LG MultiSITE^{TM} Supervisor Platform Software Manual

PROPRIETARY DATA NOTICE

This document, as well as all reports, illustrations, data, information, and other materials are the property of LG Electronics U.S.A., Inc., and are disclosed by LG Electronics U.S.A., Inc., only in confidence.

⊘ ***Do not throw away, destroy, or lose this manual.***

Please read carefully and store in a safe place for future reference.
Content familiarity required for proper installation.

The instructions included in this manual must be followed to prevent product malfunction, property damage, injury, or death to the user or other people. Incorrect operation due to ignoring any instructions will cause harm or damage. A summary of safety precautions begins on page 5.

For more technical materials such as submittals, engineering databooks, and catalogs, visit www.lghvac.com.

SOM_MultiSITE_Supervisor_Platform_05_17

For continual product development, LG Electronics U.S.A., Inc., reserves the right to change specifications without notice.

This document, as well as all reports, illustrations, data, information, and other materials are the property of LG Electronics U.S.A., Inc.

TABLE OF CONTENTS

CHAPTER 1 MultiSITE Supervisor Platform 10
Platform models 10
Embedded controllers 12
Windows-based controllers 14
Platform daemon (niagarad) 16
Platform daemon port 16
Platform credentials 16
Platform access without a platform connection 16
Platform daemon on a PC 16
Types of platform views 17
Opening a secure platform connection 18
Application Director (station management) 20
Distribution File Installer 28
File Transfer Client 36
Lexicon Installer 38
License Manager 40
Platform Administration 48
Commissioning 69
Software Manager 71
Station Copier 81
TCP/IP Configuration 94
Provisioning as a way to automate platform tasks 99
Upgrading a controller 108
Chapter 2 Platform Services 110
About Platform Services 110
PlatformServiceContainer parameters 112
SystemService (under PlatformServices) 117
Using platform services in a station 119
About the NtpPlatformService 120
Chapter 3 Platform Component Guides 125
platCrypto-CertManagerService 125
platform-DaemonSecureSession 125
platDataRecovery-DataRecoveryService 125
Components in platform module 126
Components in platHwScan 132
Components in platPower module 132

Components in platSerialQnx module 134
Chapter 4 Platform Plugin Guides........ 135
Plugins in platCrypto 135
Plugins in platDaemon module........ 141
Plugin in platDataRecovery........ 149
Plugins in platform module........ 150
Plugins in platHwScan........ 151
Plugins in platPower........ 151
Chapter 5 License Tools and Files 152
License-related tools 152
Workbench License Manager........ 153
Request License........ 157
About the local license database........ 158
About license archive (.lar) files 160
About Niagara license files 161
Global capacity licensing 171
Chapter 6 Time Zones 176
Time zones and terminology 176
Selecting a time zone 177

SAFETY INSTRUCTIONS

The instructions below must be followed to prevent product malfunction, property damage, injury or death to the user or other people. Incorrect operation due to ignoring any instructions will cause harm or damage. The level of seriousness is classified by the symbols described below.

TABLE OF SYMBOLS

⚠DANGER	This symbol indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	This symbol indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠CAUTION	This symbol indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
Note:	This symbol indicates situations that may result in equipment or property damage accidents only.
🛇	This symbol indicates an action that should not be performed.

This manual provides information about the LG MultiSITE™ Supervisor software platform for LG MultiSITE™ VM3 controller. It provides information about Niagara platform services, components and plugins, license tools and other topics related to a Niagara host.

Refer to the LG MultiSITE VM3 Installation Manual for installation and mounting instructions of the controller.

⚠DANGER

🛇 **Do not use or store flammable gas or combustibles near the unit.**
There is risk of fire, explosion, and physical injury or death.

Disconnect power before installing or servicing the unit.
There is risk of physical injury or death due to electric shock.

🛇 **Do not touch any exposed outdoor unit wiring, terminals, or other electrical components with tools or exposed skin. Only qualified technicians should install, use, or remove this unit.**
Improper installation or use may result in fire, explosion, electric shock, physical injury and/or death.

SAFETY INSTRUCTIONS

⚠WARNING

All electric work must be performed by a licensed electrician and conform to local building codes or, in the absence of local codes, with the National Electrical Code, and the instructions given in this manual.
If the power source capacity is inadequate or the electric work is not performed properly, it may result in fire, electric shock, physical injury or death.

⊘ **Do not change the settings of the protection devices.**
If the pressure switch, thermal switch, or other protection device is shorted and forced to operate improperly, or parts other than those specified by LG are used, there is risk of fire, electric shock, explosion, and physical injury or death.

Dispose of any packing materials safely.
Packing materials, such as nails and other metal or wooden parts may cause puncture wounds or other injuries.

Tear apart and throw away plastic packaging bags so that children may not play with them and risk suffocation and death.

⊘ **Do not install the MultiSITE VM3 unit if it will be exposed to rain or other precipitation.** ⊘ **Do not install the unit in a location exposed to open flame or extreme heat.** ⊘ **Do not touch the unit with wet hands.**
There is risk of fire, electric shock, physical injury and/or death.

⚠CAUTION

Wear protective gloves when handling equipment.

Sharp edges may cause personal injury.

SAFETY INSTRUCTIONS

Note:

Disconnect power before installing or servicing the unit.

There is risk of equipment damage or degraded performance.

MultiSITE VM3 unit is for use with select LG air conditioning systems only. 🛇 Do not attempt to use this unit with any other type of system.

There is risk of equipment damage or degraded performance.

Clean up the site after all procedures are finished, and check that no metal scraps, screws, or bits of wiring have been left inside or surrounding the controller or indoor units.

🛇 Do not allow water, dirt, or animals to enter the controller.

There is risk of unit failure or degraded performance.

🛇 Do not spill water or other liquid on the inside of the controller. 🛇 Do not drop the controller into water. If the unit is immersed in water or other liquid, contact your local authorized LG distributor for support.

There is risk of unit failure or degraded performance.

Remove all power to controller before attaching (plug in) or detaching (unplug) any option module.

There is risk of possible equipment damage.

🛇 Do not remove the controller’s cover.

No configurable or user-serviceable items (such as jumpers or a battery) require cover removal. All items are accessible as switches and connectors on the unit’s top, bottom, and side, or behind the unit’s front access door or microSD card shutter.

This device is only intended for use as a monitoring and control device. 🛇 Do not use it for any other purpose.

There is risk of data loss or equipment damage.

Before removing or inserting the microSD card, disconnect all power to the controller and use static discharge precautions.

There is risk of equipment damage.

The MultiSITE VM3 unit is not compatible with a Power-Over-Ethernet (POE) network. 🛇 Do not connect the controller on a network segment which carries power.

The unit may fail.

CERTIFICATIONS

The MultiSITE VM3 controller has the following agency listings, compliances, and certifications:

UL-916, Energy Management Equipment - Edition 4

FCC Part 15, Class B - Federal Communications Commission, with FCC Part 15, Subpart C - WiFi

ICES-003, Class B - Industry Canada Interference-Causing Equipment Standard

RoHS 2 (Restriction of Hazardous Substances), Directive 2011/65/EU.

CE CE Declaration of Conformity (Council Directive 004-108-EC)

ACMA, complies with the requirements of the relevant ACMA Standards. This document covers mounting and wiring of the following products.

COMPLIANCE AND APPROVALS

Federal Communications Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and

2. This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Canadian Department of Communications (DOC)

This device complies with Industry Canada License-exempt RSS standard(s). Operation is subject to the following two conditions: 1) this device may not cause interference, and 2) this device must accept any interference, including interference that may cause undesired operation of the device.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Approved Antenna Listing

- ANT-DB1-RAF-RPS

Transmitter Module Listing

- Contains Transmitter Module FCC ID: W98-12977
- Contains Transmitter Module IC: 8339A-12977

To comply with FCC and Industry Canada RF exposure limits for general population /uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CHAPTER 1 MULTISITE SUPERVISOR PLATFORM

About this guide

This guide provides information about the LG MultiSITE™ Supervisor software platform for LG MultiSITE™ VM3 controller. The guide provides details about Niagara platform services, components and plugins, license tools and other topics related to a Niagara host.

LG MultiSITE™ Supervisor will be referred to as MultiSITE Supervisor in this document. LG MultiSITE™ VM3 will be referred to as MultiSITE VM3 in this document.

The following topics are covered in this chapter:

- Platform models
- Platform daemon (niagarad)
- Types of platform views
- Provisioning as a way to automate platform tasks
- File locations
- Upgrading a controller

Platform is the name for everything that is installed on a host that is not part of a station. The platform interface provides a way to address all the support tasks that allow you to setup and support and troubleshoot a host.

Platform models

Among the two groups of MultiSITE Supervisor controllers (embedded controllers and Windows-based), there are different models, each of which has a host model text descriptor. You see this descriptor in the Station Manager view of a NiagaraNetwork (Host Model column), and also in platform views, such as Platform Administration, as well as the PlatformServices container of a station running on that host.

The following table lists various controller models starting with the host model text descriptor.

A few models (and the SoftJACE) listed are not compatible with Niagara 4, and are so noted. However, it is possible that some may exist on a job site where the Supervisor was migrated to N4.0, along with some number of controllers that are compatible. In addition, several models discontinued more than 10 years are not listed.

LonWorks®

BACnet and ASHRAE are registered trademarks of ASHRAE. 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, NiagaraAX Framework, and Sedona Framework are registered trademarks, and Workbench, WorkPlaceAX, and AXSupervisor, are trademarks of Tridium Inc. All other product names and services mentioned in this publication that is known to be trademarks, registered trademarks, or service marks are the property of their respective owners.

The following table lists the host models of JACE platforms.

Model description	Actual Model	Notes	Compatible with Niagara 4?
JNXS	JACE-NXS	Discontinued Win32-based (Windows XP Embedded), model before JACE-NXT series.	No
JNXT	JACE-NXT series	Discontinued Win32-based controller (Windows XP Embedded).	No
Jsoft	SoftJACE installed on user-supplied PC	Windows-based. This is different than a Supervisor for example, which appears instead as "Workstation".	No
JVLN	JACE-7 series (JACE-700)	Discontinued model, with more processing power than JACE-2/6 series.	No, the WiFi option for this controller is not supported.
NPM2	JACE-2 series	Discontinued QNX-based controller. Uses the IBM J9 JVM (Java Virtual Machine).	No
NPM3	JACE-3E series, introduced in mid 2013.	QNX-based controller, JACE-3E is between the JACE-2 series and the JACE-6E series in performance, and includes onboard SRAM for battery-less operation (if desired).	Yes
NPM6	JACE-6 series	Discontinued QNX-based, with more processing power than the JACE-2 series. Note that security controllers are not compatible.	Yes, except for security controller
NPM6E	JACE-6E, as well as "retrofit board" controllers JACE-603 and JACE-645.	QNX-based controllers. The JACE-6E is like a JACE-6, but includes onboard SRAM for battery-less operation (if desired). The JACE-603 and JACE-645 are retrofitted R2 JACE-403 and JACE-545 controllers.	Yes
TITAN	JACE-8000 series	QNX-based controller, with the most processing power and resource capacity of any controller. Includes onboard SRAM for operation without a battery, integral WiFi, and a USB port for backup/ restore usage using a USB flash drive. Plug-in option modules provide additional communications ports. Supports Niagara 4, and AX-3.8U1 (with the JACE-8000-AX license feature). Note that the USB Backup/Restore and WiFi functionality are not supported on a JACE-8000 platform running AX-3.8U1.	Yes, except when running older version of software
Workstation	User-supplied PC, for example, a Supervisor or engineering workstation.	Windows-based customer supplied PC that runs MultiSITE Supervisor, minimally.	Yes

Some platform views differ depending on the type of controller.

