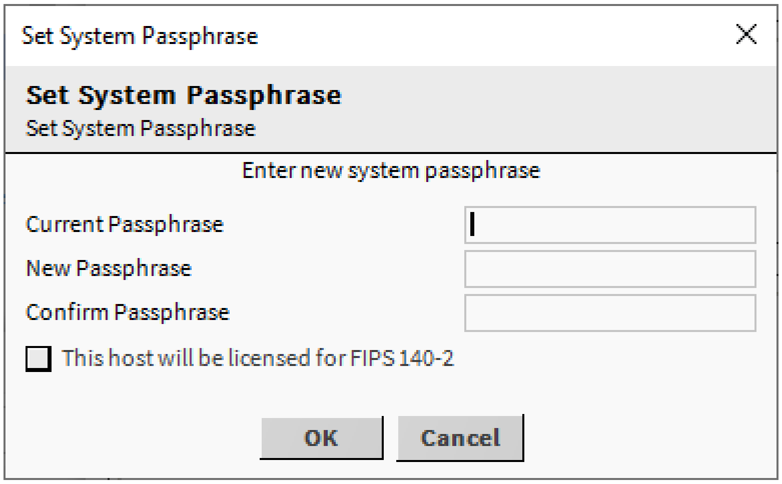
Prerequisites:
You are working in Workbench running on a PC.

Step 1. Open a platform connection to the PC.

Step 2. Double-click the Platform node in the Nav tree and double-click Platform Administration or right-click the platform node and click Views > Platform Administration.
The Platform Administration view opens.

Step 3. Click System Passphrase.

The **Set System Passphrase** window opens.



Set System Passphrase

Set System Passphrase
Set System Passphrase

Enter new system passphrase

Current Passphrase	
New Passphrase	
Confirm Passphrase	

□ This host will be licensed for FIPS 140-2

Step 4. Enter the current passphrase, create a new passphrase and click **OK**.
If your installation is licensed for FIPS (Federal Information Processing Standard), this phrase must be at least 14 characters including at least one number, as well as lower and upper case letters.

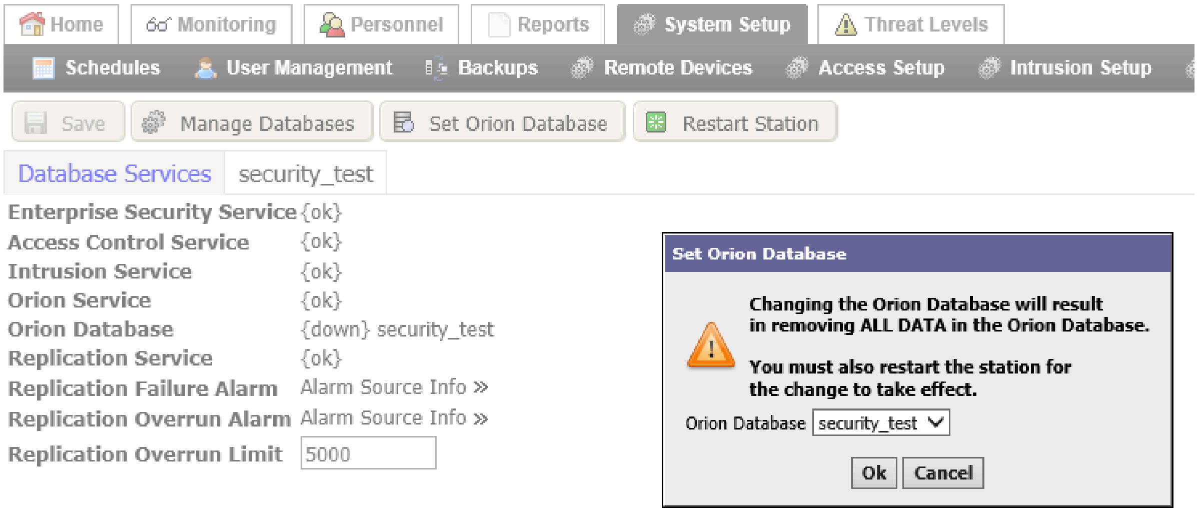
Changing the system database

If upgrading a system requires you to change the current Orion database, you may do so using the web UI.

Step 1. Download the new database software (MySQL or MSSQL), create the new database, and ensure that it is running.

Step 2. In the web UI, click **System Setup** > **Miscellaneous** > **Configure Database**.

Step 3. Click **Set Orion Database**.
The **Set Orion Database** window opens.



Enterprise Security Service	{ok}
Access Control Service	{ok}
Intrusion Service	{ok}
Orion Service	{ok}
Orion Database	{down} security_test
Replication Service	{ok}
Replication Failure Alarm	Alarm Source Info »
Replication Overrun Alarm	Alarm Source Info »
Replication Overrun Limit	5000

Set Orion Database

Changing the Orion Database will result in removing ALL DATA in the Orion Database.

You must also restart the station for the change to take effect.

Orion Database: security_test

Step 4. Select the new database and click **Ok**.

Step 5. When the system has used the new database without incident for a week or two, delete the database device from the rdb (Relational Database Management) driver in the Supervisor station.

Step 6. For security purposes, delete the database from the old location.

Viewing and updating module firmware

The Device Module view indicates the installed version of the module firmware and if a more recent version is available.

Prerequisites:
You are connected to a controller using the web UI.

Step 1. Navigate to **Controller Setup** > **Remote Devices** > **Remote Modules** > **Remote Module Setup.** The view lists the connected modules.

Step 2. Compare the Installed Version with the Available Version column.

Step 3. If a more recent version of the firmware is available, click Upgrade Firmware ( ).

Step 4. To discover and match the base board module of the new controller with the baseboard module in the database, click the **Discover** button, select the discovered station and click the Match button ( ).

Step 5. Set the network's TCP/IP settings in the new controller to the same settings as the old controller (**Controller (System) Setup** > **Miscellaneous** > **Network TCP/IP Settings**).

Step 6. If necessary, change the adaptor settings on your PC for testing purposes.

Step 7. Test functionality by using a card to open a door.

Managing licenses

The License Manager view allows you to view, upload and remove licenses.

Prerequisites:
The software is installed and configured. You are working in the web UI.

Step 1. To view access this view, click **Controller (System) Setup** > **Miscellaneous** > **License Manager** The License Manager view opens.

Step 2. To view a license, click on the hyperlinked file name. The license file opens in the browser.

Step 3. To remove a license, click the check box to the left of the license hyperlink and click **Delete.**

Step 4. To upload a new license, browse for the license in the **Upload New license, certificate or lar File** section, and click **Upload.**

NOTE: If you update your license file you may need to clear your browser cache to view the updated file. For how to clear the browser's cache, refer to your browser documentation.

Data export

This feature makes data collected by the system available for processing and analysis outside the system.

In the web UI you can export data wherever the **Export** button appears in the view. In Workbench, the `Export` option is available in every table view from the drop-down list in the upper right corner of the view.

Exporting a schedule to a CSV file

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

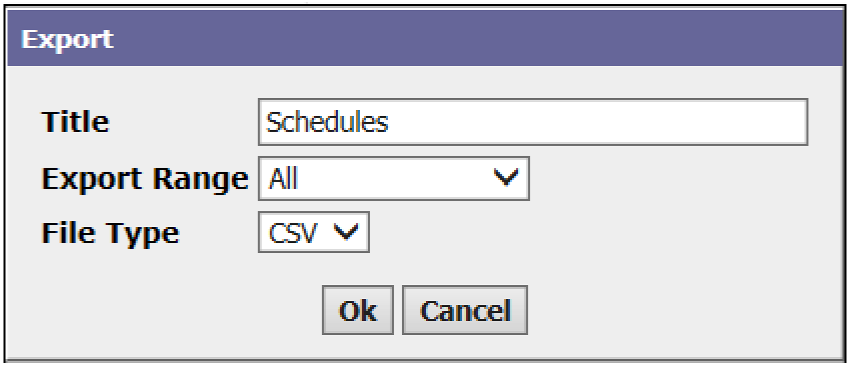
Prerequisites:

You start out working on a Supervisor station.

Step 1. From the main menu, click **System Setup** > **Schedules**.
The Schedules view opens.

Step 2. Select the schedule to export and click the Export button ( ).

Step 3. Select `CSV` for **`File Type`**.
The window changes size.



Export

Title: Schedules

Export Range: All

File Type: CSV

Step 4. To continue, click **Ok**.
The system prompts to confirm the download and downloads the CSV file.

Step 5. Save the file to a location where you can be sure to find it.

One way to discover and export schedules

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

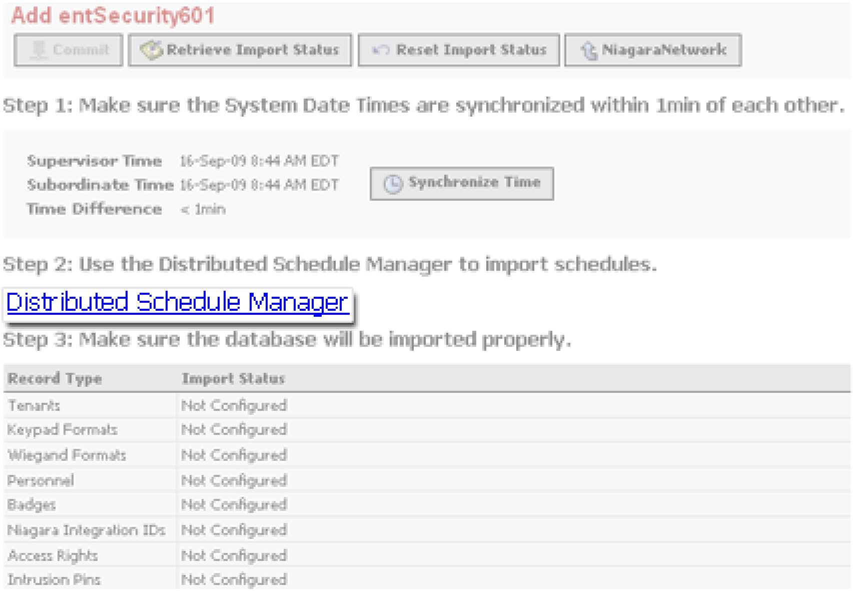
Prerequisites:
You are working in either the Supervisor or a controller station using the web UI.

Step 1. If needed, return to the main menu.

Step 2. Click **Controller (System) Setup** > **Remote Devices** > **Station Manager**.
The Station Manager - Database view opens.

Step 3. Select a station in the database and click the **Join** button ( ).

The Add Station view opens.



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

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

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

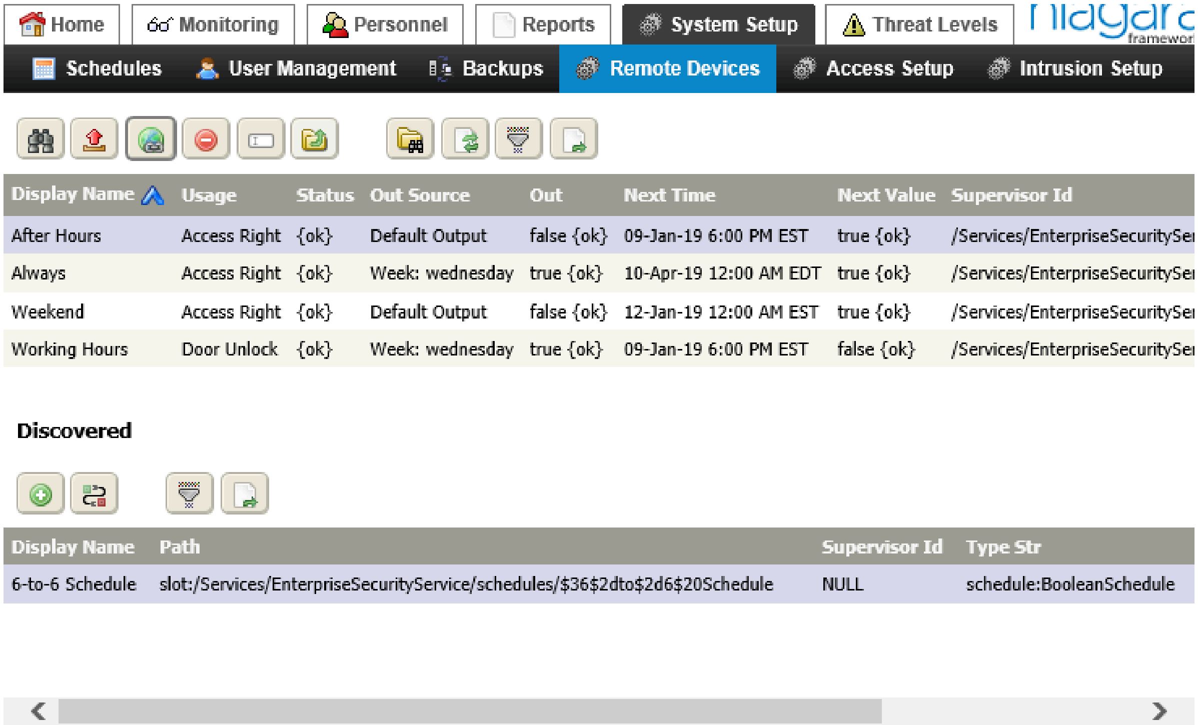
Distributed Schedule Manager

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

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

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

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



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

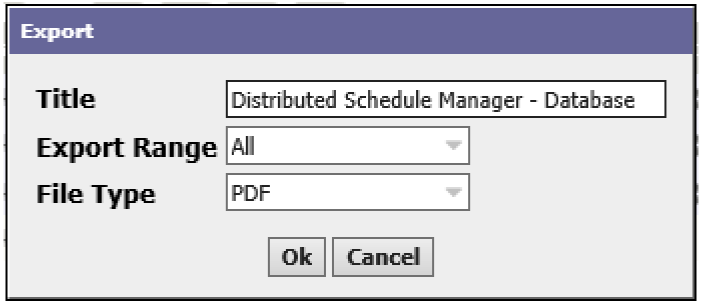
Discovered

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

Step 5. To discover additional schedules, click the Discover button ( ).
The Discovered pane opens with the additional schedule(s).

Step 6. Select the schedule records to export in either pane.

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



Export

Title	Distributed Schedule Manager - Database
Export Range	All
File Type	PDF

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

Another way to discover and export schedules

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

Step 1. If needed, return to the main menu.

Step 2. Click **System/Controller Setup** > **Remote Devices** > **Station Manager**.
The Station Manager - Database view opens.

Step 3. Select a station and click the **Summary** button in the toolbar.
The Station Device Properties view opens.

Step 4. Choose the Device Exts tab and click on the `Schedules` link.
The Distributed Schedule Manager - Database view opens.

Step 5. Click the Export button ( ).
The **Export** window opens.

Step 6. Fill in the properties and click **Ok**.

Matching schedules

It is important to keep shared schedules up-to-date between the Supervisor and remote stations. Schedules may get out of synchronization for any number of reasons. For example, if you remove a Supervisor from a remote Station Manager Database, the system deletes from the remote controller station any schedules that are mastered on the Supervisor. You use the match feature to recreate and synchronize schedules between the remote and Supervisor stations.

Prerequisites:
You are working in the Supervisor station. The Supervisor and remote platforms are connected to the shared network and both stations are running.

Step 1. Click **Schedules** > **Schedules**.

Step 2. Click the Discover button ( ).
The system runs a schedule discovery job to learn (find) and display the schedules that are available. When the discovery job finishes all discovered objects appear in the Discovered pane below the Database pane. It is important to discover from the Supervisor station before doing anything else to make sure that the latest schedules are available in the Supervisor and remote stations.

Step 3. Do one of the following:

- If schedule changes do not appear in the remote stations, initiate a replication from the

Supervisor station.

- If the schedule exists in both stations, select the schedule in the Discovered pane and click the Match button (

).