Embedded controllers

Sometimes called embedded JACE controllers, these include the JACE-8000 controllers as well as JACE-3,-6,-7 series models, all shipped with the QNX operating system. All use flash memory for file storage, Oracle's Sun Hotspot Java VM, and provide wired Ethernet connectivity.

The JACE-8000 platform, introduced with the release of Niagara 4, provides a number of exclusive features, such as integral WiFi (802.11b/g) support, backup and restore to and from a removable USB drive, and easy communications expansion using attachable modules.

JACE-8000 controllers support Niagara 4, as well as AX-3.8U1. Whereas the JACE-3,-6,-7 series controllers were originally released withNiagaraAX, and may be migrated to Niagara 4 if already running AX-3.8, or else configured from scratch using Niagara 4.

Backup Battery

For a number of controller models, the station provides a power monitoring component to track its AC power and backup battery level, with a configurable delay for orderly shutdown of the controller upon AC power failures. You access power monitoring in the PowerMonitorService in a running station.

JACE-6 and JACE-7 controller models use an onboard NiMH backup battery (nickel metal hydride), to preserve runtime data, and also allow continuous operation during brief power outages. The JACE-3E and JACE-6E controllers use integral SRAM to back up runtime data, but can also optionally use an onboard NiMH battery for continuous power event operation. The JACE-7 and JACE-603/JACE-645 models support an additional external 12V SLA (sealed lead acid) battery for backup usage.

Note:

A JACE-8000 controller has no backup battery. Instead, onboard SRAM preserves runtime data upon any power event. Therefore, its station's PlatformServices has no PowerMonitorService. For continuous operation across power events, an external battery-backed UPS must be used to power the controller.

Battery-less controllers

The JACE-8000 controller and previous JACE-3E and JACE-6E controllers include integral onboard SRAM, which preserves runtime data upon a power loss. By default, these controller platforms do not have batteries. An SRAM option card is also available for any JACE-6 and JACE-7 series controller. These controllers can operate without any backup battery, onboard NiMH or otherwise.

SRAM support works via a station platform service, the DataRecoveryService. This platform service continuously records all database changes in SRAM, and upon reboot from a power event, restores (plays back) these changes.

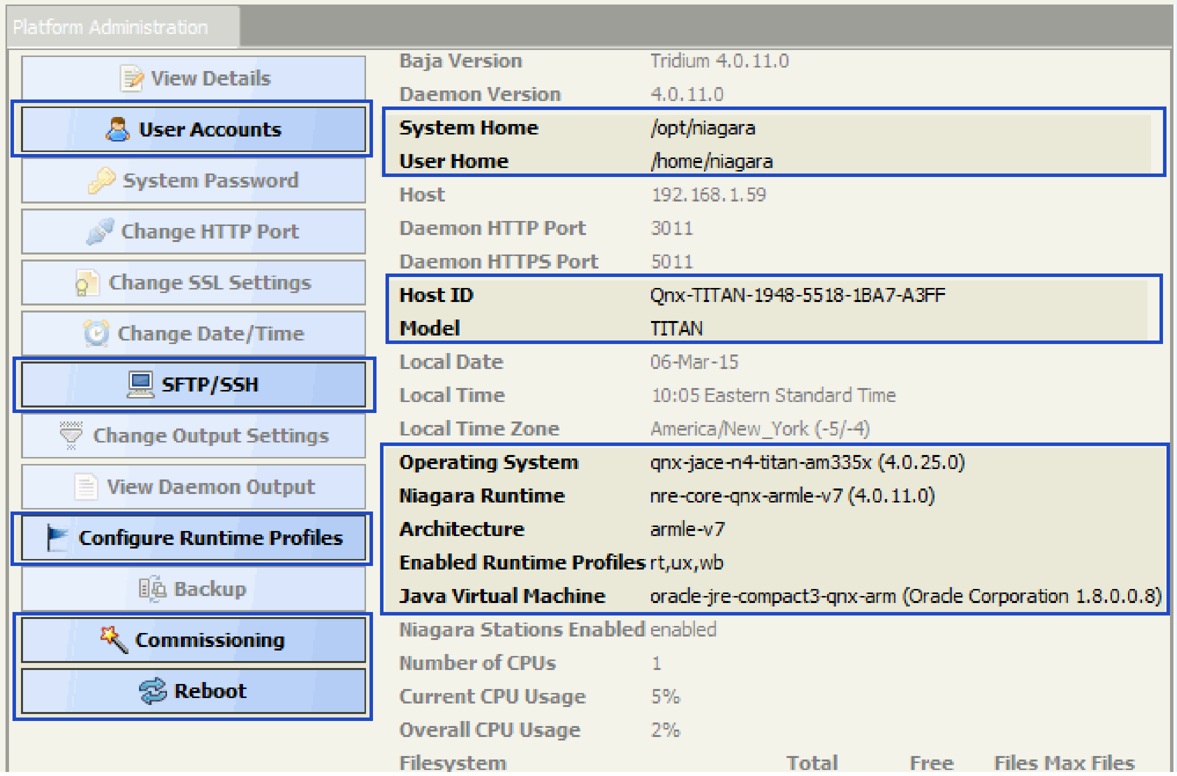
Except for a JACE-8000 controller, any SRAM-equipped controller can also have a backup battery, and be configured to use either SRAM or backup battery, or both. By default, its station's PlatformServices contains both the PowerMonitorService and the DataRecoveryService.

Due to our policy of continuous product innovation, some specifications may change without notification

Platform Administration on an embedded controller

The Platform Administration views available on an embedded controller differ from those that are available on a Windows-based platform. Platform Administration for a controller platform differs as shown in the figure below.

Figure 1: Platform Administration for a controller



Baja Version	Tridium 4.0.11.0
Daemon Version	4.0.11.0
System Home	/opt/niagara
User Home	/home/niagara
Host	192.168.1.59
Daemon HTTP Port	3011
Daemon HTTPS Port	5011
Host ID	Qnx-TITAN-1948-5518-1BA7-A3FF
Model	TITAN
Local Date	06-Mar-15
Local Time	10:05 Eastern Standard Time
Local Time Zone	America/New_York (-5/-4)
Operating System	qnx-jace-n4-titan-am335x (4.0.25.0)
Niagara Runtime	nre-core-qnx-armle-v7 (4.0.11.0)
Architecture	armle-v7
Enabled Runtime Profiles	rt,ux,wb
Java Virtual Machine	oracle-jre-compact3-qnx-arm (Oracle Corporation 1.8.0.0.8)
Niagara Stations Enabled	enabled
Number of CPUs	1
Current CPU Usage	5%
Overall CPU Usage	2%

Filesystem	Total	Free	Files	Max Files

- A User Accounts button is available.
- An Advanced options button is available.
- A Configure Runtime Profiles button is available.
- A Commissioning button and a Reboot button are available.
- Various data in the view (repeated in “View Details”) differ greatly from that for Windows hosts.

Due to our policy of continuous product innovation, some specifications may change without notification.

Windows-based controllers

Windows-based platforms in Niagara 4 include Windows-based Supervisor PC hosts and/or engineering workstations.

Note:

All JACE controllers that can run Niagara 4 use the QNX operating system. Prior Windows-based JACE controllers that run Windows XP Embedded are not supported.

File storage on Windows-based platforms is typically a hard drive, and the operating system is a minimum of Windows 7 Professional, with Windows 8 Professional often used. Alternatively, a Supervisor may run Windows Server 2012.

Most platforms use a 64-bit Windows OS (Win64-based). Although a Win64 Supervisor uses a 64-bit JVM (Java Virtual Machine) and different NRE core binaries, its platform interface is nearly identical to any Win32 based Supervisor.

For any Windows-based platform, the Platform Administration view differs from JACE controller platform's Platform Administration view.

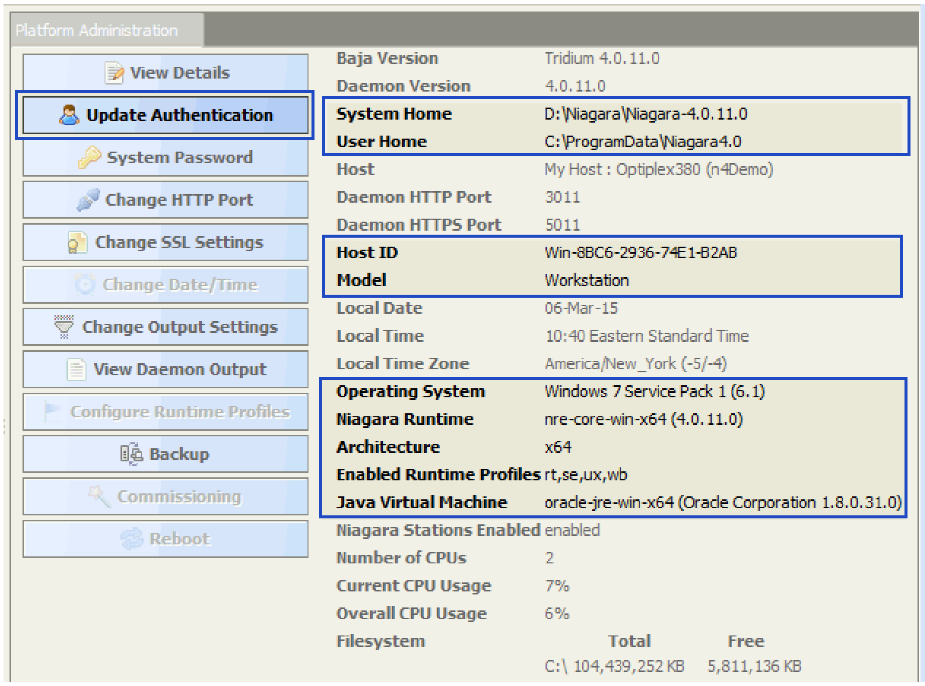
Note:

When connected to any Windows host, the TCP/IP Configuration platform view is always read-only. Intended configuration use is for JACE controllers only. On any Windows host, you configure TCP/IP and other network settings using the normal Windows Control Panel interface.

Platform Administration on a workstation

Platform Administration for a Windows-based platform is different from the same for a controller.

Figure 2: Platform Administration for Windows-based platform



Baja Version	Tridium 4.0.11.0	
Daemon Version	4.0.11.0	
System Home	D:\Niagara\Niagara-4.0.11.0	
User Home	C:\ProgramData\Niagara4.0	
Host	My Host : Optiplex380 (n4Demo)	
Daemon HTTP Port	3011	
Daemon HTTPS Port	5011	
Host ID	Win-8BC6-2936-74E1-B2AB	
Model	Workstation	
Local Date	06-Mar-15	
Local Time	10:40 Eastern Standard Time	
Local Time Zone	America/New_York (-5/-4)	
Operating System	Windows 7 Service Pack 1 (6.1)	
Niagara Runtime	nre-core-win-x64 (4.0.11.0)	
Architecture	x64	
Enabled Runtime Profiles	rt,se,ux,wb	
Java Virtual Machine	oracle-jre-win-x64 (Oracle Corporation 1.8.0.31.0)	
Niagara Stations Enabled	enabled	
Number of CPUs	2	
Current CPU Usage	7%	
Overall CPU Usage	6%	
Filesystem	Total	Free
	C:\ 104,439,252 KB	5,811,136 KB

- No User Accounts button is available, as platform authentication is handled differently, with credentials managed only in Windows.
- No SFTP/SSH button is available (equivalent configuration can be done using Windows, if needed). More typically, the “Remote Desktop Connection” feature of Windows is used.
- The Change Date/Time button is disabled (unavailable). To change the date and time, use Windows.
- The Configure Runtime Profiles button is dimmed (unavailable). Windows hosts are invariably enabled for all runtime profiles.
- The Commissioning button is disabled. The Commissioning Wizard is intended only for initial Niagara installation and startup in a remote controller, or whenever upgrading a controller.
- The Reboot button is dimmed. This is intended only for remote platforms. Any Windows host must be rebooted using Windows.
- Various data in summary information (repeated in View Details) differ greatly from QNX hosts.

Win64-based Supervisor notes

Supervisor support for installations on PCs running a 64-bit Windows operating system is typical, for example Windows Server 2012 or Windows 7 or 8 Professional 64-bit. The primary application for a 64-bit installation is for a Supervisor station with a large NiagaraNetwork (a job with a large numbers of controllers, each with many proxy points), and therefore, a large station database.

In particular, the 64-bit Java VM (Virtual Machine) does not have a 2GB memory limit, unlike the Java VM on a Win32-based Supervisor. Typically, any PC with 64-bit Windows also has 4GB or more of RAM installed, and, unlike a 32-bit Windows PC, the 64-bit OS can effectively utilize all of it. Therefore, a 64-bit Windows host may be the solution for the largest enterprise level Supervisor.

Known Limitations

Currently there are several known limitations for a Supervisor running on a 64-bit Windows operating system. Although most of these do not apply to a typical Supervisor, they should be understood before installation time.

These 64-bit Windows platform limitations include the following:

- NRE serial support is available for a 64-bit Windows platform. However, serial-based drivers (for example, modbusAsync, flexSerial, various legacy drivers) are not typically licensed on a Supervisor, and therefore are not fully tested or supported on a 64-bit platform.

Exceptions to such license rules can occur with 64-bit engineering workstations and demo machines. Again, 64-bit serial operation is not fully guaranteed.

A known issue with the 64-bit serial library may present itself in initialization phases, with usage of a 64-bit Niagara Serial Tunnel client.

- Lonworks FTT-10 is not fully supported on a 64-bit Windows platform—although there are Echelon 64-bit drivers, most are 32-bit drivers in a “64-bit wrapper”, and are likely unsuitable. Further, a Supervisor is not typically licensed for Lonworks. However “LonIP” is supported.

Installation and interface differences

Installation of the Win64-based Supervisor is like the Win32-based installation, except that separate executables in the root of the Supervisor product image or CD are used to install (setup_x64.exe instead of setup_ x86.exe, respectively).

A platform connection to a Win64-based Supervisor provides the identical collection of views as with a Win32-based host. Also, when opening a station running on a Win64 host, you see the same child platform services under its PlatformServices as with a station running on a Win32 host.

Platform daemon (niagarad)

The platform daemon is an executable that runs independently from Niagara core runtime, is pre-installed on every controller as factory-shipped, and runs whenever the controller boots up. The daemon is Java-based, running in its own Hotspot Java VM (Virtual Machine). An additional (and separate) Hotspot Java VM is used for the running the station process.

Platform daemon port

The Niagara host's platform daemon monitors a different TCP/IP port for client connections than does a running station.

By default, this TCP port is either:

- 5011 for a secure (TLS) Platform connection (if available).
- 3011 for a Platform connection that is not secure (unencrypted) .

If necessary, you can change either TCP port monitored to a different (non-default) port during platform configuration.

Platform credentials

As a platform client, you sign on using host level credentials for authentication. This is a user account and password separate from any station user account. Consider it the highest level access to that host.

Note:

A new controller ships with default platform credentials that are widely known, and if left unchanged, the controller is extremely susceptible to being hacked. Starting with the Niagara 4 startup commissioning process, you must change the default user name and password to something known only to your company and/or customers.

Platform access without a platform connection

A station user with admin-level permissions on the Services container (in the component Config space) of a running station also has access to a special subset of platform functions, via Platform Services.

Platform daemon on a PC

When you install Niagara on your PC, one of the last "Would you like to?" install options is to Install and Start Platform Daemon.

The default selection is to install. You need the platform daemon locally installed and running to host a station on your local PC, such as for a Supervisor. This lets you open a Workbench client platform connection to your local (My Host) platform. It also allows remote client platform connections to your PC.

Once installed and started on a PC, you can see the platform daemon listed as a Service from the Windows Control Panel, by selecting Administrative Tools > Services.

Alternatively, after Niagara installation on your PC, you can install and start the platform daemon at any time, if needed. From the Windows Start menu, select Start→ All Programs→ Niagara 4.n.n→ Install Platform Daemon (shortcut for "plat.exe installdaemon").

In summary, your MultiSITE Supervisor PC's local platform daemon is not necessary for making client platform connections to other hosts, only to provide the ability to run a station locally on your PC.

Types of platform views

MultiSITE Supervisor platform connections to a host, either remote controller or Supervisor, provides various functional views.

Note:

In addition to the platform views listed below, a Commissioning Wizard is available as a right-click platform option. This wizard provides a step-by-step method to perform a sequence of platform tasks used to prepare a new controller, or when upgrading the software in a controller.

The following sections summarize the various platform functions and views, including typical usage:

- Application Director

To start, stop, restart, or kill a station on the platform. The output from the station displays in the view pane. This is useful for monitoring and troubleshooting. You also configure a station's Auto-Start" and Restart on Failure settings from this view.

- Certificate Management

To import signed PKI certificates into the platform's key store and trust store for TLS secure connections, and to perform related functions.

- Distribution File Installer

To restore a backup .dist file to the target controller, or to install a clean dist file to wipe the file system of a controller to a near-factory minimum state. This view is available when connected to a remote host.

- File Transfer Client

To copy files between your MultiSITE Supervisor PC and the remote platform (in either direction). For example, you use this platform view when editing a controller's system.properties file: once to copy it from the controller to your MultiSITE Supervisor PC (for local editing) and then afterwards to copy it back to the controller. This view is available when connected to a remote host.

- Lexicon Installer

To install file-based Niagara lexicon sets from your MultiSITE Supervisor PC to the remote platform, to provide non-English language support, or to customize English display of selected items. In Niagara 4, usage of this view and file-based lexicons may be atypical.

- License Manager

To review, install, save, or delete licenses and (license) certificates on the remote Niagara platform.

- Platform Administration

To perform configuration, status, and troubleshooting of the Niagara platform daemon. Included are commands to change time/date, backup all remote configurations, and reboot the host platform. Also included are functions to modify platform users, specify the TCP port monitored by the platform daemon, and various settings for a secure (TLS) platform connection.

- Software Manager

To review, install, update, or uninstall "Niagara modules (.jars)" on the remote Niagara platform. The Software Manager compares modules installed on the connected platform against those available (locally) in Sys Home on your MultiSITE Supervisor PC. This view is available when connected to a remote host.

- Station Copier

To install (copy) a station from your MultiSITE Supervisor User Home to a remote platform (or if it is a Supervisor, to the local PC's daemon User Home). Also to backup (copy) a station to your MultiSITE Supervisor User Home, or to delete a remote station. You can also rename stations.

- TCP/IP Configuration

To review and configure the TCP/IP settings for the network adapter(s) of the Niagara platform.

- Remote File System

For read-only access to folders and files on the remote platform, including all those under its system home (Sys Home) and daemon User Home.

Opening a secure platform connection

A platform (host) connection differs from a station connection. When connected to a platform, Workbench communicates (as a client) to the host’s platform daemon, niagarad (Niagara daemon), a server process. Unlike a station connection that uses the Fox/Foxs protocol, a client platform connection ordinarily requires full MultiSITE Supervisor. This means that it is unavailable using a standard Web browser (Web MultiSITE Supervisor applet). Using a browser, a Supervisor station can connect to a remote platform through its ProvisioningService.

Prerequisites: The platform (PC localhost or controller) has been physically installed and connected.

Step 1 Launch MultiSITE Supervisor.

Step 2 Right-click My Host in the Nav tree and click Open Platform.

The Connect window opens with the name of your computer as the Host name.

It is possible to make this type of secure TLS (Transport Layer Security), encrypted platform connection to any Niagara 4 host, provided it is properly configured.

Note:

For best security, always use TLS. In MultiSITE Supervisor, the default Open Platform and Open Station (Foxs) commands assume a secure connection. To make an unencrypted connection you must change the connection Type first.

Once the platform is connected, the available platform functions are identical, regardless of connection method.

Step 3 To accept the host name, click OK.

The Authentication window opens.

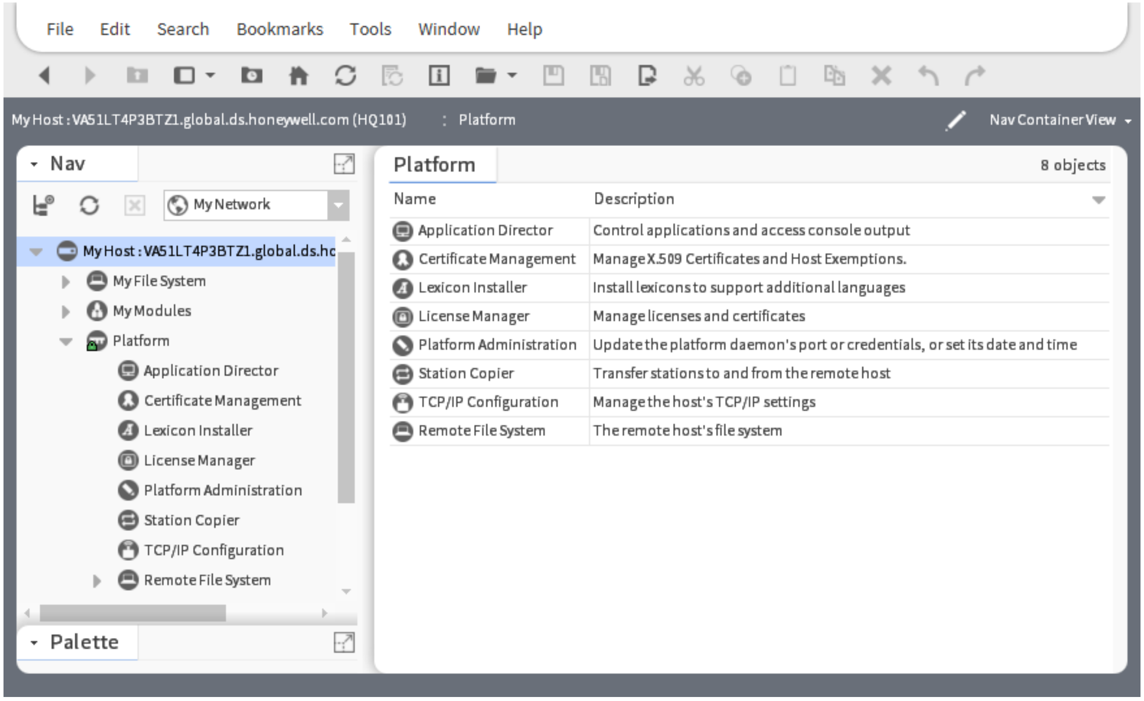
Step 4 Do one of the following:

- If connecting to a controller, enter the credentials (user name and password) required by the controller.
- If connecting to your PC localhost, enter the credentials you use to log on to your computer.