When you match a schedule between a Supervisor and remote controller stations, the Supervisor version takes priority and overwrites the remote controller version of the schedule so that they are the same.

NOTE: To keep the schedule, remove the schedule out of the NiagaraNetwork using Workbench and change the schedule's read-only flag.

Result

If you rename schedules, do it only while the Supervisor and subordinate stations are both online to allow for synchronization. If you rename a schedule while a Supervisor and subordinate are disconnected, you must discover and match each schedule in the remote stations.

Upgrading a device

Individual devices require updating if you changed the device or if the device's firmware needs upgrading.

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

Step 2. Check that the modules have the latest firmware version by comparing the Installed Version Column with the Available Version column.

NOTE: During a firmware upgrade, the modules are taken off-line temporarily. If a system is in use, the upgrade process makes the system unavailable until the upgrade is complete.

Step 3. If the Available Version number is greater for any of the modules, click the **Upgrade Firmware** button.
This initiates the upgrade on all modules in the database. You do not have to select a module for the system to upgrade it. The system reports Upgrading Access Devices.... After the upgrade, all modules should have the same firmware version number.

Supervisor platform upgrade

These procedures are unique to upgrading the Supervisor PC.

You may need to upgrade the software running on the Supervisor PC for several reasons:

- A new software version is available.
- New features need to be added to the system.
- The PC needs to be replaced.

Updating reader count

Before deleting a subordinate station, you should update the reader count. This action updates the counts for all hardware components and removes items that no longer exist.

Step 1. Click (**System Setup** > **Miscellaneous** > **Server Maintenance**).
The Maintenance view opens.

Step 2. Click the **Update Reader Count** button.
This action updates the counts for all hardware components and removes items that no longer exist.

Removing the Supervisor from a remote station database

You may need to remove the Supervisor from a remote station database if you are replacing or adding a new Supervisor PC to the network.

Step 1. While connected to the remote station, click **Controller Setup** > **Remote Devices** > **Station Manager**.

Step 2. Select the Supervisor station row and click the Delete button (⊖).
The system removes the Supervisor station. In the process it also removes any schedules that were mastered on the Supervisor. You will need to discover and match schedules in the remote station with the schedules in the new Supervisor.

Remote controller upgrade

If your controller is connected to a Supervisor, upgrade the Supervisor first and then upgrade the controller station from the Supervisor.

The procedures in this section are unique to upgrading a controller. There are several reasons to upgrade the software in a controller:

- A new version of software has come out.
- The company wants to implement new features.
- The controller needs to be replaced with a new controller of the same model.
- The controller is being replaced by a different model controller.

If the upgrade is replacing the current software without making a hardware change, you should back up the station by making a distribution file backup or a station copy, but you may not need to restore the station after the upgrade.

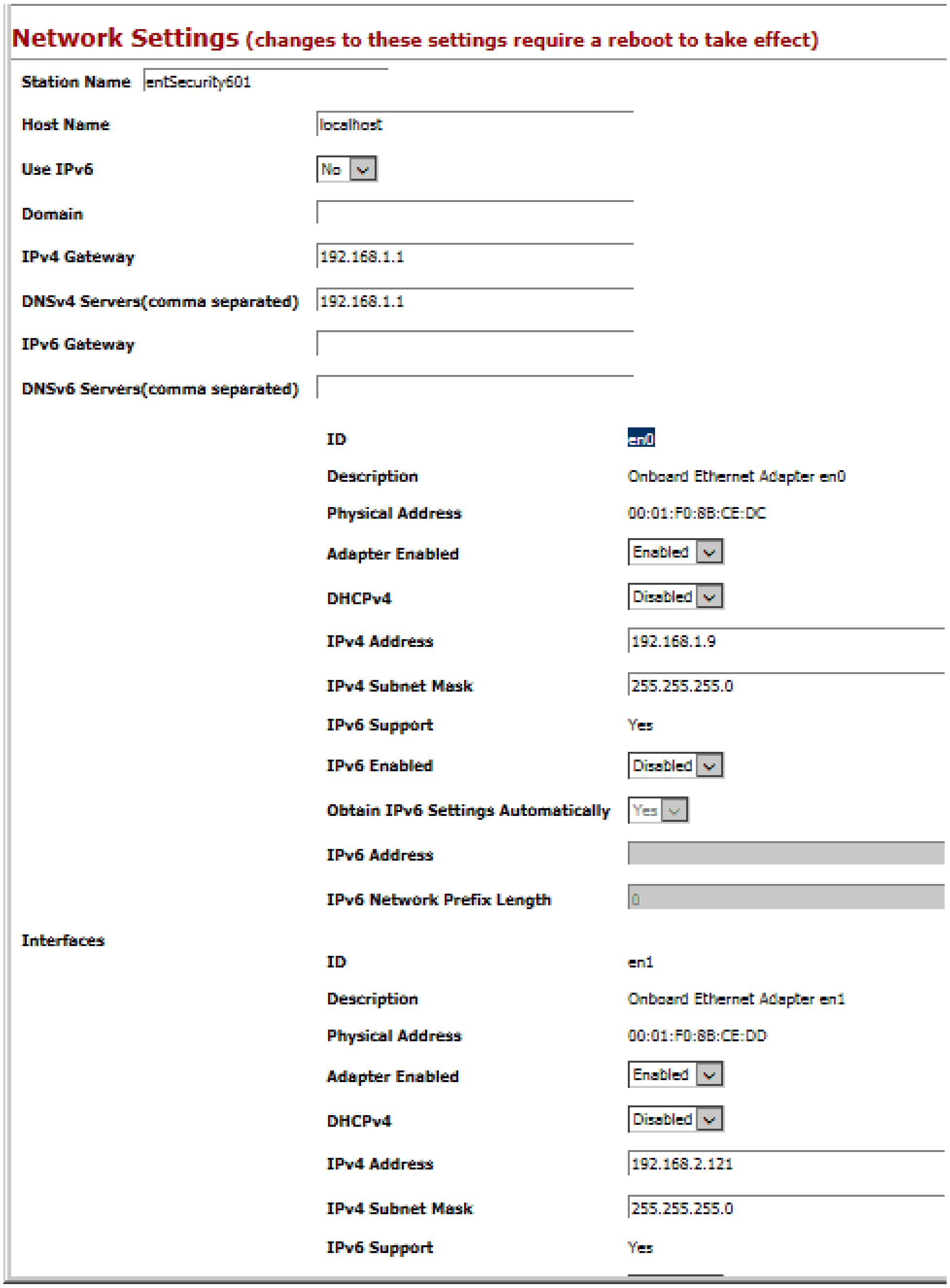
If you are replacing the controller with a new controller of the same model, a distribution backup of the station is the recommended best practice for upgrading the software.

If you are replacing the controller with a different model, a distribution file will not work. You must make a copy of the station instead.

Disconnecting an old controller

Before you disconnect the existing controller, make sure that you take a note of its IP address and other network settings. You will need to enter this information into the replacement controller before it will operate on the network.

Step 1. To take note of the network settings, select **Controller Setup** > **Miscellaneous** > **Network TCP/IP Settings**.



Network Settings (changes to these settings require a reboot to take effect)

Station Name	entSecurity601	
Host Name	localhost	
Use IPv6	No	
Domain		
IPv4 Gateway	192.168.1.1	
DNSv4 Servers(comma separated)	192.168.1.1	
IPv6 Gateway		
DNSv6 Servers(comma separated)		
	ID	en0
	Description	Onboard Ethernet Adapter en0
	Physical Address	00:01:F0:8B:CE:DC
	Adapter Enabled	Enabled
	DHCPv4	Disabled
	IPv4 Address	192.168.1.9
	IPv4 Subnet Mask	255.255.255.0
	IPv6 Support	Yes
	IPv6 Enabled	Disabled
	Obtain IPv6 Settings Automatically	Yes
	IPv6 Address	
	IPv6 Network Prefix Length	0
Interfaces		
	ID	en1
	Description	Onboard Ethernet Adapter en1
	Physical Address	00:01:F0:8B:CE:DD
	Adapter Enabled	Enabled
	DHCPv4	Disabled
	IPv4 Address	192.168.2.121
	IPv4 Subnet Mask	255.255.255.0
	IPv6 Support	Yes

Step 2. Take a screen capture or write down the properties.
Scroll down. There are a lot of properties in this view.

Step 3. Remove both AC and battery backup power from the existing controller.

Step 4. Wait for the controller to shut down, then disconnect all connectors and remove the controller from the cabinet.

Step 5. If the existing controller has an option card, remove the card.

Installing the replacement controller

If an option card (module) was damaged when the controller failed, you may need to purchase a new option card. If possible, try to install the option card from the previous controller into the new controller using the same slot as on the old controller.

Step 1. Install the new controller in the cabinet and plug in the connectors for on-board I/O, remote modules, and your PC.

Step 2. Apply power and connect the backup batteries.

Step 3. Set up your PC network adaptor to an IP address that is compatible with the controller's default IP address: 192.168.1.120.

Step 4. Open the new controller platform.

Step 5. Continue with the configuration steps in this chapter.

Creating and updating the HSQL database password

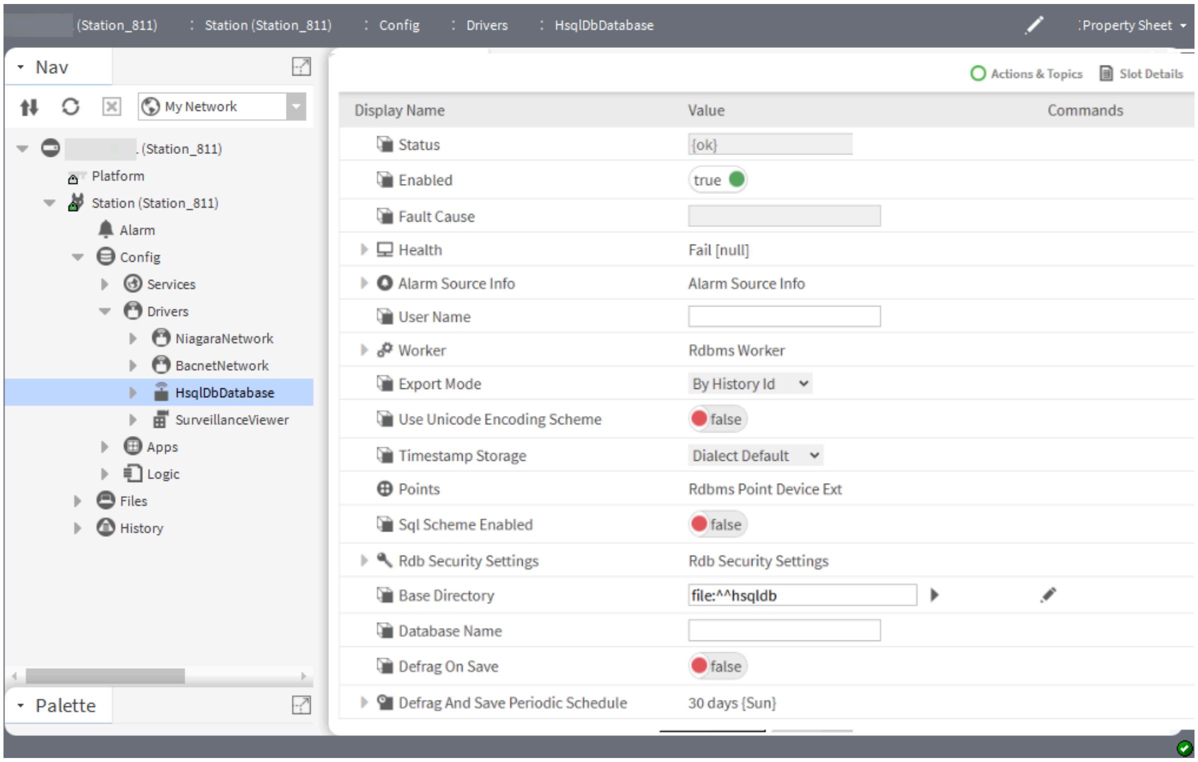
Each controller ships from the factory with a default HSQL database password and upgrading an AX station to an N4 station resets the HSQL database password back to the factory default. While the default password initially works, as soon as you install or upgrade a controller and its software, you should change this password to a unique and strong string. The password is automatically generated and successfully stored in the key ring.

Prerequisites:
You have just installed a new controller or upgraded an existing controller from AX to N4. You are using Workbench running on a PC that is connected to the network that services the controller.

Step 1. Connect to the controller station using Workbench.

Step 2. Expand **Config** > **Drivers** > **RdbmsNetwork**.

Step 3. Right-click **HsqlDbDatabase** and click **Actions** > **Ping**. The health property is updated based on the ping results.



Display Name	Value	Commands
Status	{ok}	
Enabled	true ●	
Fault Cause		
Health	Fail [null]	
Alarm Source Info	Alarm Source Info	
User Name		
Worker	Rdbms Worker	
Export Mode	By History Id	
Use Unicode Encoding Scheme	● false	
Timestamp Storage	Dialect Default	
Points	Rdbms Point Device Ext	
Sql Scheme Enabled	● false	
Rdb Security Settings	Rdb Security Settings	
Base Directory	file:^^hsqldb	
Database Name		
Defrag On Save	● false	
Defrag And Save Periodic Schedule	30 days {Sun}	

NOTE: Starting in Niagara 4.14, the HsqlDbDatabase component properties **Use Encrypted Connection**, **User Name**, and **Password** are replaced with a single **Privileged Username** property. The HSQL database is automatically generated and not editable or visible. When using HSQL, if the station keyring is corrupted, you need to load a backup station, as this instance of the HSQL database is no longer operational.

Step 4. To access a new HSSQL database instance in the N4 station, right-click the HsqlDbDatabase, navigate to **Views** > **Property Sheet**.
The device's Property Sheet opens.

Step 5. Enter the **User Name** as SA and click **Save**.

Step 6. Right-click **HsqlDbDatabase** and click **Actions** > **Ping**. The health property is updated based on the ping results.

Software upgrade

A release of the system is based on product development cycles and may lag or skip general releases of the Niagara Framework.

License requirement

CAUTION: After commissioning a controller with upgraded software, it reboots. While it is rebooting, all door lock relays are de-energized, and card readers do not respond. This may leave doors locked or unlocked, and building occupants may be locked out, or non-authorized people may gain access. Plan ahead and be prepared for how to deal with the system being down for five to ten minutes while the controller reboots.

Upgrading software may or may not require a new license and the installation of new software.

Before you upgrade

Before you install a new version of software, use this checklist to prepare the station:

- On your Supervisor PC, verify that the MySQL database reports `{ok}`.
- Confirm that you can connect to all devices.
- Resolve any reported alarms.

Make a station backup

Before upgrading any station, you should back up the station and save the backup file in a safe location. There are two ways to back up a station:

- Create a distribution (.dist) file of the station. You would use this backup method if you are upgrading just the software or are replacing a controller to the same model as the current controller.
- Perform a station copy. You would use this backup method if you are upgrading to a different controller model.

Driver modules

Be careful copying driver modules from a previous version of software to a new version. For example, an old version of the Milestone XProtect camera driver is `xprotect-se.jar`. The newer version is `xprotect-wb.jar`. Do not run a system with both files in the `modules` folder.