Step 5 Enable “Remember these credentials” and click OK.

The system makes a secure connection between the host and MultiSITE Supervisor, and displays the Nav Container View.

Figure 3: Platform functions listed in platform's Nav Container View



Name	Description
Application Director	Control applications and access console output
Certificate Management	Manage X.509 Certificates and Host Exemptions.
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
Station Copier	Transfer stations to and from the remote host
TCP/IP Configuration	Manage the host's TCP/IP settings
Remote File System	The remote host's file system

The platform-connection session icon appears in the Nav tree with a small padlock icon to indicate the connection type. The icon is either for secure TLS encryption, or for an unencrypted connection.

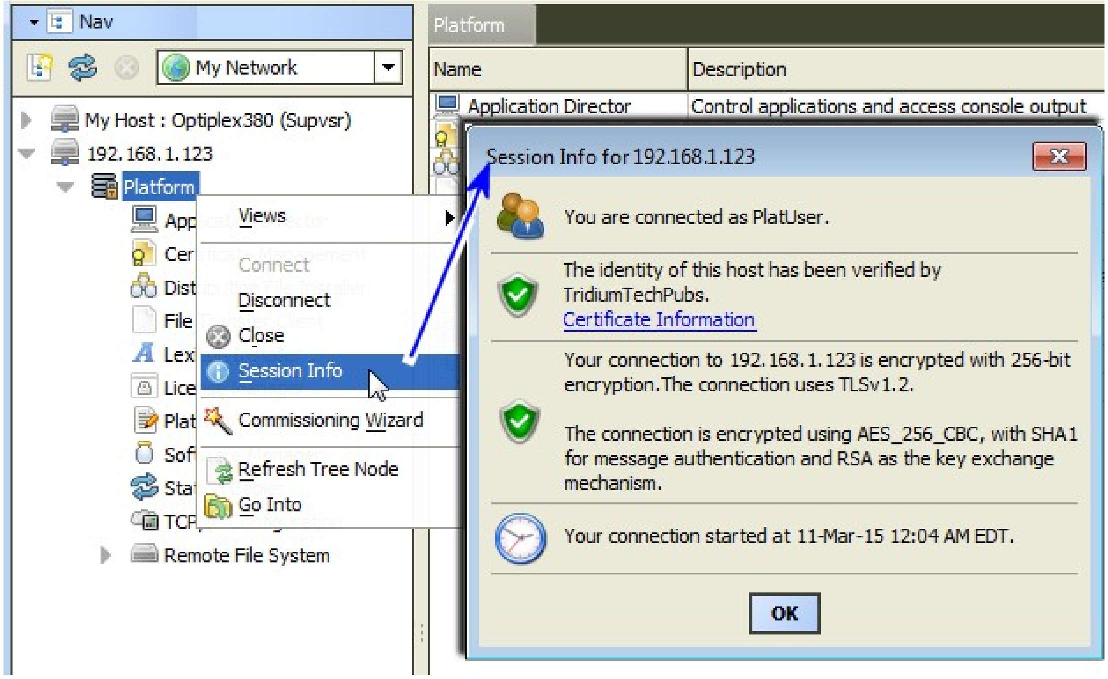
Each platform function has its own MultiSITE Supervisor view (plugin), which you access by double-clicking the view name. Most of the same platform views exist for both a platform connection to a controller and a Supervisor, with these exceptions:

- If you open a local platform connection at your computer, some platform views appear to be missing, for example the Distribution File Installer and Software Manager are not in the list. These views have no application when working at your computer. Instead, you simply use Windows Explorer.
- A few of the platform views differ depending on platform type.

Step 6 To view information about the current session, right-click Platform→Session Info.

This same information is available when right-clicking Station→Session Info

Figure 4: Session Info



Session Info for 192.168.1.123

You are connected as PlatUser.

The identity of this host has been verified by TridiumTechPubs.
Certificate Information

Your connection to 192.168.1.123 is encrypted with 256-bit encryption.The connection uses TLSv1.2.

The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and RSA as the key exchange mechanism.

Your connection started at 11-Mar-15 12:04 AM EDT.

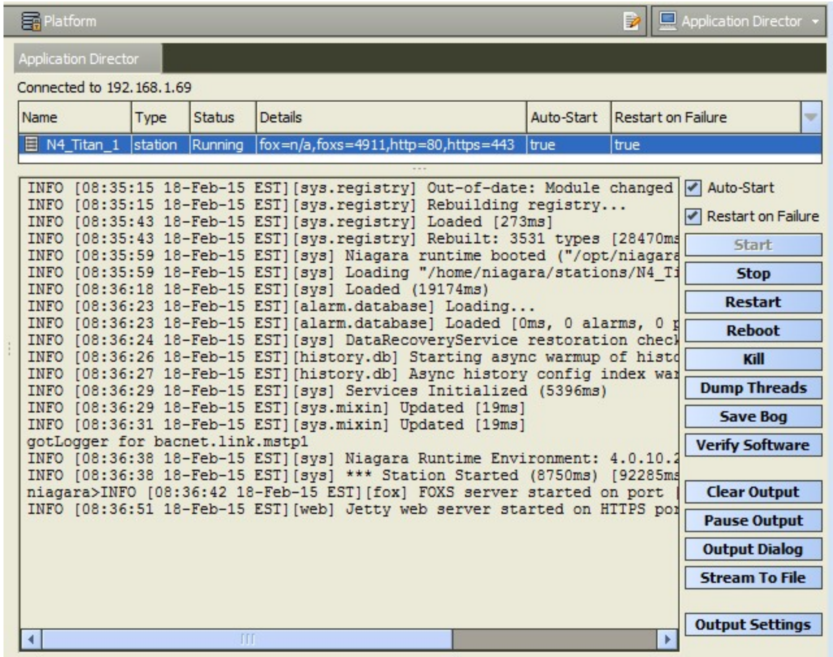
This is an example of this client session information from a secure (TLS) platform connection. The identity of the (server) has been verified by a signed certificate, and all data sent over this connection are encrypted.

Application Director (station management)

The Application Director is the platform view that allows you to start and stop a station running in any host (whether a remote JACE, a local, or a remote Supervisor PC) that is connected to a Niagara platform.

The term application refers to an installed station. In addition to starting and stopping, you use the Application Director to examine standard station output, for troubleshooting and debug purposes. From it, you define a station’s restart settings, plus have access to other station actions.

Figure 5: Application Director view, looking at a station



Connected to 192.168.1.69

Name	Type	Status	Details	Auto-Start	Restart on Failure
N4_Titan_1	station	Running	fox=n/a,foxs=4911,http=80,https=443	true	true

☑ Auto-Start

☑ Restart on Failure

```
INFO [08:35:15 18-Feb-15 EST][sys.registry] Out-of-date: Module changed
INFO [08:35:15 18-Feb-15 EST][sys.registry] Rebuilding registry...
INFO [08:35:43 18-Feb-15 EST][sys.registry] Loaded [273ms]
INFO [08:35:43 18-Feb-15 EST][sys.registry] Rebuilt: 3531 types [28470ms
INFO [08:35:59 18-Feb-15 EST][sys] Niagara runtime booted ("/opt/niagara
INFO [08:35:59 18-Feb-15 EST][sys] Loading "/home/niagara/stations/N4_Ti
INFO [08:36:18 18-Feb-15 EST][sys] Loaded (19174ms)
INFO [08:36:23 18-Feb-15 EST][alarm.database] Loading...
INFO [08:36:23 18-Feb-15 EST][alarm.database] Loaded [0ms, 0 alarms, 0 p
INFO [08:36:24 18-Feb-15 EST][sys] DataRecoveryService restoration check
INFO [08:36:26 18-Feb-15 EST][history.db] Starting async warmup of histo
INFO [08:36:27 18-Feb-15 EST][history.db] Async history config index war
INFO [08:36:29 18-Feb-15 EST][sys] Services Initialized (5396ms)
INFO [08:36:29 18-Feb-15 EST][sys.mixin] Updated [19ms]
INFO [08:36:31 18-Feb-15 EST][sys.mixin] Updated [19ms]
gotLogger for bacnet.link.mstp1
INFO [08:36:38 18-Feb-15 EST][sys] Niagara Runtime Environment: 4.0.10.2
INFO [08:36:38 18-Feb-15 EST][sys] *** Station Started (8750ms) [92285ms
niagara>INFO [08:36:42 18-Feb-15 EST][fox] FOXS server started on port
INFO [08:36:51 18-Feb-15 EST][web] Jetty web server started on HTTPS por
```

Every 1.5 seconds, the platform daemon fetches data about the station(s) and updates the Application Director.

- To select a station, click the row in the table.

This action highlights the station. When a station is selected, its standard output appears, and all enabled right-side buttons that apply to it.

- To access the station's shortcut menu, right-click the row in the table.

The shortcut menu (a subset of the application and output actions buttons) opens.

- To open a MultiSITE Supervisor (Fox) connection to a running station in the current tab, double-click the station row in the table.

If the station is not running, double-clicking will not change the view.

- To open a MultiSITE Supervisor (Fox) connection to a running station in a new tab, press Ctrl and double-click the station row in the table.

If the station is not running, double-clicking does not change the view.

Starting a station

A station must be running before it can be opened and accessed.

Prerequisites:

Note that most station–platform functions can be performed from the Application Director platform view of a host. However, you must connect to the platform where a station is hosted before you can perform these tasks.

Step 1 In the Nav side bar, expand the Platform node in the Nav tree by clicking on the plus sign (+) next to the platform icon in the tree. The contents of the platform node opens in the tree.

Step 2 In the Nav side bar, double-click the 💻 Application Director.

Step 3 In the Application Director view, select the desired station.

This action highlights the station. When a station is selected, its standard output appears, and all enabled right-side buttons that apply to it.