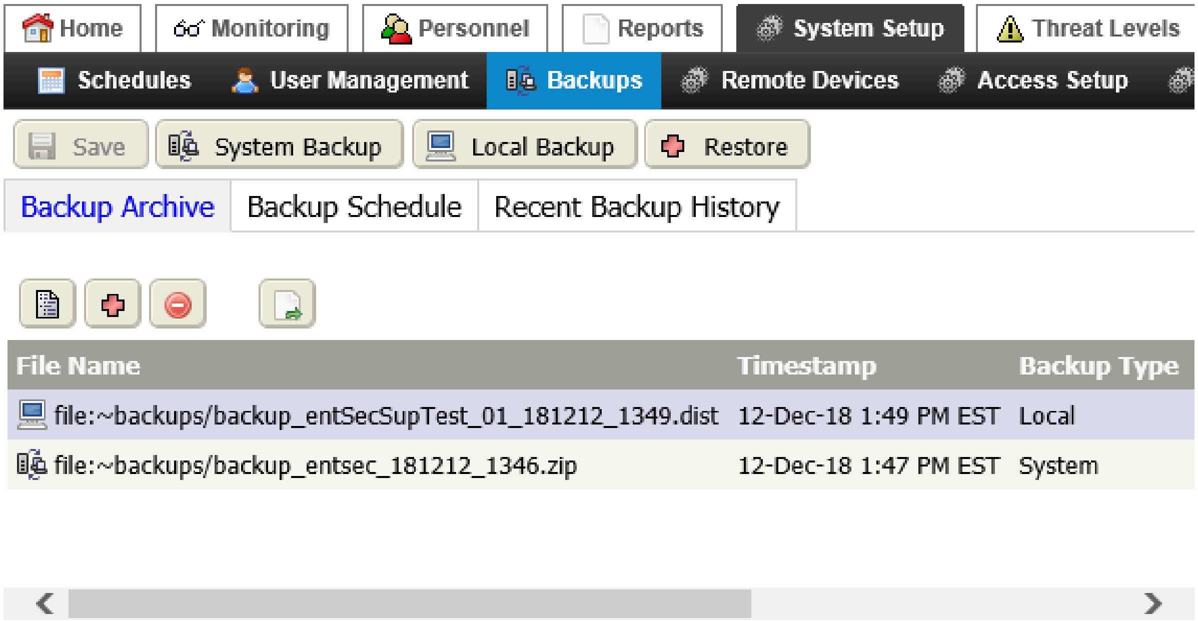
Backing up a station using the web UI

A station backup, which creates a distribution (.dist) file is the most complete way to back up a station. It includes all station data and module-dependent information. This type of backup automatically de-crypts the keyring (used to secure encrypted passwords) and stores the passwords in the .dist file. This procedure backs up the station you are currently logged into. This may be the Supervisor station or a remote controller station. You use this type of backup to replace a controller with another controller of the same model and software version and to install software on multiple same-model controllers.

Prerequisites:
Your PC is connected to the network with the remote controller. You are using the web UI.

Step 1. Open one of the supported web browsers (IE or Firefox) and connect to the remote station.

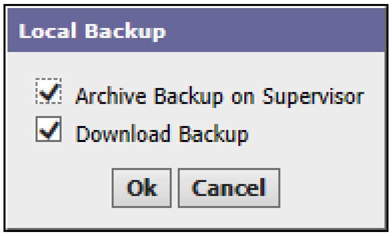
Step 2. From the Home view, click **Controller (System) Setup** > **Backups**.
The Backups view opens.



File Name	Timestamp	Backup Type
file:~backups/backup_entSecSupTest_01_181212_1349.dist	12-Dec-18 1:49 PM EST	Local
file:~backups/backup_entsec_181212_1346.zip	12-Dec-18 1:47 PM EST	System

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

A **Local Backup** window opens.

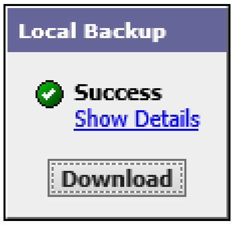


☑ Archive Backup on Supervisor

☑ Download Backup

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

Step 4. To continue, click **Ok**.
The **Job** window displays a progress bar while the backup job runs. When the job is finished, the **Local Backup** window opens.



✓ Success

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

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

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

Step 7. Save the file to a location other than the System Home or User Home, giving the file a short name that identifies the station.

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

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

Step 8. Make a note of the date and where you saved any downloaded backup files so you can find them later.
As a best practice, consider renaming the resulting backup `.dist` file to a short, meaningful name.

Step 9. If the `.dist` file is for a new Supervisor or engineering workstation on a different PC, copy the backup .dist file to the new PC, otherwise leave the backup `.dist` file in the backups folder.

Backing up a station using the BackupService

You may use this procedure to manually back up a single Supervisor or controller station. The *Niagara Provisioning Guide* explains how to set up a job prototype to back up all stations on a network.

Prerequisites:

You are using Workbench running on a PC and are connected to the remote station.

Step 1. Expand **Config** > **Services** and double-click the **BackupService**.
The **Backup Manager** view opens.

Step 2. To back up the station, select the station and click **Backup**.
A **File Chooser** window opens with a default location and name for the backup. The default `~backups` folder is in the user home: `C:\Users\<user name>\<framework version>\tridium\backups` where:

- `<user name>` is the name that identifies your PC

  .

- `<framework version>` identifies the current version of the Niagara Framework.

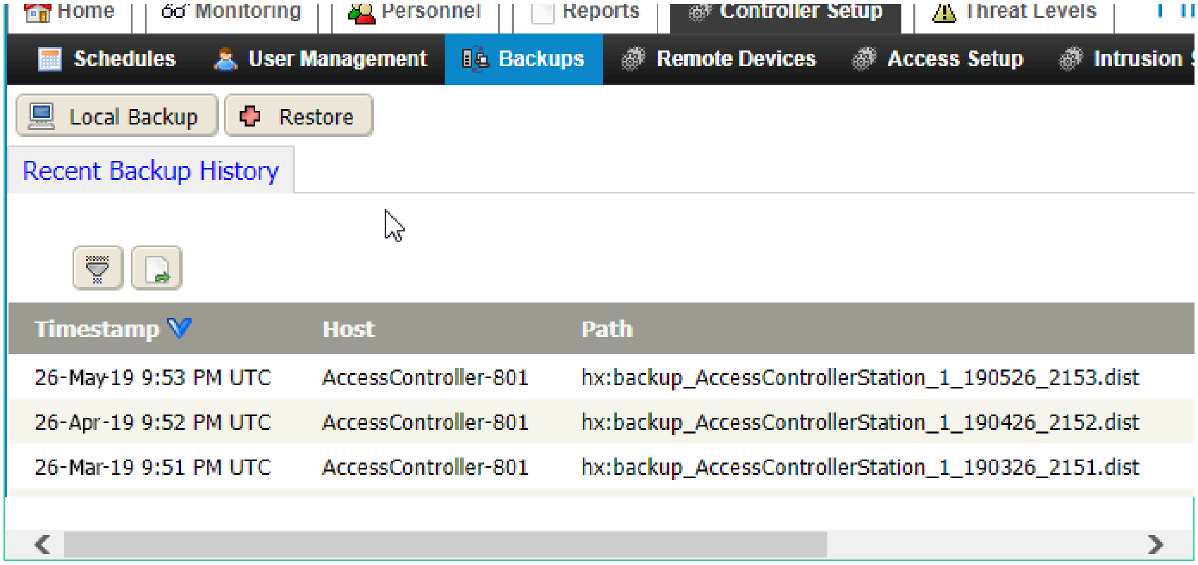
Step 3. To change the backup location, use the icons at the top of this window or accept the default and click **Save**.
The **BackupService** creates a `.dist` (distribution) file of the station in the folder you selected.

Viewing distribution file backup history

Before restoring a data backup, you may choose view the list of existing backups to see when the last backup was made. This procedure uses the web UI. It works for viewing backups of a Supervisor or remote station.

Step 1. From the main menu, select **System (Controller) Setup** > **Backups**.
The Backups view opens.

Step 2. Click the Recent Backup History tab.



Timestamp	Host	Path
26-May-19 9:53 PM UTC	AccessController-801	hx:backup_AccessControllerStation_1_190526_2153.dist
26-Apr-19 9:52 PM UTC	AccessController-801	hx:backup_AccessControllerStation_1_190426_2152.dist
26-Mar-19 9:51 PM UTC	AccessController-801	hx:backup_AccessControllerStation_1_190326_2151.dist

This tab lists all backup jobs that have been run.

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

Backing up a station using Station Copier

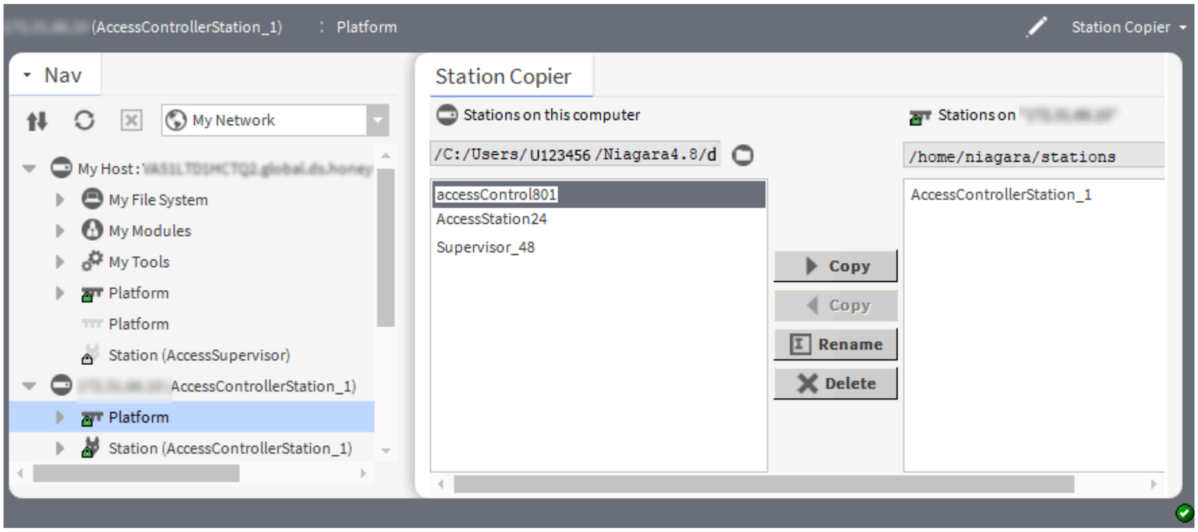
A distribution backup (.dist) depends on platform files, which makes it inappropriate when upgrading to a different model host. The Station Copier can back up all the files and subdirectories in a station so that you can restore the backed-up station to a different model host platform. In addition, Station Copier can back up just the config.bog, or just a single folder. Station copies do not contain encryption keys or software dependency information. This procedure works for both Supervisor and remote controller stations.

Prerequisites:
You are using Workbench running on a PC that is connected to the network.

For Enterprise Security customers, the web UI does not support the Station Copier.

Step 1. Open a connection to the remote platform.

Step 2. Expand the **Platform** node in the Nav tree and double-click **Station Copier** or double-click the **Platform** node, and double-click **Station Copier**.
The Station Copier view opens.


[redacted] (AccessControllerStation_1) : Platform
Station Copier
Nav
My Network
My Host : [redacted]
My File System
My Modules
My Tools
Platform
Platform
Station (AccessSupervisor)
[redacted] AccessControllerStation_1)
Platform
Station (AccessControllerStation_1)
Station Copier
Stations on this computer
Stations on [redacted]
Copy
Copy
Rename
Delete

/C:/Users/U123456/Niagara4.8/d

accessControl801
AccessStation24
Supervisor_48

/home/niagara/stations

AccessControllerStation_1

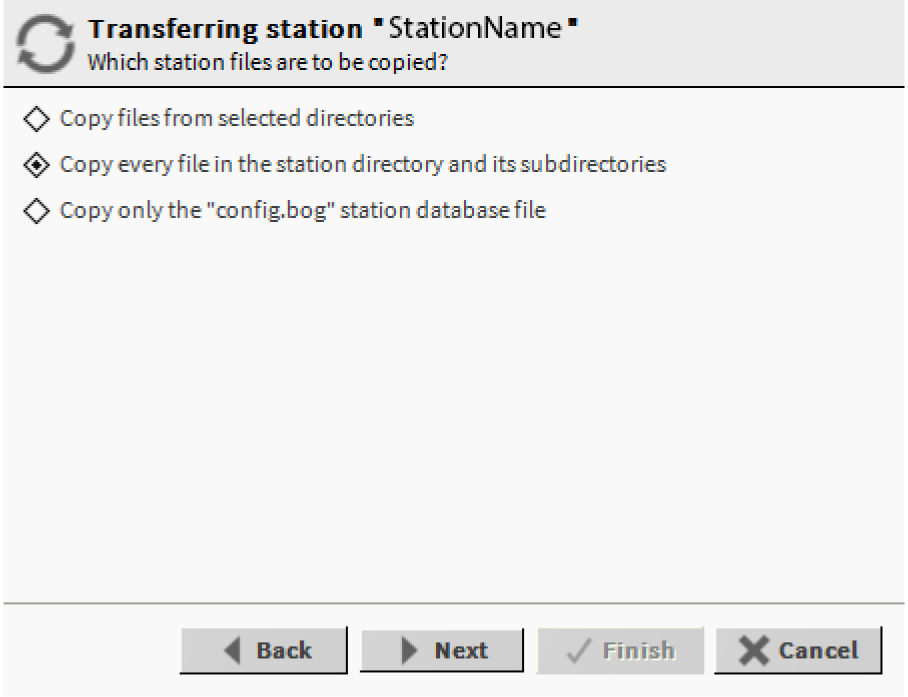
Step 3. Click the File icon (▭) on the Stations on this computer pane (left pane) and select the folder in which to store the station copy.

CAUTION: If you are copying only a `security` folder from the remote to your PC, do not overwrite the `security` folder in your PC. This folder contains encryption keys, which you will need in the new controller to decrypt user passwords.

Step 4. Select the station or folder and click **Copy**.
The **Loading Module Information** window opens followed by the Station Transfer Wizard.

Step 5. Click **Next**.

The wizard prompts you to select what to copy.



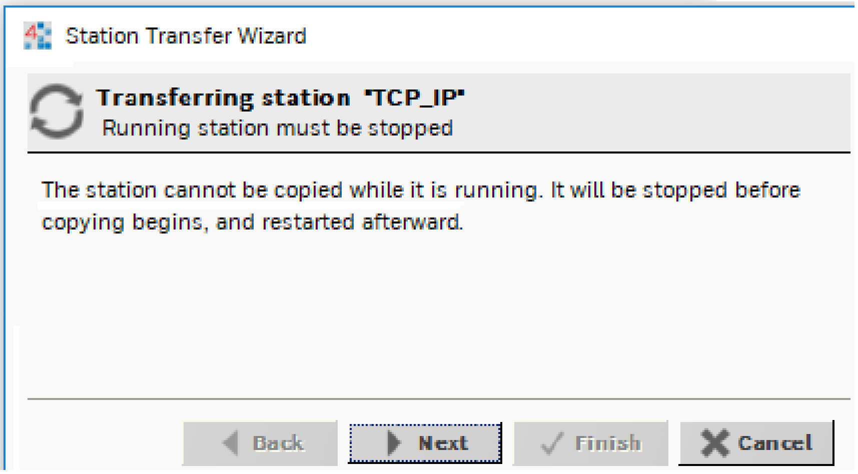
Transferring station "StationName"
Which station files are to be copied?

◇ Copy files from selected directories
◈ Copy every file in the station directory and its subdirectories
◇ Copy only the "config.bog" station database file

This option defaults to `Copy every file in the station directory and its subdirectories`. While Station Copier can back up just the config.bog, or just a single folder, it is recommended that you always back up every file in the station directory and its subdirectories.

Step 6. Make a selection, and click **Next**.
If a station with the same name exists in the target location, the wizard prompts you to delete or overwrite the existing station.

Step 7. Accept the default (delete), and click **Next**.
The wizard reminds you that the station must be stopped before it can be copied.



Station Transfer Wizard

Transferring station "TCP_IP"
Running station must be stopped

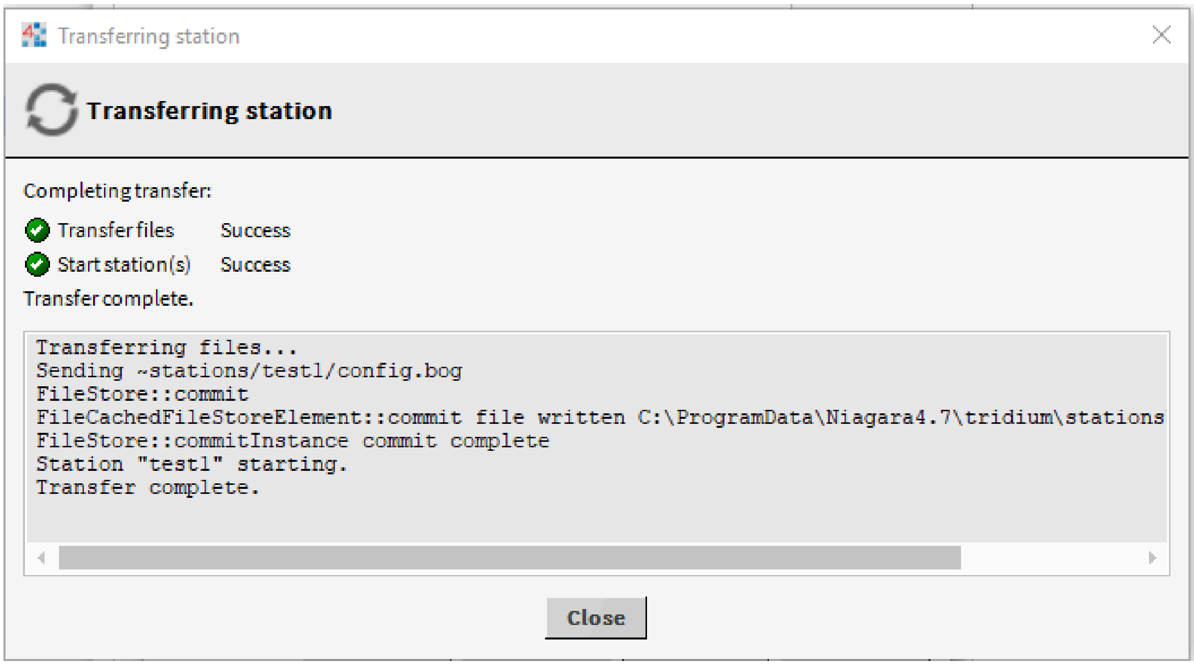
The station cannot be copied while it is running. It will be stopped before copying begins, and restarted afterward.

Step 8. To continue, click **Next**.

The wizard asks you to review the copy configuration (changes).

If you selected only specific station subdirectories to copy, they are listed.

Step 9. If needed, click **Back** and make changes, or, to complete the wizard, click **Finish**.
The Station Copier saves the station, if the remote station is currently running, begins the copy process and reports transfer status in the **Transferring Station** window.



Completing transfer:

✓ Transfer files Success

✓ Start station(s) Success

Transfer complete.

```
Transferring files...
Sending ~stations/test1/config.bog
FileStore::commit
FileCachedFileStoreElement::commit file written C:\ProgramData\Niagara4.7\tridium\stations
FileStore::commitInstance commit complete
Station "test1" starting.
Transfer complete.
```

The Station Copier saves the station if the remote station is currently running and

Step10. When the save completes, click **Close**.
The date for all copied files reflects when the files were copied.

Exporting the platform/station’s server certificate

Before upgrading software, you should export the platform/station’s server certificate so that after the upgrade you can import it to the upgraded platform/station’s Key Store.

Prerequisites:
You are working in Workbench on a PC that is connected to the network.

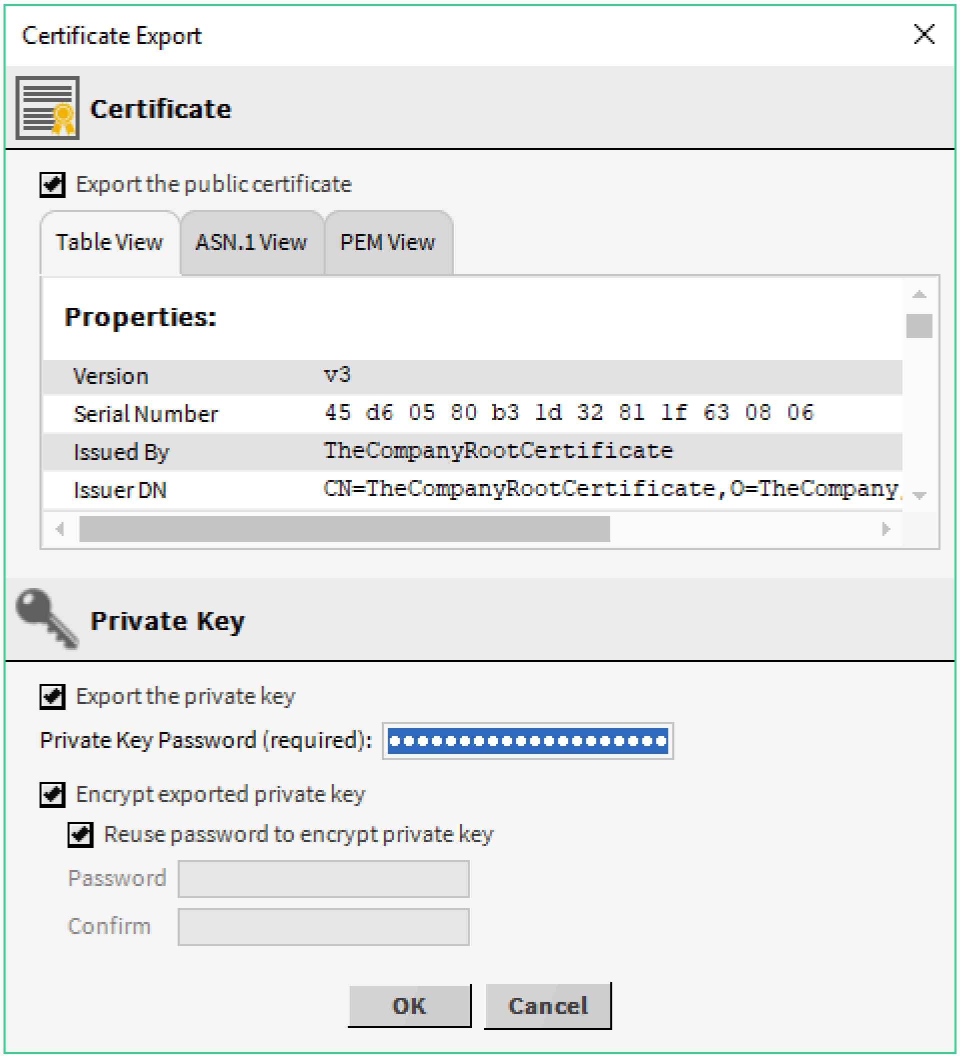
Step 1. Create a folder on the PC or a thumb drive to hold the server certificate(s).

Step 2. Open a platform connection to the platform and double-click the **Certificate Management** utility or right-click **Platform**, and click **Views** > **Certificate Management**.
The platform/station’s User Key Store tab opens.

Step 3. Confirm that this is the Certificate Management view you expected.
The IP address of the platform/station is identified below the view title.

Step 4. Select the server certificate and click **Export**.

The **Certificate Export** window opens.



Certificate Export

Certificate

☑ Export the public certificate

Properties:

Version	v3
Serial Number	45 d6 05 80 b3 1d 32 81 1f 63 08 06
Issued By	TheCompanyRootCertificate
Issuer DN	CN=TheCompanyRootCertificate,O=TheCompany,

Private Key

☑ Export the private key

Private Key Password (required): ••••••••••••••••••••

☑ Encrypt exported private key

☑ Reuse password to encrypt private key

Password

Confirm

Step 5. Select to export the certificate with its private key, create a strong password and click **OK**.
The **Certificate Export** browser window opens.

Step 6. Navigate to the folder you created and click **Save**.
A message confirms the export.

Step 7. Record in a safe place the location where you saved the certificate and the private key password.

CAUTION: Keep all certificates exported with their private keys safe. Do not email this certificate.

Installing the upgrade on a PC

You install and start a new version of Workbench following the same steps documented in the *Software Installation* chapter. This procedure summarizes the installation steps.

Prerequisites:
You are working in Workbench. You have either a distribution file or a copy of the Supervisor station and controller station(s).

Step 1. Using the **Platform** > **Application Director** disable **Auto-Start** and **Restart on Failure**, and stop the current Supervisor station.

Step 2. To install Workbench, extract the new software build and run the installer program.

Step 3. Follow the installation wizard as it sets up the System Home, User Home folders and shortcuts.

Step 4. Copy an updated license file to the `C:\niagara\niagara[version numbers]\security\licenses` folder of the new build.

Step 5. Start Workbench and open a platform connection to the Supervisor.

Result
At this point, you can use the upgraded installation to upgrade the software on a controller by commissioning the controller. But, before you commission, you should restore the Supervisor station.

Related information

- Software installation

Commissioning a controller with new software

Commissioning an existing controller with new software follows the same procedure as that required to commission a controller for the first time.

Prerequisites:

- You are on site where the controller to be upgraded is located. Commissioning a controller from a remote location is not recommended because the network connection could inadvertently be interrupted.
- You are running an updated version of Workbench is installed on a Supervisor or engineering PC, which is on the same network as the controller.
- The target remote controller is running (powered on).
- The version of the software you are using to commission the controller has identical brand properties (as defined in the license file) and is the same or a more recent version than that currently installed on the controller. A brand.123 upgrade tool cannot upgrade a brand.xyz controller. A Supervisor station will not connect to a controller on which a more recent version of software has been installed.
- Upgrading may require new licensing. The PC is connected to the Internet so that it can contact the licensing server.

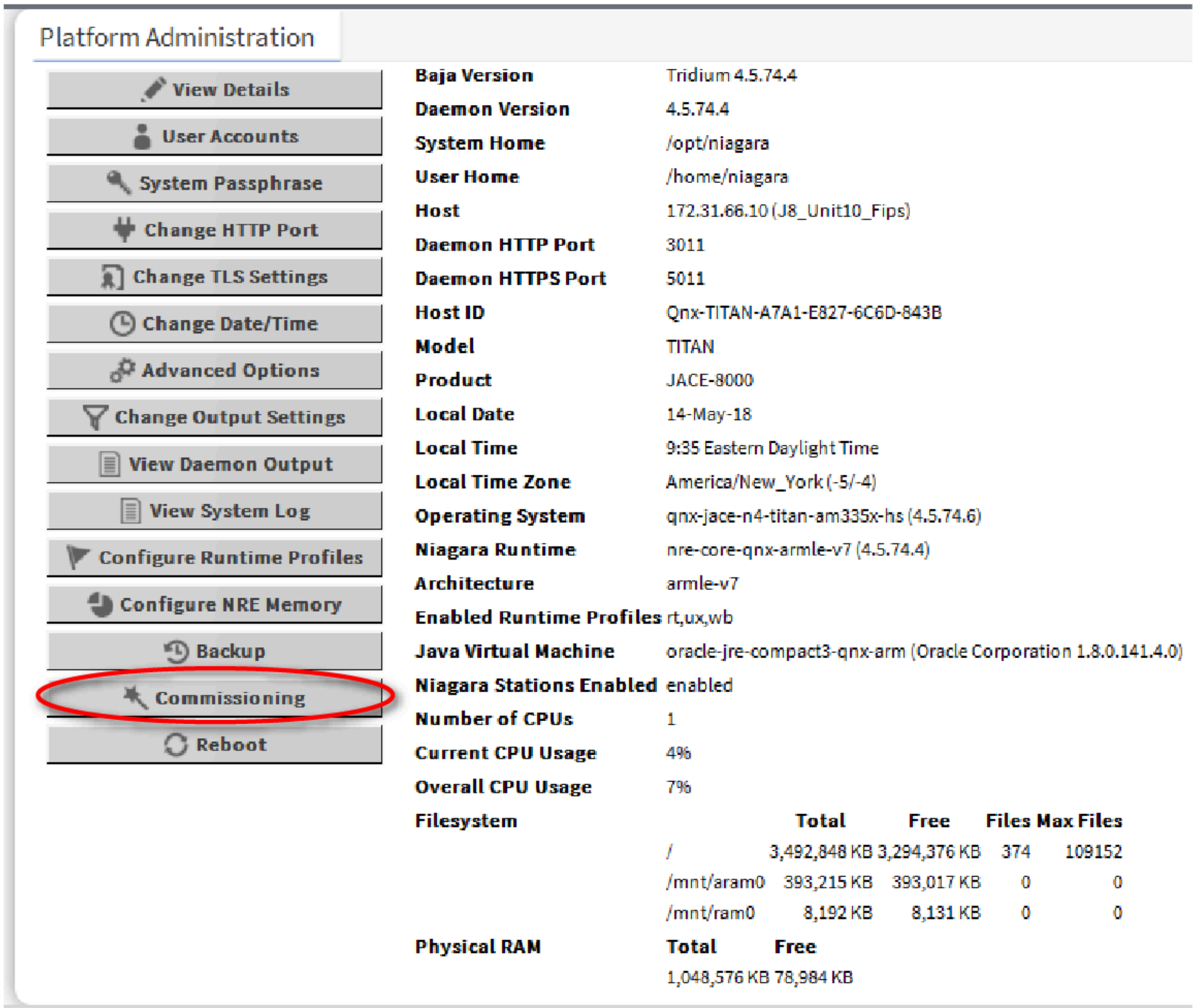
CAUTION: The reboot after commissioning de-energizes all door lock relays. Card readers do not respond. This may leave doors locked (building occupants locked in or out) or unlocked (unauthorized access a possibility). Plan ahead, and be prepared for how to deal with the system being down for five to ten minutes while the controller reboots.

Step 1. Make a platform connection to the controller by double-clicking the **Platform** node for the controller in the Nav tree.
The **Authentication** window opens.

Step 2. Enter the controller credentials.
The Nav Container View opens.

Step 3. Double-click the `Platform Administration` row in the table.

The Platform Administration view opens.