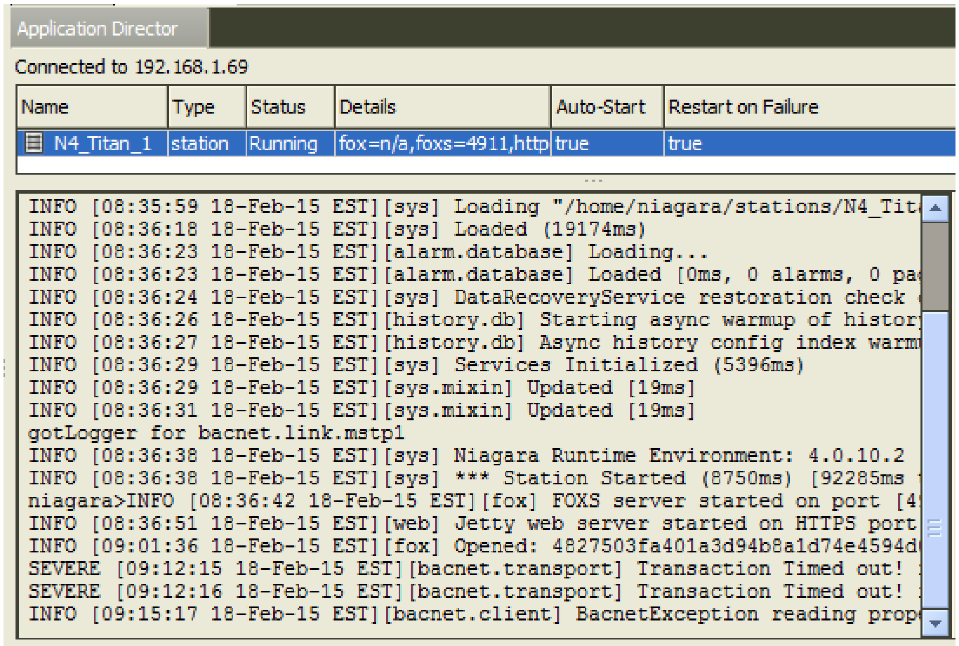
Step 4 In the right-side area of this view, select the following options, as desired:

- To start the station automatically any time the host computer is re-booted, enable the Auto-Start option. Clear this option to disable auto–start.
- To automatically attempt a restart any time a station fails, enable Restart on Failure. Clear this option to disable automatic restart.

Step 5 In the Application Director view, do one of the following:

- Select the desired station in the station table and click Start.
- Right-click the desired station in the station table and select Start from the popup menu. The station starts and displays standard output and error messages in the window.

Figure 6: Application Director



Connected to 192.168.1.69

Name	Type	Status	Details	Auto-Start	Restart on Failure
N4_Titan_1	station	Running	fox=n/a,foxs=4911,http	true	true

```
INFO [08:35:59 18-Feb-15 EST][sys] Loading "/home/niagara/stations/N4_Tit
INFO [08:36:18 18-Feb-15 EST][sys] Loaded (19174ms)
INFO [08:36:23 18-Feb-15 EST][alarm.database] Loading...
INFO [08:36:23 18-Feb-15 EST][alarm.database] Loaded [0ms, 0 alarms, 0 pa
INFO [08:36:24 18-Feb-15 EST][sys] DataRecoveryService restoration check
INFO [08:36:26 18-Feb-15 EST][history.db] Starting async warmup of histor
INFO [08:36:27 18-Feb-15 EST][history.db] Async history config index warm
INFO [08:36:29 18-Feb-15 EST][sys] Services Initialized (5396ms)
INFO [08:36:29 18-Feb-15 EST][sys.mixin] Updated [19ms]
INFO [08:36:31 18-Feb-15 EST][sys.mixin] Updated [19ms]
gotLogger for bacnet.link.mstp1
INFO [08:36:38 18-Feb-15 EST][sys] Niagara Runtime Environment: 4.0.10.2
INFO [08:36:38 18-Feb-15 EST][sys] *** Station Started (8750ms) [92285ms
niagara>INFO [08:36:42 18-Feb-15 EST][fox] FOXS server started on port [4
INFO [08:36:51 18-Feb-15 EST][web] Jetty web server started on HTTPS port
INFO [09:01:36 18-Feb-15 EST][fox] Opened: 4827503fa401a3d94b8a1d74e4594d
SEVERE [09:12:15 18-Feb-15 EST][bacnet.transport] Transaction Timed out!
SEVERE [09:12:16 18-Feb-15 EST][bacnet.transport] Transaction Timed out!
INFO [09:15:17 18-Feb-15 EST][bacnet.client] BacnetException reading prop
```

Depending on the status of the station selected, the standard output text consists of one of the following:

- If the station is running, the output updates in real time. As more text is written by the station, the system appends it to the bottom of the output area.
- If the station is not running, the output text is from the most recent execution of that station.
- If no station is selected, the output text area is blank.

Step 6 Do one of the following:

Use the scroll bars to view all text.

- Use the Windows copy shortcut (Ctrl + C) to copy output text to the clipboard for further analysis.
- Use the right-side output control buttons. One of these lets you stream station output to a file.

Due to our policy of continuous product innovation, some specifications may change without notification

Standard output messages

Station output log messages can include errors and warnings that let you know why something is not working, as well as simple informational messages about events as they occur. If needed, you can also change the log level of station output.

The general format of a station output log message is:

```
TYPE [timestamp] [station_process] message_text
```

For example:

```
INFO [17:05:18 16-Feb-15 EST][fox] FOXS server started on port [4911]
```

Message log types seen in station output include the following, by leading text descriptor

- INFO

Typical of most default station output log messages. Usually, each message lets you know some process milestone was started or reached, such as a service or the station.

INFO is equivalent to the MESSAGE level in AX station log output.

- WARNING

This informs you of a potential problem, such as inability to open a specific port. Typically, warnings do not keep a station from starting.

WARNING is equivalent to the (same) WARNING level in AX station log output.

- SEVERE

This informs you of a problem that might keep the station from starting. Or, if it can start, an error that prevents some function of the station from operating correctly. Often an exception is produced.

SEVERE is equivalent to the ERROR level in AX station log output.

- FINE

This is a verbose debug-level message that may be generated upon every process transaction. Typically, this is useful only in advanced debugging mode. You see these for station processes only if you have set the log level at FINE or even finer (FINER, FINEST, ALL).

Such levels (FINE, FINER, FINEST) are equivalent to the TRACE level in AX station log output.

In addition to the verbose output messages, occasionally you may see a string of java exception text in a station's output. This indicates an unforeseen station execution issue, which can range from a licensing problem, a misconfiguration, or some other unexpected problem.

Station output logs in Niagara 4 use a standard Java logging API (java.util.logging), which has more log severity levels than the NiagaraAX Baja logging API (javax.baja.log). Any Niagara 4 station has a standard DebugService (LoggingService) for making changes. This is in addition to the spy log setup used in NiagaraAX.

Station LogHistory (LogHistoryService)

If a station is configured with the LogHistoryService (under its Services container), it maintains a buffered history (LogHistory) of some of the messages seen in the station's standard output. In the LogHistoryService's configuration, you specify its log level, meaning the minimum message type (from station output) to log. By default, the log level (property Minimum Severity) is Info. You may wish to change this to Warning.

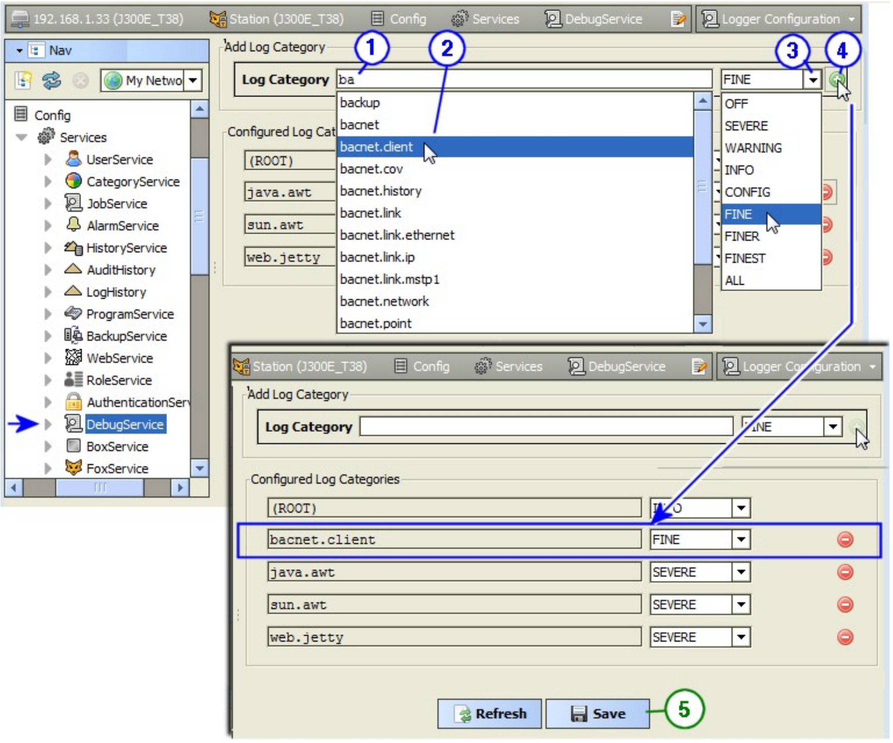
This is mentioned because when looking at a station's output, you are usually troubleshooting. As part of troubleshooting, you should always check the station's histories for the LogHistory. It should contain recently recorded station errors and (if configured) warnings. This information may help when evaluating "live" output from the station.

Station log levels (DebugService)

Using the station's DebugService (LoggingService), you can review and change the log level of the station processes of interest, in order to tune station output seen in the Application Director. Niagara 4 stations have a DebugService in which you can set log levels for modules/processes. See figure below.

In the example shown below, the "bacnet.client" process is being added with a log level of FINE. For example, such an entry might be useful to debug (troubleshoot) errors about writes to Bacnet proxy points.

Figure 7: bacnet.client



Add Log Category

Log Category: ba — FINE

Configured Log Categories

(ROOT) — INFO
bacnet.client — FINE
java.awt — SEVERE
sun.awt — SEVERE
web.jetty — SEVERE

Adding log items in a station’s DebugService

This procedure sets the log level in the DebugService.

Prerequisites: Admin write permissions on the station’s DebugService.

Step 1 In the DebugService’s default Logger Configuration view, click in the Log Category field and start typing the name of a module or module.process you wish to add.

A drop-down list opens.

Step 2 Double-click an item in the list.

This enters the item in the Log Category field.

Step 3 On the right, click the control and select a level, for example FINE (for more detail than the default INFO level offers).

Step 4 Click the Add control to add it to configured log categories.

It now appears in the listed log categories.

Step 5 Repeat steps 1 through 4, if needed, to add other items, or else make other changes on levels, etc.

Step 6 Click the Save button to save these settings to the host’s ~/logging/logging.properties file.

Settings become immediately active, affecting station output as seen in the Application Director.