Baja Version	Tridium 4.5.74.4
Daemon Version	4.5.74.4
System Home	/opt/niagara
User Home	/home/niagara
Host	172.31.66.10 (J8_Unit10_Fips)
Daemon HTTP Port	3011
Daemon HTTPS Port	5011
Host ID	Qnx-TITAN-A7A1-E827-6C6D-843B
Model	TITAN
Product	JACE-8000
Local Date	14-May-18
Local Time	9:35 Eastern Daylight Time
Local Time Zone	America/New_York (-5/-4)
Operating System	qnx-jace-n4-titan-am335x-hs (4.5.74.6)
Niagara Runtime	nre-core-qnx-armle-v7 (4.5.74.4)
Architecture	armle-v7
Enabled Runtime Profiles	rt,ux,wb
Java Virtual Machine	oracle-jre-compact3-qnx-arm (Oracle Corporation 1.8.0.141.4.0)
Niagara Stations Enabled	enabled
Number of CPUs	1
Current CPU Usage	4%
Overall CPU Usage	7%

Filesystem

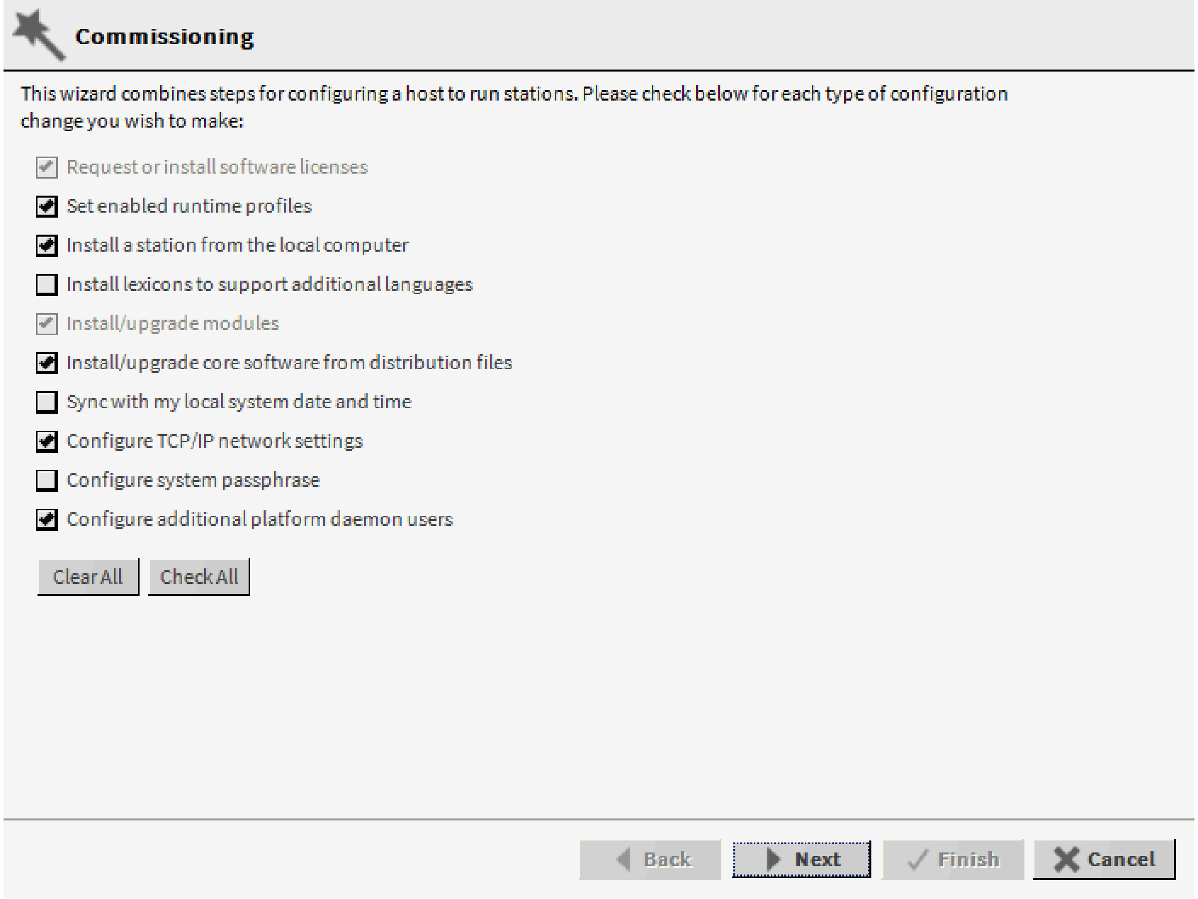
	Total	Free	Files	Max Files
/	3,492,848 KB	3,294,376 KB	374	109152
/mnt/aram0	393,215 KB	393,017 KB	0	0
/mnt/ram0	8,192 KB	8,131 KB	0	0

Physical RAM

Total	Free
1,048,576 KB	78,984 KB

Step 4. Click the **Commissioning** button.

The **Commissioning** wizard opens.



Commissioning

This wizard combines steps for configuring a host to run stations. Please check below for each type of configuration change you wish to make:

☑ Request or install software licenses

☑ Set enabled runtime profiles

☑ Install a station from the local computer

□ Install lexicons to support additional languages

☑ Install/upgrade modules

☑ Install/upgrade core software from distribution files

□ Sync with my local system date and time

☑ Configure TCP/IP network settings

□ Configure system passphrase

☑ Configure additional platform daemon users

Step 5. Follow the wizard, clicking **Next** until you configure all options.

Step 6. On the Software Installation page, click **Upgrade All out of Date** and click **Next**.

Step 7. After reviewing all changes, click **Finish**.
Commissioning begins.

CAUTION: Do not interrupt the commissioning process. If you interrupt, you may not be able to restore the station.

Step 8. When prompted, click **Close**.
After the commissioning process is complete, the controller reboots. During the reboot, any upgrades to the database required for the new version are automatically installed.

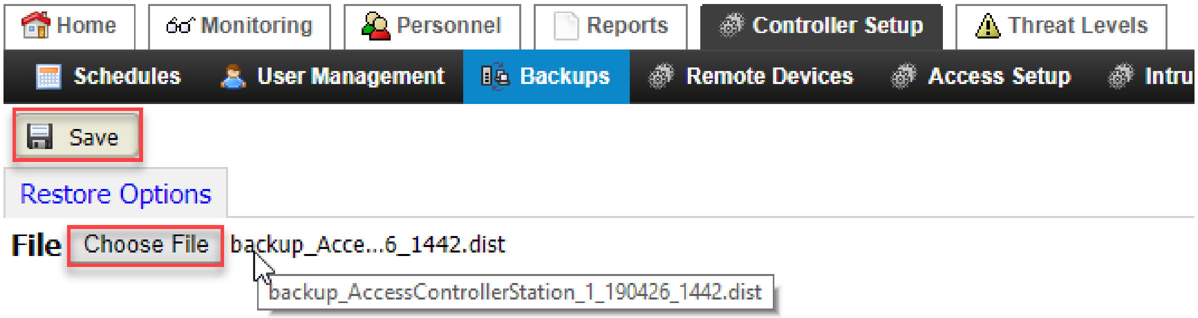
Restoring a controller station from a distribution file using the web UI

A distribution file is used to upgrade only the software (the platform did not change), or to upgrade to a new controller that is the same model as the old controller. Upon restore, the system automatically re-encrypts the stored keyring to the key material file that is unique to each controller. This ensures adequate security for all encrypted passwords. This procedure works for a Supervisor or a controller station.

Prerequisites:
You have a distribution file backup of the station. You are using the web UI.

Step 1. Log in to the platform, and click **Controller (System) Setup** > **Backups**.
The Backups view opens.

Step 2. Click **Restore**.
The Restore Options tab opens.



Step 3. Click **Choose File** and browser to locate the distribution (.dist) file.

Step 4. Click **Save**.
The system restores the station.

Restoring a controller station from a distribution file using Workbench

A software upgrade may require that you restore the controller station from a backup .dist file. This procedure works for a controller station only. You cannot restore a Supervisor station from a backup .dist file.

Prerequisites:
A recent distribution (.dist) of the station exists.

Step 1. Open Workbench in the newly-installed build.

Step 2. In the Nav tree, right-click on the **Platform** node and choose **Views** > **Distribution File Installer**.
The Distribution File Installer defaults to the `C:/Niagara/<framework version>/cleanDist` folder (where `<framework version>` represents the version of software).

Step 3. Use the buttons at the bottom of the view to initiate a restoration of your backed-up controller station to the newly installed station directory.
If you just upgraded the controller software and chose to install the platform daemon during the software installation process, your existing station may not start automatically with a new platform daemon.

Step 4. Maintaining your platform connection, change views to the Application Director view and select the newly restored station.

Step 5. To configure auto-start, enable the **`Auto-Start`** property.

Step 6. To start the station, click the **Start** button.
The station is now ready. A Supervisor station should communicate successfully with any subordinate stations, which should operate normally.

Step 7. To log in to the station, double-click the station entry.

Restoring a copied controller station to a new platform

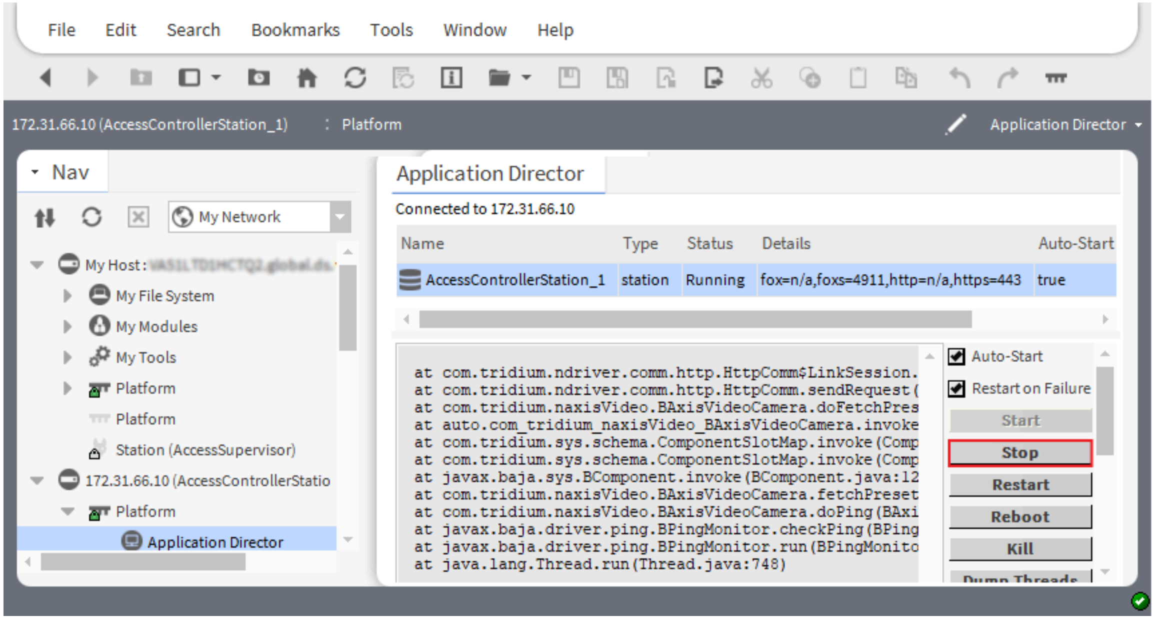
A copied station installs the station files from a previous controller to a controller that is a different model. This procedure works for a Supervisor or controller station.

Prerequisites:
The new controller is running Niagara 4.9 or later. You have a station copy that was made before disassembling the old controller. You are working in Workbench running on a PC.

First you stop the new station, then copy the hardware certificates and software licenses folder, followed by copying the backed-up station.

Step 1. Open a platform connection to the remote controller.

Step 2. Stop the station using the Application Director.



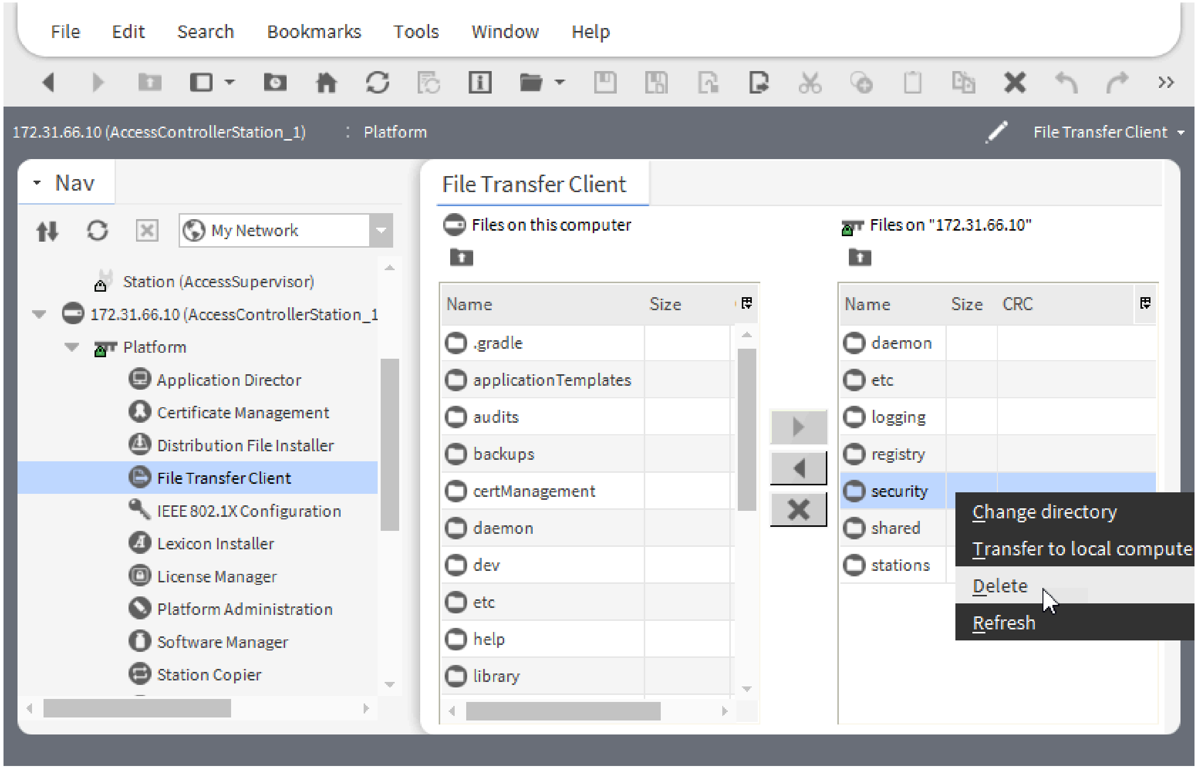
Connected to 172.31.66.10

Name	Type	Status	Details	Auto-Start
AccessControllerStation_1	station	Running	fox=n/a,foxs=4911,http=n/a,https=443	true

```
at com.tridium.ndriver.comm.http.HttpComm$LinkSession.
at com.tridium.ndriver.comm.http.HttpComm.sendRequest(
at com.tridium.naxisVideo.BAxisVideoCamera.doFetchPres
at auto.com_tridium_naxisVideo_BAxisVideoCamera.invoke
at com.tridium.sys.schema.ComponentSlotMap.invoke(Comp
at com.tridium.sys.schema.ComponentSlotMap.invoke(Comp
at javax.baja.sys.BComponent.invoke(BComponent.java:12
at com.tridium.naxisVideo.BAxisVideoCamera.fetchPreset
at com.tridium.naxisVideo.BAxisVideoCamera.doPing(BAxi
at javax.baja.driver.ping.BPingMonitor.checkPing(BPing
at javax.baja.driver.ping.BPingMonitor.run(BPingMonito
at java.lang.Thread.run(Thread.java:748)
```

☑ Auto-Start
☑ Restart on Failure

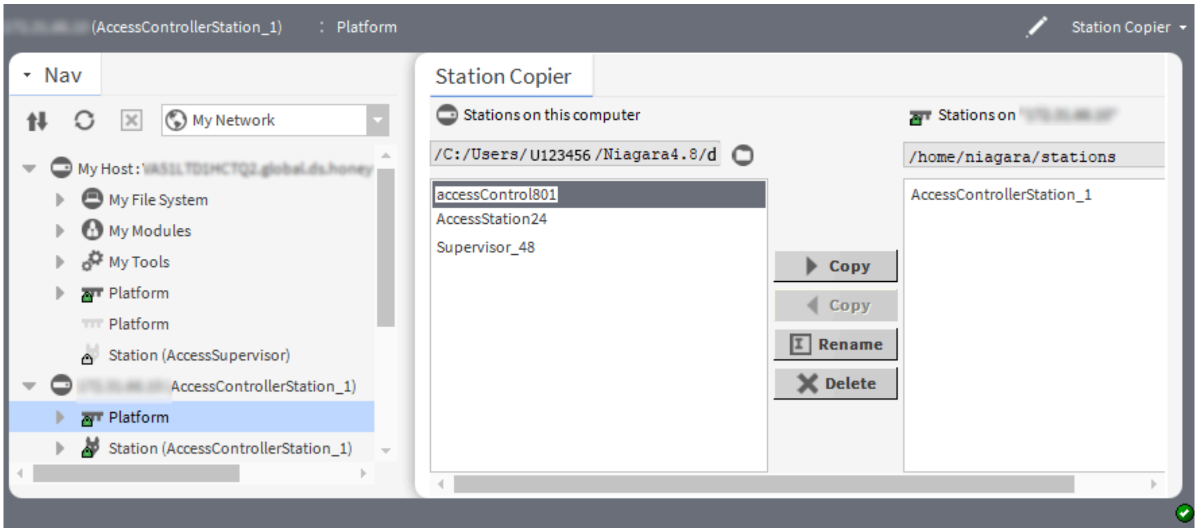
Step 3. Open the File Transfer Client and, on the controller side, delete the `security` folder on the controller side (the `security` folder is in the `/Niagara` path).