Note:

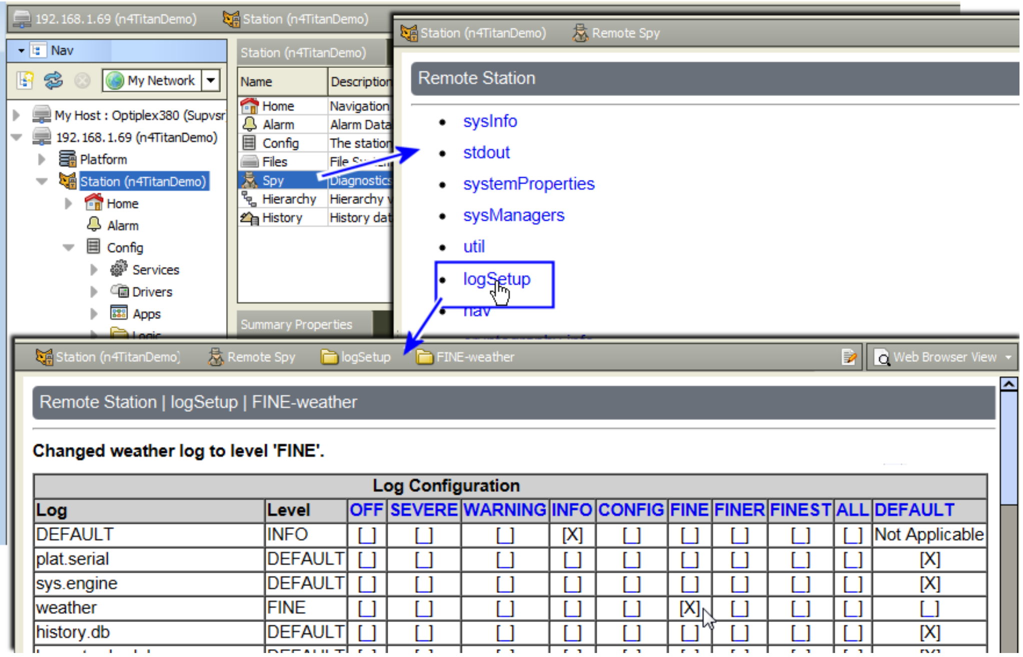
Be aware that persisted log settings are not part of a station’s configuration, even though you access them through a station’s DebugService. Settings apply to any station run on the host, until changed and saved again. Therefore, be sure to return settings back to normal levels and/or delete additions after concluding a debug session. Otherwise, excessive station output could adversely impact station performance.

MultiSITE Supervisor has a similar log interface for its console, available in the Tools menu (Tools→ Logger Configuration). This log affects output seen in the console window when you start MultiSITE Supervisor with the shortcut MultiSITE Supervisor (Console), for (wb.exe). Changes to it are stored in your User Home ~/logging/logging properties file.

Station log levels (spy:/logSetup)

As an alternative to using the station's DebugService to tune station log output, you can use the station spy HTML interface for log setup. (This is the only method available for a NiagaraAX station.) To access the station's logSetup page in MultiSITE Supervisor, double-click the running station in the Nav tree for its Station Summary view. From there, double-click Spy, then click logSetup.

Figure 8: Station spy logSetup (from Station Summary)



Remote Station | logSetup | FINE-weather

Changed weather log to level 'FINE'.

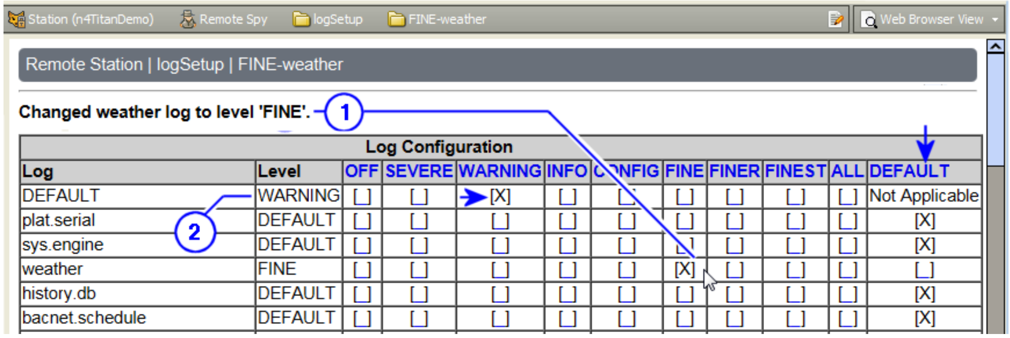
Log Configuration											
Log	**Level**	**OFF**	**SEVERE**	**WARNING**	**INFO**	**CONFIG**	**FINE**	**FINER**	**FINEST**	**ALL**	**DEFAULT**
DEFAULT	INFO	[ ]	[ ]	[ ]	[X]	[ ]	[ ]	[ ]	[ ]	[ ]	Not Applicable
plat.serial	DEFAULT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[X]
sys.engine	DEFAULT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[X]
weather	FINE	[ ]	[ ]	[ ]	[ ]	[ ]	[X]	[ ]	[ ]	[ ]	[ ]
history.db	DEFAULT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[X]

Spy logSetup lists station processes, each showing its current log level, and starts with a (new) DEFAULT level. If you are familiar with spy logSetup in NiagaraAX, note these changes:

- Level selection columns are ordered left-to-right in increasing order of message volume.
- The number of severity levels has increased: 9 in N4, versus 5 in AX.
- Unlike in AX, log levels are persisted each time you click to set/clear a check box, saved in the host's ~/logging/logging.properties file. There is no separate Save To File in N4.0.
- The level given to the top DEFAULT row is global to any row with the far-right DEFAULT box set. See the next example figure.

The following figure shows the top of the spy logSetup page after the DEFAULT level has been changed from INFO to WARNING, and then the weather process set to the non-default level FINE.

Figure 9: Example spy logSetup for a station after a couple of changes



Remote Station | logSetup | FINE-weather

Changed weather log to level 'FINE'.

Log Configuration											
Log	**Level**	**OFF**	**SEVERE**	**WARNING**	**INFO**	**CONFIG**	**FINE**	**FINER**	**FINEST**	**ALL**	**DEFAULT**
DEFAULT	WARNING	[ ]	[ ]	[X]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	Not Applicable
plat.serial	DEFAULT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[X]
sys.engine	DEFAULT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[X]
weather	FINE	[ ]	[ ]	[ ]	[ ]	[ ]	[X]	[ ]	[ ]	[ ]	[ ]
history.db	DEFAULT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[X]
bacnet.schedule	DEFAULT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[X]

Callouts in the figure above show:

1. Last change made, reflected in this status line area (Changed weather log to level 'FINE'.)

2. The DEFAULT log level, which in this case has been set to WARNING. Note this log level now applies to all rows where one of the 9 non-default levels (OFF to ALL) has not been set.

Increasing station output by assigning various log levels above INFO consumes extra station resources and may exact a performance penalty! After troubleshooting, always return log levels to default values.

You can also easily review, and if necessary, adjust log levels from the station.

Opening a running station

This procedure gives details on how to connect to a running station.

Step 1 From the File menu, select Open→Open Station (Fox).

The popup Open Station window opens, or if AX-3.8, the Open Station with SSL window opens (this is the default).

Step 2 Complete the fields in the Open Station or Open Station with SSL window as follows:

- Type

Select either Station SSL Connection or Station Connection, as appropriate. If you change, the default Port changes between 4911 (SSL) to 1911 (non-SSL).

- Host

Select the IP option and type in the IPv4 address of the host platform that you wish to access.

- Port

Verify the port shown, with the default as either 1911 (non-SSL) or 4911 (SSL). If you know the remote host is using a different (non-default) platform daemon port, enter it here.

Step 3 Click the OK button and do one of the following:

- If you chose Open Station (non-SSL), go to Step 4.
- If you chose Open Station with SSL, different results are possible:
  - – If the station's FoxService is not enabled for SSL, an error results with "Cannot connect. Ensure server is running on specified port". Retry from Step 1, changing the Type to Station Connection.
  - – If the station's FoxService is enabled for SSL, but you have not yet installed a certificate for it, a popup Identity Verification window with certificate details opens. In most cases, click Accept to proceed to the next step.
  - – An Authentication popup window opens. Go to the next step.

Step 4 In the popup Authentication window, enter your station user credentials, and click OK.

Note:

Be sure to use your station username and password, not your credentials for the platform.

If the "Remember these credentials option" is available, you can select it, so that MultiSITE Supervisor remembers these user credentials. However, this can pose a future security risk; therefore, this option may be disabled.

If the station user credentials were correct, the station opens, and the Fox connection icon appears in the side bar pane. Where Fox connection icons are either

- Station or
- Station TLS

The view pane shows the Station Summary view, listing primary components and details on the host.

If the station user credentials were not correct, you are prompted to enter them again.

Distribution File Installer

This platform view is used to install dist (distribution) files.

A dist file is a zip that contains other files and a manifest that describes the contents of the distribution. Use this view for either of these two tasks:

- To restore a locally available backup dist file to a remote controller. Such a restore can be initiated using the Backup command from the platform's Platform Administration view, or, more commonly, from the BackupService in the station running on that host.

Note:

To be able to restore a backup dist file, your MultiSITE Supervisor installation requires the same versions of software, including modules, to be available in its software database. Therefore, it is recommended that you make and keep frequent backups as you upgrade remote hosts. Also, for this reason, you may need to import the software database from prior revisions of Niagara into your current MultiSITE Supervisor installation.

- To install a clean dist file. This downgrades a controller to an older Niagara 4 release level, or restores it to a known empty state. Following a clean dist install, you must recommission the controller, as this wipes the file system (almost all software, as well as all station files), leaving the controller in an empty near-factory state.

Do not use this view to upgrade a controller. Instead, use the Commissioning Wizard in a controller. The Commissioning Wizard is a right-click option on a platform when opened in MultiSITE Supervisor.

About backup distribution files

A backup dist includes not only the entire station folder, but all other configuration information that may be customized for the platform. This allows for a complete replication from the one backup file.

Typically, station backups are done from MultiSITE Supervisor station connections (a station is running, and has the BackupService). In the Nav tree, right-click the opened station, and select Backup Station.

Less typical is an offline backup from the Platform Administration view.

By default, station backup dist files are saved in your MultiSITE Supervisor User Home, in a ~/backups folder.

Restoring a backup distribution file

This procedure restores a remote station to the state it was in when a backup was made.

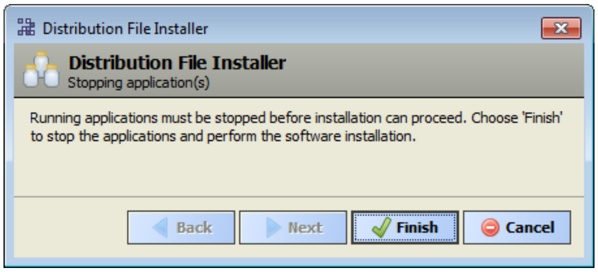
Prerequisites:

- A backup dist file of the station on the target controller exists.
- The software database of your Niagara 4 installation includes matching versions of all software modules used by the station when the station backup was made. Without these modules, restoring the backup dist will fail.
- Any controlled equipment, which might be adversely affected by the station stopping (and the removal of software) is put in a manually controlled state.

Step 1 Using MultiSITE Supervisor, open a platform connection to the remote host.

Step 2 If a station is already running on the remote host, stop any running applications (stations).

Figure 10: Distribution File Installer



Running applications must be stopped before installation can proceed. Choose 'Finish' to stop the applications and perform the software installation.

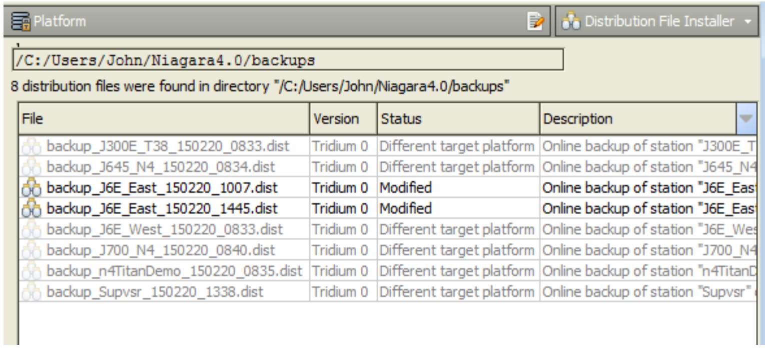
Step 3 Do one of the following:

- In the Distribution File Installer click the Backups button (🗄) for the !/backups folder.
- Click the Choose Directory button to point to another backup dist file location.