Step 4. Navigate to the location that contains the backup of the `security` folder.

Step 5. To restore the backup `security` folder to the controller's `/Niagara` folder, select the folder in the left pane and click the copy button (▶).

Step 6. To copy the station, double-click the **Station Copier** Platform utility.
The utility opens.


[redacted] (AccessControllerStation_1) : Platform
Station Copier
Nav
My Network
My Host : [redacted]
My File System
My Modules
My Tools
Platform
Platform
Station (AccessSupervisor)
[redacted] AccessControllerStation_1)
Platform
Station (AccessControllerStation_1)
Station Copier
Stations on this computer
Stations on [redacted]
/C:/Users/ U123456 /Niagara4.8/d
/home/niagara/stations
accessControl801
AccessStation24
Supervisor_48
AccessControllerStation_1
Copy
Copy
Rename
Delete

Step 7. Navigate to the folder in the User Home that contains the station, select the station in the left pane, and click **Copy**.

The station may be under an earlier version of Niagara.

Starting the restored controller station

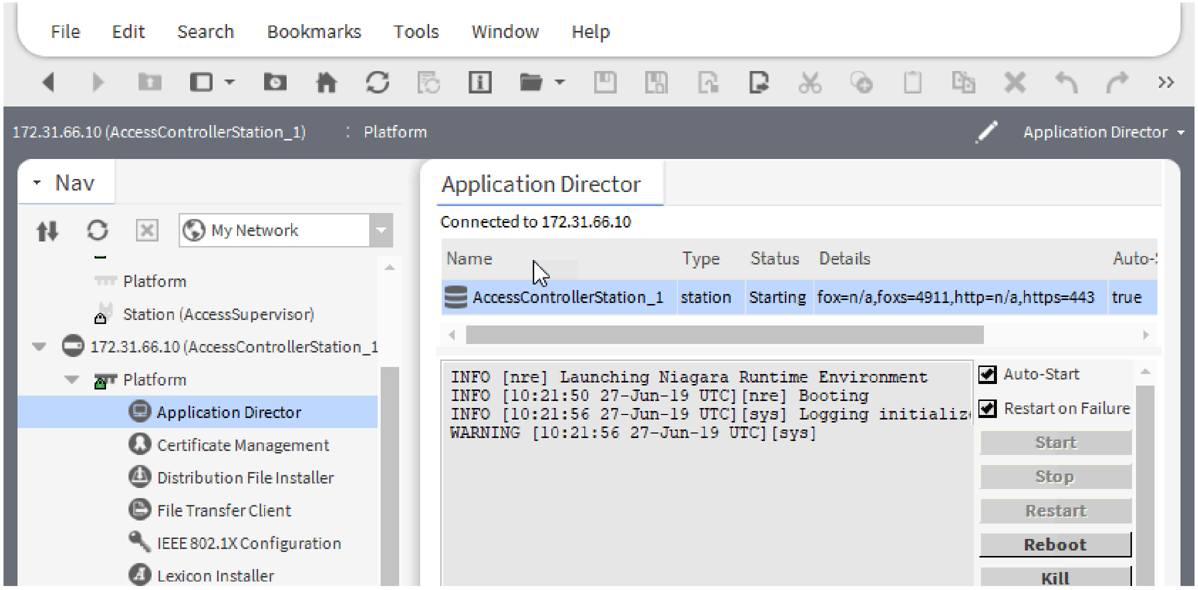
After restoring a station from a `.dist` file, you can perform the following task to restart it.

Prerequisites:
You have restored a station from a .dist file. You are working in Workbench.

Step 1. Open a platform connection to the restored controller.

Step 2. If the system reports that it is unable to verify the host identity, verify that both **`Issued By`** and **`Subject`** contain `Niagara4`, and click **Accept**.

Step 3. Open the Application Director and verify that the station started or is starting.
If you chose to install the platform daemon during the software installation process, your existing station may not start automatically with the new platform daemon.



Connected to 172.31.66.10

Name	Type	Status	Details	Auto-:
AccessControllerStation_1	station	Starting	fox=n/a,foxs=4911,http=n/a,https=443	true

```
INFO [nre] Launching Niagara Runtime Environment
INFO [10:21:50 27-Jun-19 UTC][nre] Booting
INFO [10:21:56 27-Jun-19 UTC][sys] Logging initializ
WARNING [10:21:56 27-Jun-19 UTC][sys]
```

☑ Auto-Start
☑ Restart on Failure

Step 4. If the station is not already starting, click the **Start** button.

Step 5. Confirm that the station has started (Status reports `Running`).

Step 6. To configure the station to start automatically in the event of an unexpected failure, enable the **`Auto-Start`** property.

`Auto-Start`

- If the electrical grid drops power to the building, an UPS (Uninterruptible Power Supply) or other backup battery can maintain power to the controller and its access network as long as is practical.
- If an emergency generator starts, the controller, access network, door locks and sensors should be powered by critical circuits to the extent that the company considers physical security to be a priority.
- If power to the controller ultimately fails, the system backs up the station automatically.
- When power is restored, the platform should automatically start the station and restore physical security to the building (unless the building's occupants over-road the door locks) with no operator action.

`Restart on Failure`

- If the station fails, it automatically attempts to restart.
- A **`Failure Reboot Limit`** (defaults to three attempts) defines how many times a station attempts to restart within a specific **`Failure Reboot Limit Period`** (defaults to 10 minutes). You can configure both.

Step 7. To log in to the station, double-click the station entry in the Nav tree.

Result

The station is now upgraded. A Supervisor station should communicate successfully with any subordinate stations, which should operate normally.

Importing a server certificate into an upgraded platform/station

After upgrading software, you import the exported server certificate back into a platform/station. Do this for each Supervisor PC and platform/station. This procedure is not required by the Workbench stores because Workbench is always a client, never a server.

Prerequisites:

You are working in Workbench running on a PC.

Step 1. Open a platform connection to the platform and double-click the **Certificate Management** utility or right-click **Platform**, and click **Views** > **Certificate Management**.
The platform/station's User Key Store tab opens.

Step 2. Click **Import** and navigate to the folder that contains your backed-up server certificates.

Step 3. Select the supervisor or controller certificate and click **Open**.
This certificate was exported with its private key.

Step 4. Supply the password that protects the private key and click **OK**.
The certificate opens.

Step 5. Confirm that the **`Alias`**, **`Issued By`**, and **`Subject`** are as expected and click **OK**.
The system imports the certificate.

Connecting to the upgraded controller station

Once upgraded, you connect to either a Supervisor or controller station.

Prerequisites:

You are working in Workbench running on the Supervisor PC.

Step 1. Right-click the station in the Nav tree and click **Connect**.
The **Authentication** window opens.

Step 2. Enter the admin station credentials.
The Platform Setup view opens.

Step 3. To change the display names, enter new names and click **Update Display Names**.

Step 4. To keep the network settings as they are, click **Reload Without Changes**.
The **Guided Setup Tour** window opens.

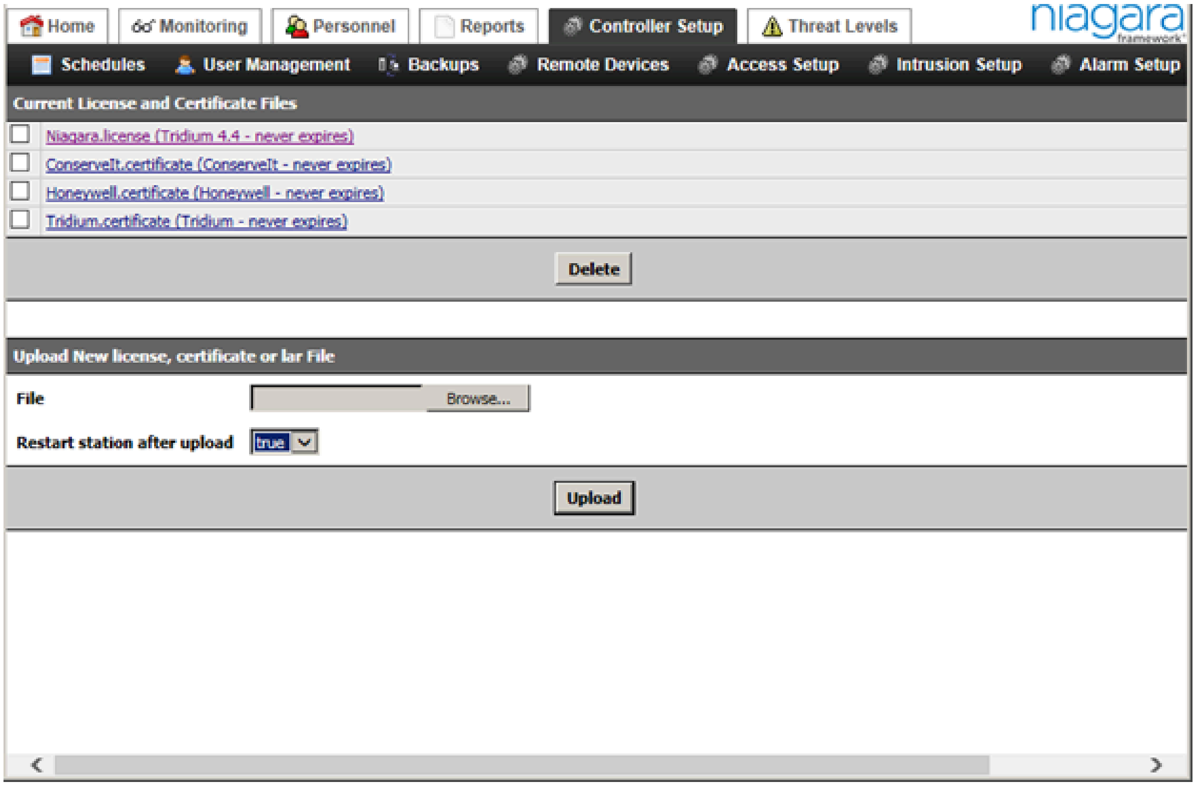
Step 5. If you do not need the tour, select **Skip Guided Setup** and click **Ok**.

Upgrading a license using the web UI

Updating a license is similar to installing a new license. The License Manager for updating a license is available under the station in Workbench and in the web UI. This procedure uses the web UI.

Prerequisites:
The new license is for a software version that is greater than or equal to the version you are upgrading from.
You are performing this procedure during off hours when few people require access to the building.

Step 1. Navigate to **Controller (System) Setup** > **Miscellaneous** > **License Manager**.
The LicensePlatformService view opens.



Current License and Certificate Files

□ Niagara.license (Tridium 4.4 - never expires)
□ ConserveIt.certificate (ConserveIt - never expires)
□ Honeywell.certificate (Honeywell - never expires)
□ Tridium.certificate (Tridium - never expires)

Upload New license, certificate or lar File

File

Restart station after upload: true

Step 2. To select the license file to install, click the **Browse** button.

Step 3. Select `true` for **Restart station after upload**.
The system does not update the license until the station restarts.

Step 4. To continue, click **Upload**.
The controller reboots.

NOTE: While the controller reboots, all door lock relays are de-energized, and card readers do not respond. This may leave doors locked or unlocked, and building occupants may be locked out, or non-authorized people may gain access. Make sure to plan on how to deal with the system being down for 5-10 minutes while the controller reboots.

Rejoining a replacement remote controller to the Supervisor station

After the controller has been replaced, and the station has been configured, you will need to join the controller to the Supervisor to synchronize the cardholder database.

Step 1. Unplug your PC and plug in the network cable that was plugged into the old controller.

Step 2. If you are connected to a Supervisor PC, use Workbench to confirm the new controller has connected to the Supervisor.
Make sure that the network variables are set correctly, the ports are open, and communication can be established.

Step 3. To join the new controller station to the supervisor click **Controller Setup** > **Remote Devices** > **Station Manager**, discover and select the station in the table and click the Recovery button (⬇).

Step 4. Open the Station Manager and observe that the replication status for the newly-replaced controller reports `{ok}`.

Step 5. To confirm that access activity at the controller is shown in the Supervisor activity report, **Reports** > **Access History**.
The door open test should appear on this report.

Clearing browser cache after a license upgrade

You may need to upgrade a license if you are adding features to the installation.
If you update your license file you may need to clear your browser cache to view the updated file. The following steps may vary, depending on your browser version.

- Microsoft® Internet Explorer Select **Tools** > **Internet Options** and click **Delete Files...** under the Temporary Internet files heading. Then click the **Ok** button.
- Mozilla® Firefox™ do one of the following (depending on your version, the steps may vary).
  - Select**Tools** > **Clear Private Data** and click **Clear Private Data Now** with the Cache option checked.
  - Select**Tools** > **Clear Recent History...**, select the Cache option and click **Clear Now**.

Troubleshooting

These suggestions and procedures can help you resolve problems that occur when installing, upgrading, and maintaining stations.

Networking

To run through this checklist you need a computer that has Workbench installed. The computer must be on the same network as the remote controller(s).

Are you having networking issues?

You configure network properties in the operating system. Although you can view network settings using Workbench and the web UI, you configure them in the operating system.

Database

Do you have a MySQL or other database? Is it running?

If you do not have a database, you will need to download and install one. Refer to the *Software Installation* chapter.

If you are using a MySQL database, do you have the database driver in the `C:\Niagara\MySoftware\jre\lib\ext` folder, where `MySoftware` is your version of the system.

The driver filename is `mysql-connector-java-5.1.11-bin.jar`. Refer to the *Software Installation* chapter.

Platform

Is the daemon process running?

If not, or if a different (older or newer) version of the daemon is running than the one that comes with the version of the system you are using, you need to install the daemon (Windows **Start** menu, followed by expanding the software folder and clicking **Install Platform Daemon** command.

Is the platform running?

Launch the Enterprise Security, right-click **Platform**, click **Connect**, and log in with valid platform credentials.

Station

Is the station running?

If not, double-click the platform, double-click the **Application Director**, select the appropriate station template and click **Start**.