The Installer parses through the distribution files, and makes selectable only those files that are compatible with the opened platform. When done parsing, available backup dists open in a list.

Dist files that are inappropriate, for example that are for a different target platform or have unmet dependencies, are dimmed. The Install button does not become active if you select such a file.

Figure 11: Platform



/C:/Users/John/Niagara4.0/backups

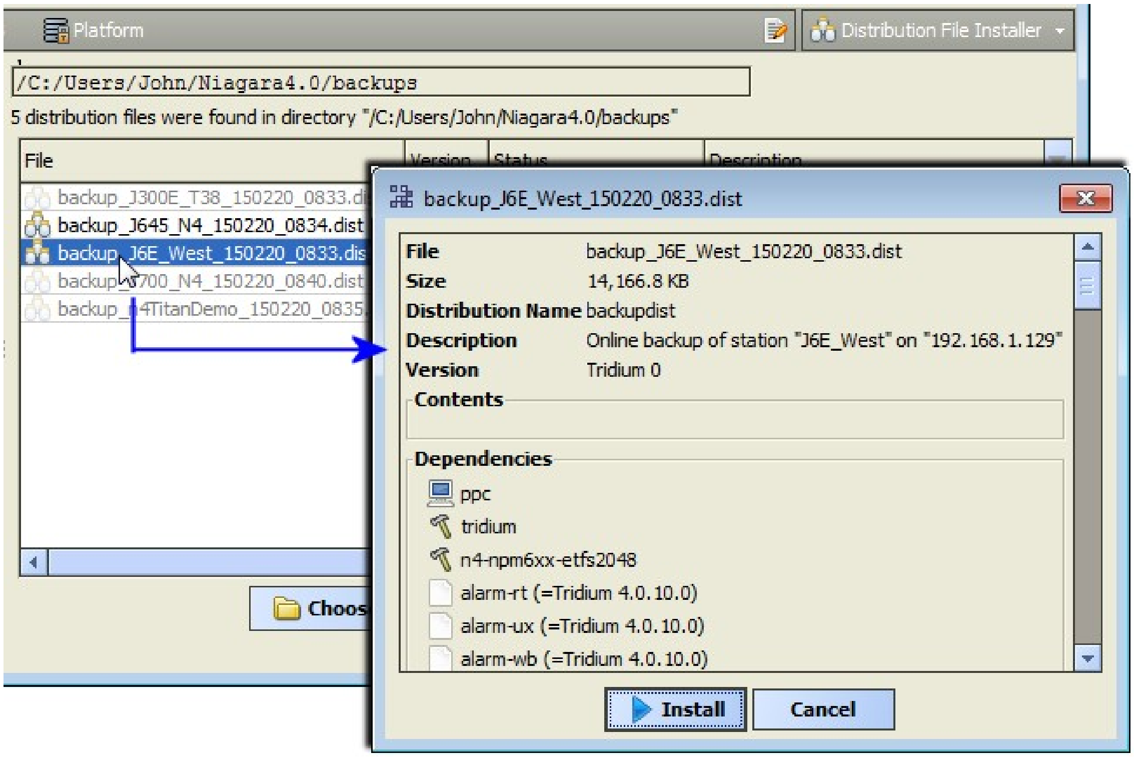
8 distribution files were found in directory "/C:/Users/John/Niagara4.0/backups"

File	Version	Status	Description
backup_J300E_T38_150220_0833.dist	Tridium 0	Different target platform	Online backup of station "J300E_T
backup_J645_N4_150220_0834.dist	Tridium 0	Different target platform	Online backup of station "J645_N4
backup_J6E_East_150220_1007.dist	Tridium 0	Modified	Online backup of station "J6E_Eas
backup_J6E_East_150220_1445.dist	Tridium 0	Modified	Online backup of station "J6E_Eas
backup_J6E_West_150220_0833.dist	Tridium 0	Different target platform	Online backup of station "J6E_Wes
backup_J700_N4_150220_0840.dist	Tridium 0	Different target platform	Online backup of station "J700_N4
backup_n4TitanDemo_150220_0835.dist	Tridium 0	Different target platform	Online backup of station "n4TitanD
backup_Supvsr_150220_1338.dist	Tridium 0	Different target platform	Online backup of station "Supvsr"

Step 4 For details on any dist file, double-click it.

The system opens a popup that includes a list of its dependencies.

Figure 12: Dependencies



/C:/Users/John/Niagara4.0/backups

5 distribution files were found in directory "/C:/Users/John/Niagara4.0/backups"

File
- backup_J300E_T38_150220_0833.di
- backup_J645_N4_150220_0834.dist
- backup_J6E_West_150220_0833.dis
- backup_J700_N4_150220_0840.dist
- backup_n4TitanDemo_150220_0835.

backup_J6E_West_150220_0833.dist

File	backup_J6E_West_150220_0833.dist
Size	14,166.8 KB
Distribution Name	backupdist
Description	Online backup of station "J6E_West" on "192.168.1.129"
Version	Tridium 0

Contents

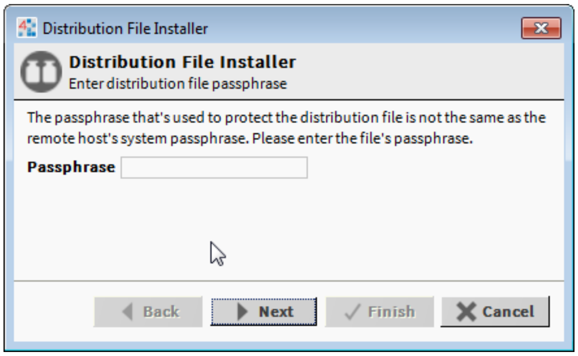
Dependencies
- ppc
- tridium
- n4-npm6xx-etfs2048
- alarm-rt (=Tridium 4.0.10.0)
- alarm-ux (=Tridium 4.0.10.0)
- alarm-wb (=Tridium 4.0.10.0)

When you click Install, the system attempts to validate the file's passphrase.

- If the file passphrase and system passphrase are the same, the process continues without prompting for a passphrase.
- If the file passphrase and system passphrase are different, you are prompted to enter the file's passphrase, as shown below.

Note that if you do not know the .dist file passphrase, you cannot install the file.

Figure 13: Distribution File Installer prompts for file passphrase


Distribution File Installer
Distribution File Installer
Enter distribution file passphrase

The passphrase that's used to protect the distribution file is not the same as the remote host's system passphrase. Please enter the file's passphrase.

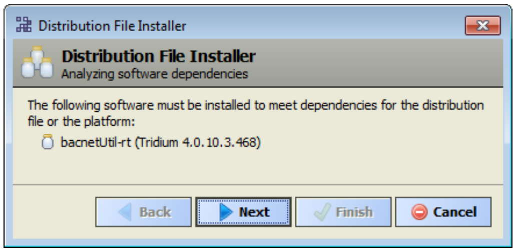
Passphrase

Step 5 To restore any selected backup, click Install.

If the host is already running a station, a window opens telling you that the station must be stopped.

If the station backup .dist file contains software modules different from (or in addition to) those already installed in the remote host, another window opens. See figure below.

Figure 14: Distribution File Installer


Distribution File Installer
Distribution File Installer
Analyzing software dependencies

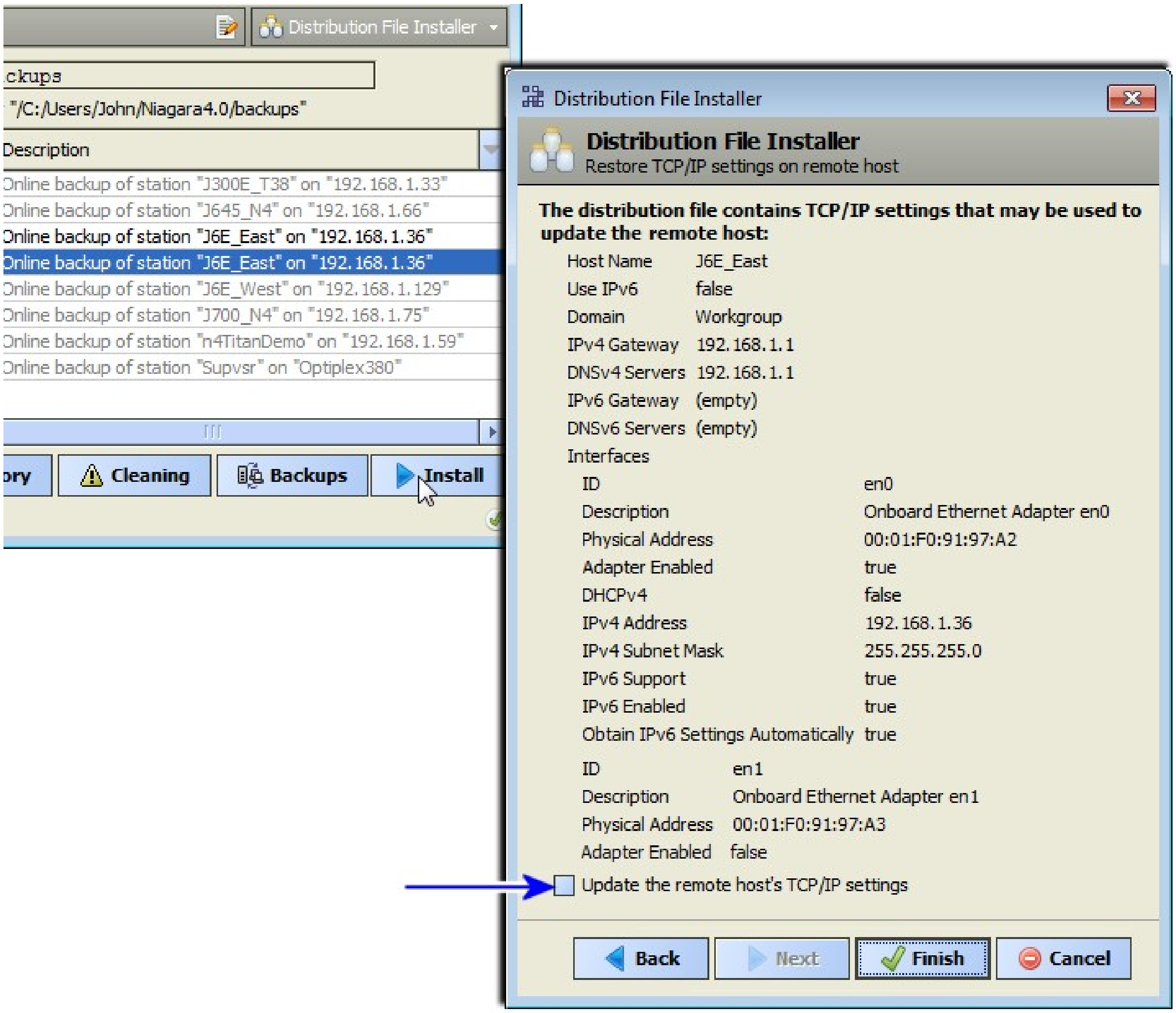
The following software must be installed to meet dependencies for the distribution file or the platform:

bacnetUtil-rt (Tridium 4.0.10.3.468)

Step 6 To continue, click Next.