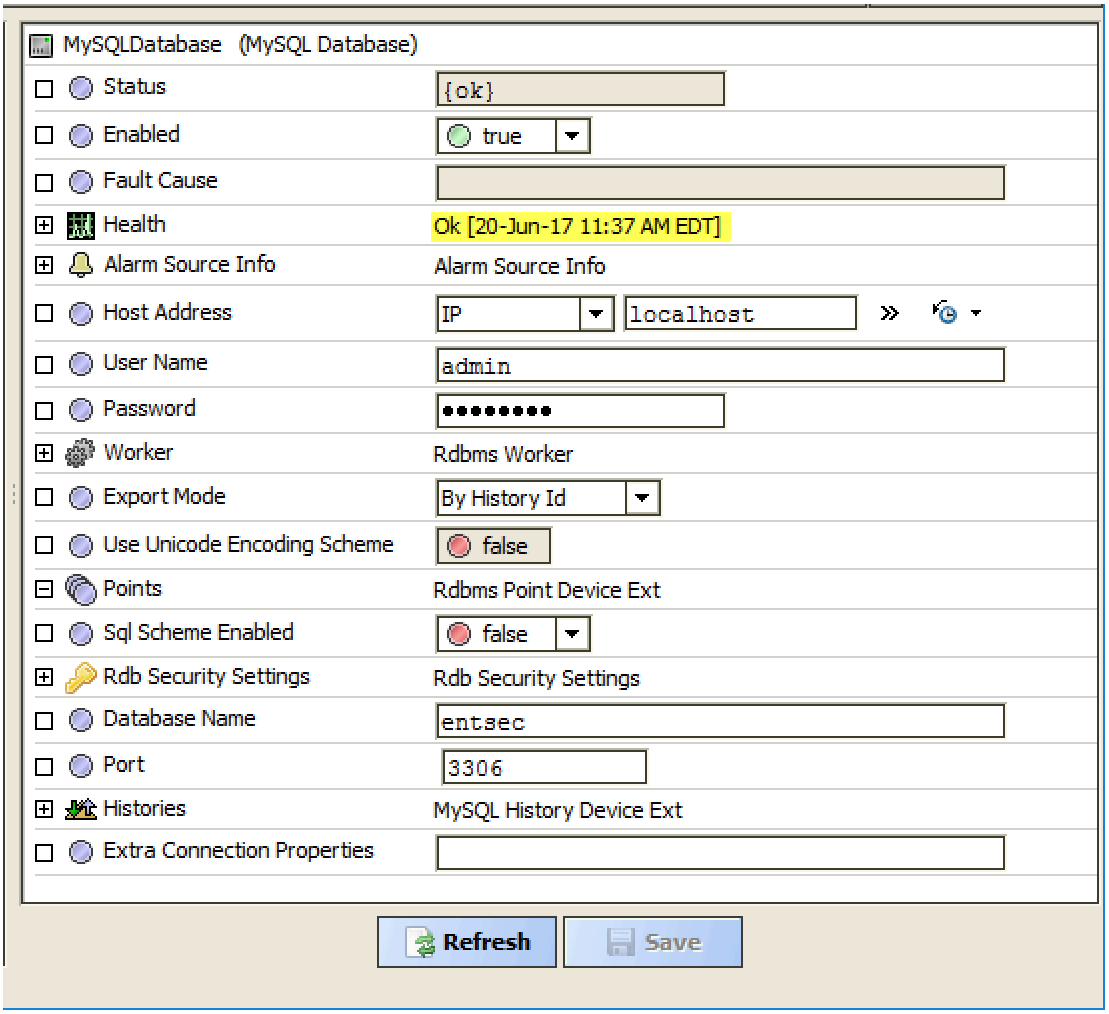
What messages are reported in the station log?

To view the log, double-click the **Application Director** and select the running station.

If you are using a MySQL database, can the station find the database?

To check this in Workbench, expand **Station** > **Config** > **Drivers** > **RdbmsNetwork**, and double-click **MySQLDatabase**.

Figure 41. MySQLDatabase properties



MySQLDatabase (MySQL Database)

☐ Status	{ok}
☐ Enabled	true
☐ Fault Cause	
⊞ Health	Ok [20-Jun-17 11:37 AM EDT]
⊞ Alarm Source Info	Alarm Source Info
☐ Host Address	IP localhost
☐ User Name	admin
☐ Password	●●●●●●●●
⊞ Worker	Rdbms Worker
☐ Export Mode	By History Id
☐ Use Unicode Encoding Scheme	false
⊟ Points	Rdbms Point Device Ext
☐ Sql Scheme Enabled	false
⊞ Rdb Security Settings	Rdb Security Settings
☐ Database Name	entsec
☐ Port	3306
⊞ Histories	MySQL History Device Ext
☐ Extra Connection Properties	

If the station and database are connected, the **Health** property reports Ok.

Other properties to confirm on this property sheet include:

- Is the **Host Address** correct?
- Are the **Username** and **Password** correct? These are the credentials required by the database, not your credentials.
- Is the **Database Name** correct?
- Is the **Port** correct?

Certificates

Does the host (Supervisor PC or remote controller) have a unique signed server certificate in its Key Store?

This certificate must be signed by a CA root certificate, either one belonging to your company, or one supplied by a third-party Certificate Authority. This certificate provides communication security when the platform functions as a server.

Does the host have the signed root CA certificate in its Trust Store?

This certificate provides communication security when the platform functions as a client.

Related information

- Software installation

Q and A

This topic covers questions users ask as they install and use the software.

A person authorized to manage the system is locked out.

The user type associated with the person's assigned role may be locked out because in attempting to log in, the person exceeded the maximum number of failed log-in attempts. At the Supervisor station, click **System Setup** > **User Management**, select the user type and click the **Clear Lockout** button, which displays at the top of the view. Clicking this button immediately clears the locked-out state.

Is there a way to reset a controller to the factory defaults?

Yes. Turn the controller off. Hold in the reset button, and turn the power back on.

CAUTION: These steps wipe all data off the controller including all software. Do not do this unless you fully understand the implication. If you are concerned about losing data, back up the station before you restore factory defaults.

For more information, refer to the *JACE-8000 Install and Startup Guide*

I scheduled a report to be sent by email, but the recipient did not receive the report.

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

When installing a new controller, the Change Platform Defaults Wizard displays these messages when I attempt to create the System Passphrase: "Request to platform daemon at ... failed: System Pw: Failed to check system password," and "Invalid passphrase, factory default value provided."

You must change the password. You cannot use the factory default passwords.

The video from a camera appears stretched out, distorted or has black bars on the sides.

The camera's **`Preferred Resolution`** may be linked to the video stream options and inherited. In some cases, this may adversely affect the aspect ratio of your streaming video. Try setting the camera's **`Preferred Aspect Ratio`** to the `Standard Definition` option.

These camera options are available by clicking **Controller Setup** > **Remote Devices** > **Remote Drivers** followed by double-clicking the driver row for the camera or DVR in the table, clicking the **Cameras** tab, and double-clicking the camera row in the table.

I have a database that is configured and reports {ok}, but when I try to add records to it I get "Cannot display page, HTTP ERROR 500, Problem accessing /ord. Reason: password must be at least 112 bits"

You have a license for FIPS mode and a station password does not meet the FIPS minimum requirement of a 14-character password (112 bits).

My xprotect camera will not connect or it connects, but drops off-line.

Confirm that you have only one xprotect driver module in the `c:\Niagara\MySoftware\modules` folder. The name of the driver module is: `xprotect-wb.jar`. Delete any other driver files.

I created a MySQL database and successfully ping'ed it to confirm that it is on line. Even so, my station indicates that the database is down.

Did you download the Connector/J from the MySQL web site? If yes, did you rename it from its downloaded name to `mysql-connector-java.jar`? Finally, did you copy the renamed connector to your `niagara.home\jre\lib\ext` folder?

If you forgot any of these steps, do them now, restart your station and confirm that the database is running.

Adjusting controller memory

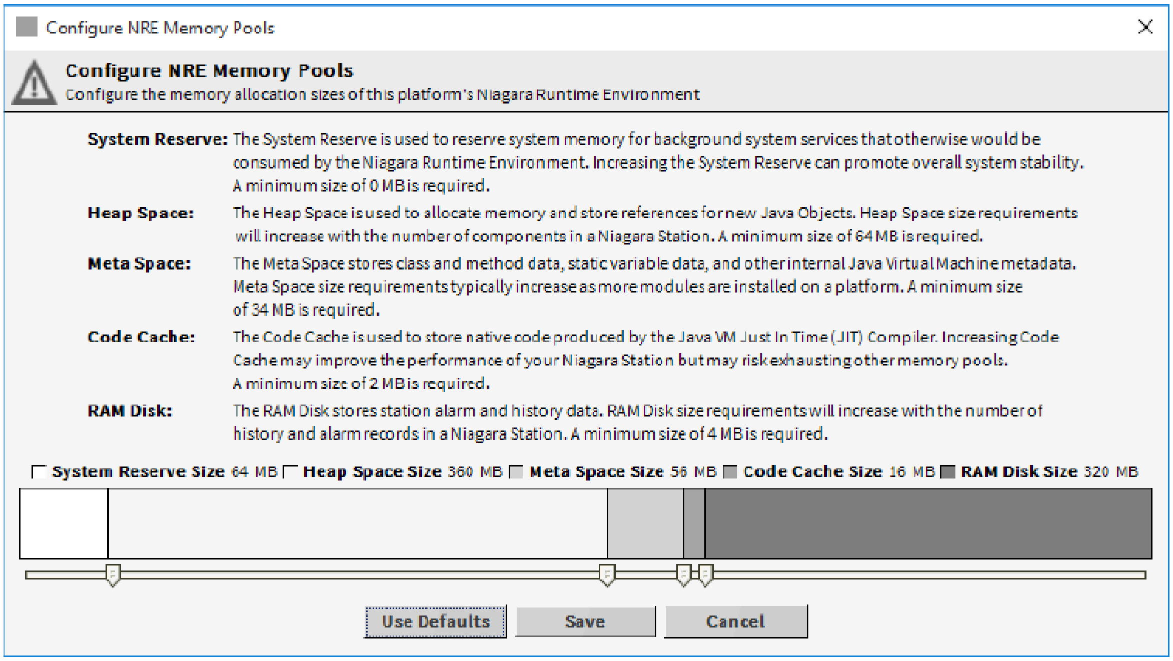
Large applications with multiple readers, persons, badges and zones may experience memory issues that cause remote station crashes. Adjusting the NRE (Niagara Runtime Environment) memory pools can provide room for station operations.

Prerequisites:
You are using Workbench and are connected to a remote controller platform.

To adjust the memory pools values for Niagara Enterprise Security 4.10 follow the below mentioned steps:

Step 1. Double-click **Platform Administration.**
The **Platform Administration** view opens.

Step 2. Click **Configure NRE Memory Pools.**
The **Configure NRE Memory Pools** window opens.



Configure NRE Memory Pools

Configure NRE Memory Pools
Configure the memory allocation sizes of this platform's Niagara Runtime Environment

System Reserve: The System Reserve is used to reserve system memory for background system services that otherwise would be consumed by the Niagara Runtime Environment. Increasing the System Reserve can promote overall system stability. A minimum size of 0 MB is required.

Heap Space: The Heap Space is used to allocate memory and store references for new Java Objects. Heap Space size requirements will increase with the number of components in a Niagara Station. A minimum size of 64 MB is required.

Meta Space: The Meta Space stores class and method data, static variable data, and other internal Java Virtual Machine metadata. Meta Space size requirements typically increase as more modules are installed on a platform. A minimum size of 34 MB is required.

Code Cache: The Code Cache is used to store native code produced by the Java VM Just In Time (JIT) Compiler. Increasing Code Cache may improve the performance of your Niagara Station but may risk exhausting other memory pools. A minimum size of 2 MB is required.

RAM Disk: The RAM Disk stores station alarm and history data. RAM Disk size requirements will increase with the number of history and alarm records in a Niagara Station. A minimum size of 4 MB is required.

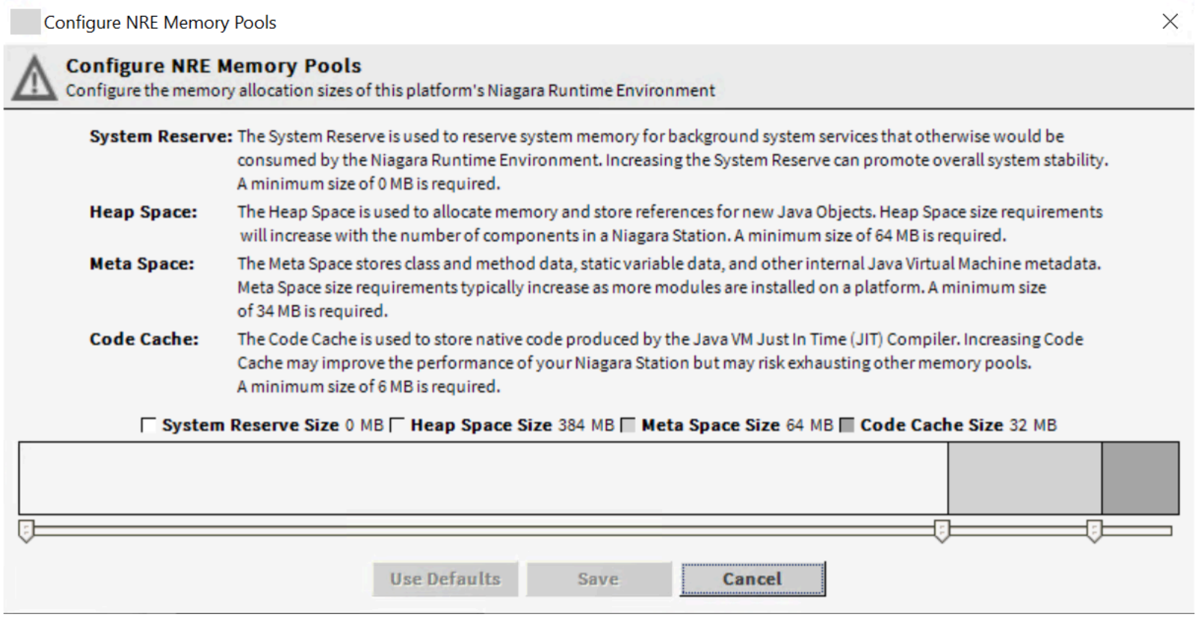
□ **System Reserve Size** 64 MB □ **Heap Space Size** 360 MB □ **Meta Space Size** 56 MB ▨ **Code Cache Size** 16 MB ■ **RAM Disk Size** 320 MB

Step 3. Using the sliders, adjust the memory pools values as per requirement and click **Save**:

- System Reserve Size: 64 MB
- Heap Space Size: 360 MB
- Meta Space Size: 56 MB
- Code Cache Size: 16 MB
- Ram Disk Size: 320 MB

This will provide adequate memory to accommodate the needs of Niagara Enterprise Security 4.10

NOTE: By default the memory values forNiagara Enterprise Security 4.11 are set as follows:



Configure NRE Memory Pools

Configure NRE Memory Pools
Configure the memory allocation sizes of this platform's Niagara Runtime Environment

System Reserve: The System Reserve is used to reserve system memory for background system services that otherwise would be consumed by the Niagara Runtime Environment. Increasing the System Reserve can promote overall system stability. A minimum size of 0 MB is required.

Heap Space: The Heap Space is used to allocate memory and store references for new Java Objects. Heap Space size requirements will increase with the number of components in a Niagara Station. A minimum size of 64 MB is required.

Meta Space: The Meta Space stores class and method data, static variable data, and other internal Java Virtual Machine metadata. Meta Space size requirements typically increase as more modules are installed on a platform. A minimum size of 34 MB is required.

Code Cache: The Code Cache is used to store native code produced by the Java VM Just In Time (JIT) Compiler. Increasing Code Cache may improve the performance of your Niagara Station but may risk exhausting other memory pools. A minimum size of 6 MB is required.

□ **System Reserve Size** 0 MB □ **Heap Space Size** 384 MB ▨ **Meta Space Size** 64 MB ■ **Code Cache Size** 32 MB

- System Reserve Size: 0 MB
- Heap Space Size: 384 MB
- Meta Space Size: 64 MB
- Code Cache Size: 32MB

Connection errors

These errors you may see in the Station Manager view, in the **Station Error** window, or buried in a log after you click **Details**.

AlreadyParentedException ... Client credentials

Cannot complete reverse connection to address:ip:[address]

Attempting to connect the remote station to the Supervisor station from the standpoint of the Supervisor station. This error indicates that the remote station cannot find the Supervisor station. The Supervisor platform, which should be identified as localhost, is unknown to the system. This can happen if you are attempting a connection over a VPN (Virtual Private Network).

Cannot complete reverse connection to address: ip: [IP address of the remote controller], reverting to oldAddress

The connection timed out.

Cannot connect from remote station to local station

Attempting to connect the remote station to the Supervisor station from the standpoint of the Supervisor station. The attempt timed out.

Failure during remote configuration of station [station name]

Attempting to connect the remote station to the Supervisor from the standpoint of the remote station.

Failure during reverse side disabling of ‘[station name]’

Attempting to delete a station from the Station Manager view.

Mismatched station names: [station name1] != [station name2]

Attempting to connect the remote station to the Supervisor from the standpoint of the Supervisor station.

Removed local NiagaraStation for ‘[station name]’ even though reverse side could not be reached.

This message goes with “Failure during reverse side disabling of ‘[station name]’

Station name [station name] already exists, station names must be unique

Instead of adding the new station, click the Edit button (📝).

SysDef extension not in a valid state to change roles: {down}

Attempting to connect the remote station to the Supervisor station from the standpoint of the Supervisor station.

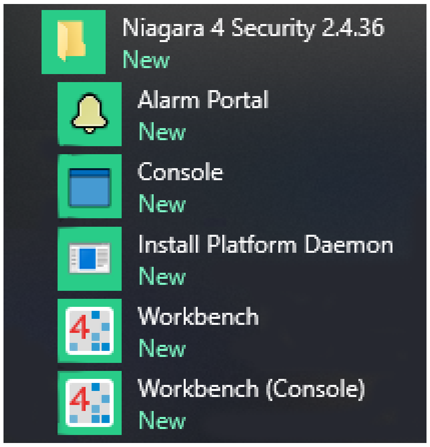
The station [station name] cannot be a supervisor

Attempting to connect the remote station to the Supervisor from the standpoint of the remote station. The software attempts to treat the Supervisor as a controller station.

Installing the platform daemon

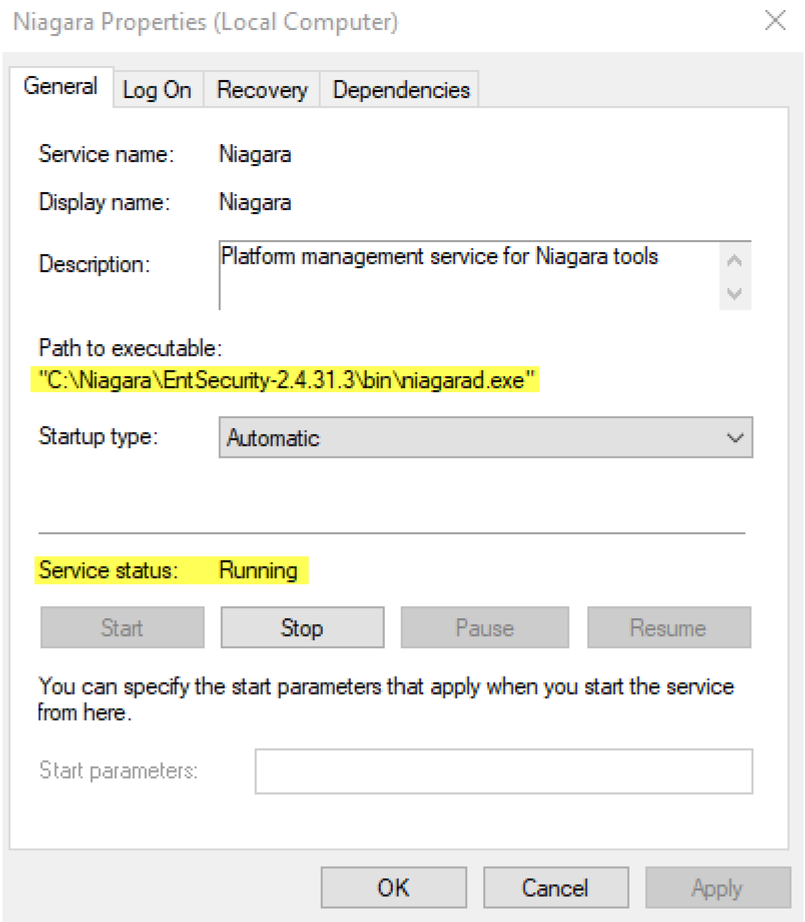
To run a Supervisor station on a PC, the system requires the installation of the platform management service (daemon). If you just installed Workbench for the first time, chose to have the installation program load the platform management service and launch the software, you can skip this procedure. You may need to re-install the platform daemon as a step in troubleshooting station problems.

Step 1. To start the platform management service, click Start, expand the software version you installed, and click Install Platform Daemon.



Briefly, a command prompt opens and the installation command runs. When the daemon is successfully installed, the command prompt closes.

Step 2. To verify that the platform daemon is running, click **Start** > **Control Panel** > **Administrative Tools** > **Services**, and double-click the Niagara service.



Service name: Niagara

Display name: Niagara

Description: Platform management service for Niagara tools

Path to executable:
"C:\Niagara\EntSecurity-2.4.31.3\bin\niagarad.exe"

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Make a mental note of the location of the daemon/Niagara service file: niagarad.exe.

Notice that you can check the status of the Niagara service, stop, pause, and resume it.

A compatible platform daemon/service works with each version of Niagara that is installed on a PC, but only a single platform daemon can be running at a time.

Step 3. To reinstall the daemon once Workbench is running, click **Window** > **Console**.
This opens a command prompt at the bottom of the About view.

The console is inside the red rectangle.

Step 4. Type `plat installdaemon` and press **Enter**.

Verifying database services

Once you finish configuring the Supervisor's database services you should go back and verify that all services are functioning as expected. This procedure also applies when troubleshooting.

Prerequisites:
You are working in the web UI and are logged in to the Supervisor station with admin privileges. This procedure should follow a database driver installation, setting the Orion database, and a station reboot.

Step 1. If needed, click **System Setup** > **Miscellaneous** > **Configure Database**
The Configure Database view opens. The Database Services tab displays the status of the database services.

Step 2. Verify that all services are showing a status of `{ok}`. Check any associated error message to help

find the cause of any status other than `{ok}`.
If your MySQL database user name is “root,” you may receive an error. Open the MySQL Workbench, create a new user with a strong password, and update this view with the new User Name and Password.

Step 3. To save any changed settings, click the **Save** button at the top of the view.
The `Save` command opens the **Restart Station** window.

Step 4. To initiate a station restart, click the **Ok**.

Step 5. Verify settings after the station has restarted.

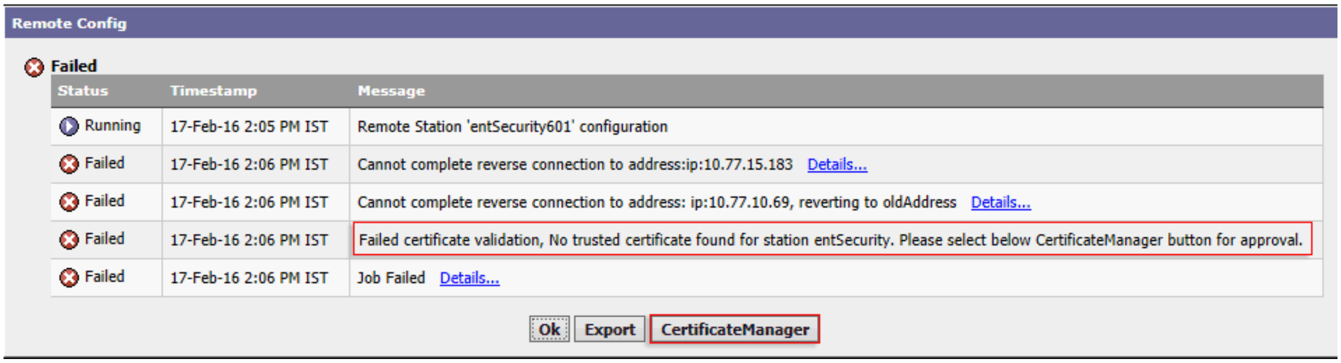
Failed certificate validation

All system components should use secure communication. Since each station (Supervisor and remote controller) can serve as both a client and a server, each station requires a root CA certificate in its User Trust Store and a server certificate signed by the root CA certificate in its User Key Store. Each connected device, such as a camera may also require a server certificate signed by a root CA certificate.

Failure to add or join

An attempt to add or join a remote station to a Supervisor station is an example of a server (the remote station) connecting to a client (the Supervisor station). If the remote controller station does not have a server certificate signed by a root CA certificate in the Supervisor station’s system or user trust store, the add or join fails and one or more error messages appear in the **Remote Config** window.

Figure 42. Foxs requires certificate approval for station join or add



Remote Config

Failed

Status	Timestamp	Message
Running	17-Feb-16 2:05 PM IST	Remote Station 'entSecurity601' configuration
Failed	17-Feb-16 2:06 PM IST	Cannot complete reverse connection to address:ip:10.77.15.183 Details...
Failed	17-Feb-16 2:06 PM IST	Cannot complete reverse connection to address: ip:10.77.10.69, reverting to oldAddress Details...
Failed	17-Feb-16 2:06 PM IST	Failed certificate validation, No trusted certificate found for station entSecurity. Please select below CertificateManager button for approval.
Failed	17-Feb-16 2:06 PM IST	Job Failed Details...

If you get this message because the remote station presented its self-signed certificate, you may approve the certificate and the add or join may complete, but a better solution is to figure out why the remote station presented its self-signed certificate or, if it presented a signed server certificate, why the root CA certificate that signed the server certificate is missing from the Supervisor station’s system or user trust store. Import the correct certificates into each station’s trust store and attempt the add or join again.

NOTE: Relying on a self-signed certificate provides encryption only. It cannot verify server identity, which is required to prevent man-in-the-middle attacks.

Failure to connect to a remote camera

A browser connection between a local station and a camera requires a secure connection. The browser, serving as a client to a remote camera, requires the root CA certificate in its trust store that signed the server certificate in the remote camera.

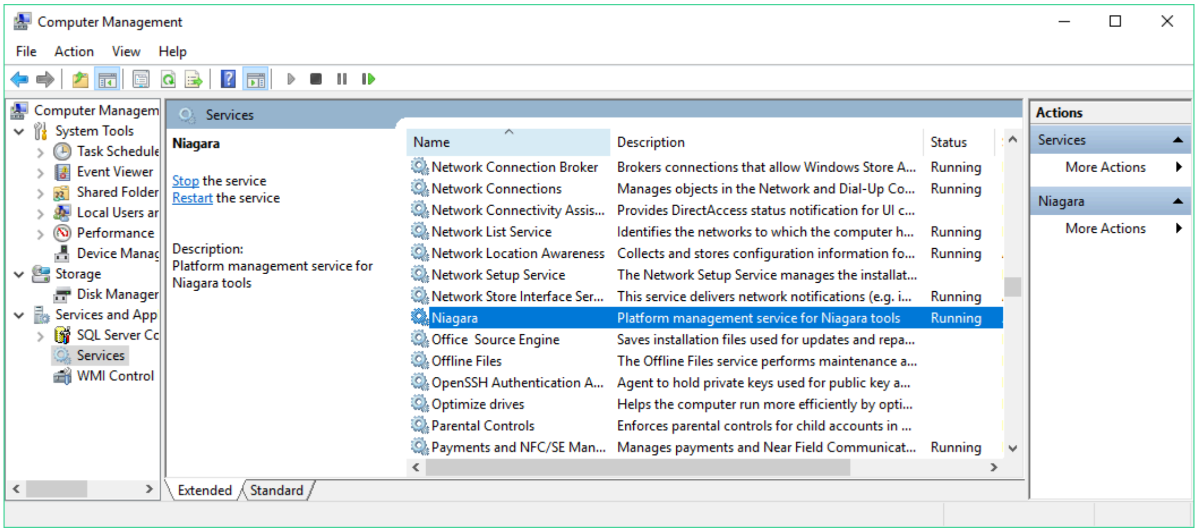
If these certificates are not in place, the camera will not connect to the browser, and through the browser to the station. Refer to the “System Security” chapter in this document for how to work with certificates.

Stopping and starting the Niagara service

This topic describes how to stop the Niagara service under Windows Services.

Step 1. On a Windows 10 system, click the **Start** menu and type **Computer Management** and click to select it.
The operating system's **Computer Management** window opens with three vertical panes.

Step 2. In the central pane, double-click **Services and Applications**, then double-click **Services**.
The system displays all services in the central pane.



Niagara

Stop the service
Restart the service

Description:
Platform management service for Niagara tools

Name	Description	Status
Network Connection Broker	Brokers connections that allow Windows Store A...	Running
Network Connections	Manages objects in the Network and Dial-Up Co...	Running
Network Connectivity Assis...	Provides DirectAccess status notification for UI c...	
Network List Service	Identifies the networks to which the computer h...	Running
Network Location Awareness	Collects and stores configuration information fo...	Running
Network Setup Service	The Network Setup Service manages the installat...	
Network Store Interface Ser...	This service delivers network notifications (e.g. i...	Running
Niagara	Platform management service for Niagara tools	Running
Office Source Engine	Saves installation files used for updates and repa...	
Offline Files	The Offline Files service performs maintenance a...	
OpenSSH Authentication A...	Agent to hold private keys used for public key a...	
Optimize drives	Helps the computer run more efficiently by opti...	
Parental Controls	Enforces parental controls for child accounts in ...	
Payments and NFC/SE Man...	Manages payments and Near Field Communicat...	Running

Step 3. To stop the service, right-click on the Niagara service and select **Stop** or **Restart**.

Step 4. To start the stopped service, right-click on the Niagara service and click **Start**.

Photo ID configuration troubleshooting

These conditions relate specifically to PhotoID.

I changed a property, but it did not change in the database.

Make sure that you saved the change before leaving the view.

I cannot connect to my PhotoID station.

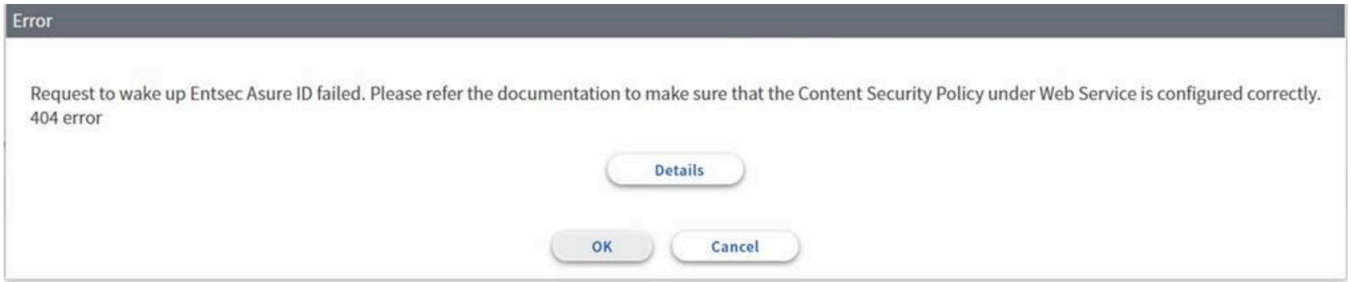
Make sure that you have a good connection from the Supervisor to the PhotoID host platform. If the Photo ID platform does not have a fixed IP address, the address may have changed.

Also, make sure that the EntsecAsureID applet is running and has the correct settings. If settings have changed, you may need to restart the applet, verify that you have a good Obix Network connection, and ping the device to confirm the connection.

The EntsecAsureID rejects credentials. I tried using an existing user. I created a new user with all roles. None will log in. I also tried each authentication scheme, but to no avail. Can you help me set up the obix user so it will log in?

The framework requires a special machine-to-machine user and password whose configuration defines the `HttpBasicScheme` for server authentication and a user role with permissions that include read access to the Obix Network. If you are setting up a new system, you must create and configure this user. If you upgraded your station from NiagaraAX, the migration tool created an oBix user for you. You need to confirm the configuration, set the password and configure the Photo ID Settings.

After clicking the Discover button to discover a template or template data, EntsecAsureID displays this message.



Request to wake up Entsec Asure ID failed. Please refer the documentation to make sure that the Content Security Policy under Web Service is configured correctly.
404 error

The **WebService** Content-Security-Policy HTTP header provider needs to be configured. Refer to "Configuring Asure ID secure communication" in the "Personnel setup" chapter of this guide.

Chapter 15. Glossary

The following glossary entries relate specifically to the topics that are included as part of this document.

To find more glossary terms and definitions refer to glossaries in other individual documents.

Alphabetical listing

Alarm Class

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.

web UI

web user interface refers to the framework software used to access a platform and station, which runs in a browser.

Orion database

A relational database system developed at Purdue University for managing uncertain, probabilistic data. Implementations of this database include MySQL and MSSQL.