Another window appears, asking if you wish to restore the TCP/IP settings stored in the dist file (as displayed) into the remote host.

Figure 15: Distribution File Installer



"/C:/Users/John/Niagara4.0/backups"

Description
Online backup of station "J300E_T38" on "192.168.1.33"
Online backup of station "J645_N4" on "192.168.1.66"
Online backup of station "J6E_East" on "192.168.1.36"
Online backup of station "J6E_East" on "192.168.1.36"
Online backup of station "J6E_West" on "192.168.1.129"
Online backup of station "J700_N4" on "192.168.1.75"
Online backup of station "n4TitanDemo" on "192.168.1.59"
Online backup of station "Supvsr" on "Optiplex380"

Distribution File Installer

Distribution File Installer
Restore TCP/IP settings on remote host

The distribution file contains TCP/IP settings that may be used to update the remote host:

Host Name	J6E_East
Use IPv6	false
Domain	Workgroup
IPv4 Gateway	192.168.1.1
DNSv4 Servers	192.168.1.1
IPv6 Gateway	(empty)
DNSv6 Servers	(empty)
Interfaces	

ID	en0
Description	Onboard Ethernet Adapter en0
Physical Address	00:01:F0:91:97:A2
Adapter Enabled	true
DHCPv4	false
IPv4 Address	192.168.1.36
IPv4 Subnet Mask	255.255.255.0
IPv6 Support	true
IPv6 Enabled	true
Obtain IPv6 Settings Automatically	true

ID	en1
Description	Onboard Ethernet Adapter en1
Physical Address	00:01:F0:91:97:A3
Adapter Enabled	false

□ Update the remote host's TCP/IP settings

The TCP/IP settings contained in the dist file are listed, and by default, the check box Update the remote host's TCP/IP settings is cleared.

Step 7 Do one of the following:

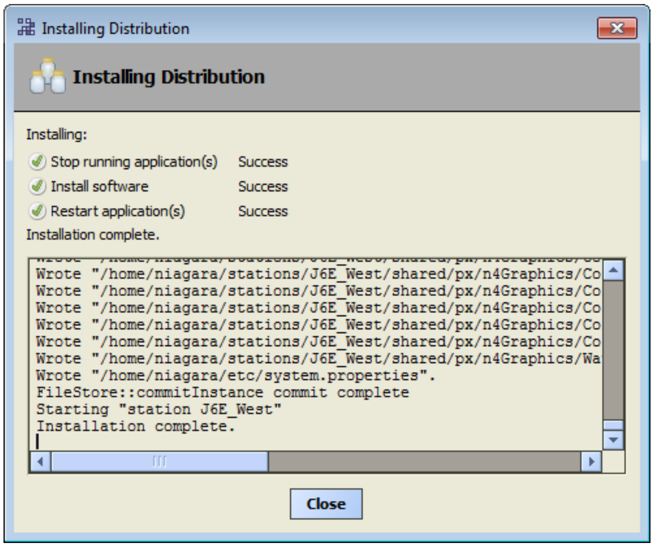
- To use the same dist file on differently addressed hosts, leave this check box cleared.
- To use the TCP/IP settings stored in the dist file, enable the Update the remote host's TCP/ IP settings check box.

Depending on your choice, after the dist file installs and the host reboots, it retains its current TCP/ IP settings or uses the TCP/IP settings stored in the dist file.

Step 8 Click Finish to begin installation.

The dist installation process opens a window that tracks its progress.

Figure 16: Installing Distribution



Installing:

✓ Stop running application(s)	Success
✓ Install software	Success
✓ Restart application(s)	Success

Installation complete.

```
Wrote "/home/niagara/stations/J6E_West/shared/px/n4Graphics/Co
Wrote "/home/niagara/stations/J6E_West/shared/px/n4Graphics/Co
Wrote "/home/niagara/stations/J6E_West/shared/px/n4Graphics/Co
Wrote "/home/niagara/stations/J6E_West/shared/px/n4Graphics/Co
Wrote "/home/niagara/stations/J6E_West/shared/px/n4Graphics/Co
Wrote "/home/niagara/stations/J6E_West/shared/px/n4Graphics/Wa
Wrote "/home/niagara/etc/system.properties".
FileStore::commitInstance commit complete
Starting "station J6E_West"
Installation complete.
```

The installer automatically stops the station, and then continues with the distribution file install process, which overwrites all stations, After the distribution file (and modules, if selected) are installed on the platform, the controller reboots, and the progress window indicates complete.

Step 9 To continue, click Close and open a new platform connection, perhaps to view output in the Application Director

About returning a controller to factory defaults

At times it may be necessary to restore a controller to a known good empty state, either to recommission it with the current release build, or before recommissioning it with an earlier build. To do this, you can install a clean dist (distribution) file.

Wiping a controller clean is typically unnecessary if you are upgrading an operational controller to later software build. Using the Commissioning Wizard should be all that is necessary. However, if you are downgrading a controller to an earlier build, you should install a clean dist file first, to avoid compatibility problems. This applies especially to JACE controllers, as binaries for the (QNX) OS are included in dist files.

Note:

You cannot downgrade an N4 controller to an AX controller. To upgrade a controller from AX to N4 requires one-time-only dist files.

Installing a clean dist wipes the entire file system and installs an appropriate version of Niagara platform daemon, resetting the unit to a near factory state. If the controller came with an appliance installed, installing a clean dist also removes the appliance. Only the following settings are preserved:

- TCP/IP settings
- license files
- brand.properties
- most secure communication (TLS) configuration

All other data is deleted from the file system, including station bog files, Px files, modules, etc. Note that the unit’s TLS private key information is also deleted. In addition, installing a clean dist deletes all configured platform users, restoring the factory-default platform credentials and port (3011).

Returning a controller to near factory defaults

Prerequisites:

- The controller is a Niagara 4 unit.
- You have backed up any station files as well as any other files needed later, for example digital certificate keys. Always export certificate keys for any TLS-configured unit (and store the exported keys in a safe place), such that if the controller needed to be replaced (hardware swap-out), you could re-import those keys.

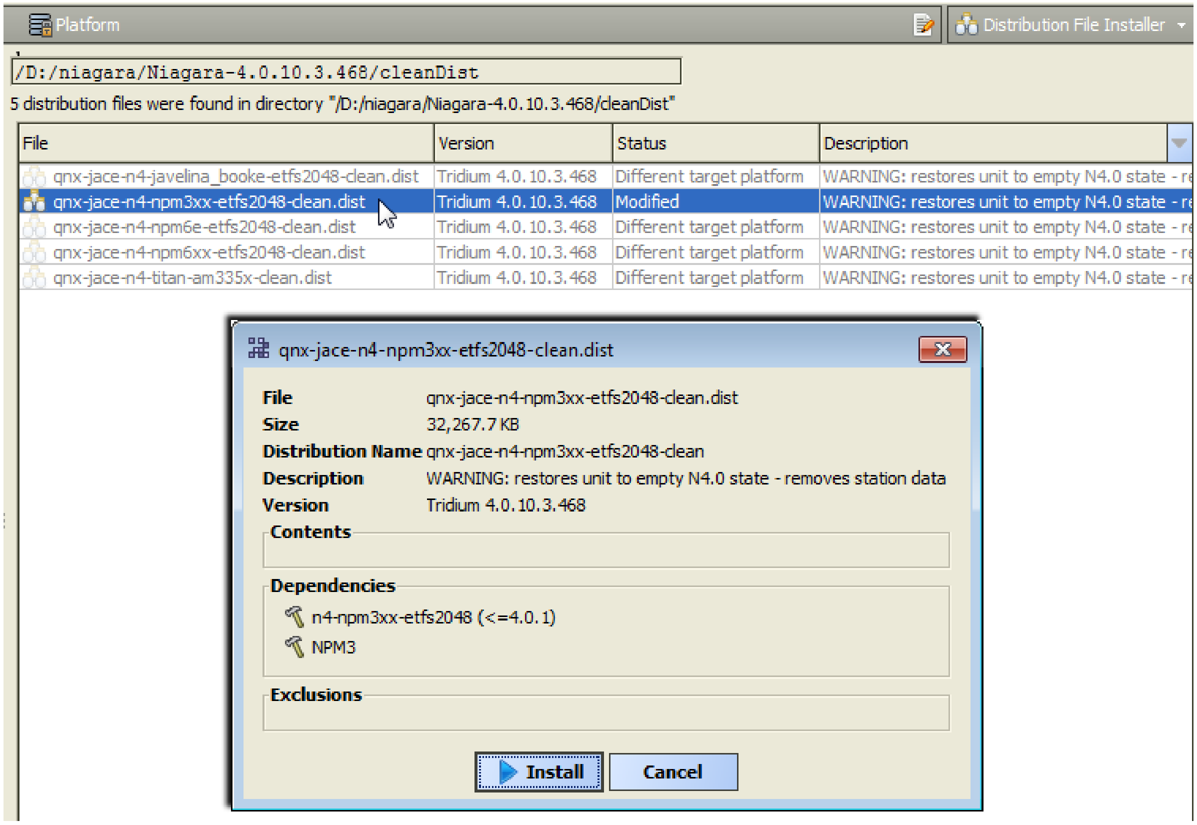
Step 1 Using MultiSITE Supervisor, open a platform connection to the controller.

Step 2 To access the !cleanDist directory, open the Distribution File Installer and click the Cleaning button.

Each clean dist file has the suffix -clean in its name. Clean distribution files are located in your Sys Home !cleanDist folder, apart from other dist files under your software database.

Clean dist files appear listed with a WARNING in the Description. You can select only the appropriate file for the currently opened platform.

Figure 17: Distribution File Installer



/D:/niagara/Niagara-4.0.10.3.468/cleanDist

5 distribution files were found in directory "/D:/niagara/Niagara-4.0.10.3.468/cleanDist"

File	Version	Status	Description
qnx-jace-n4-javelina_booke-etfs2048-clean.dist	Tridium 4.0.10.3.468	Different target platform	WARNING: restores unit to empty N4.0 state - re
qnx-jace-n4-npm3xx-etfs2048-clean.dist	Tridium 4.0.10.3.468	Modified	WARNING: restores unit to empty N4.0 state - re
qnx-jace-n4-npm6e-etfs2048-clean.dist	Tridium 4.0.10.3.468	Different target platform	WARNING: restores unit to empty N4.0 state - re
qnx-jace-n4-npm6xx-etfs2048-clean.dist	Tridium 4.0.10.3.468	Different target platform	WARNING: restores unit to empty N4.0 state - re
qnx-jace-n4-titan-am335x-clean.dist	Tridium 4.0.10.3.468	Different target platform	WARNING: restores unit to empty N4.0 state - re

qnx-jace-n4-npm3xx-etfs2048-clean.dist

File qnx-jace-n4-npm3xx-etfs2048-clean.dist
Size 32,267.7 KB
Distribution Name qnx-jace-n4-npm3xx-etfs2048-clean
Description WARNING: restores unit to empty N4.0 state - removes station data
Version Tridium 4.0.10.3.468

Contents

Dependencies

n4-npm3xx-etfs2048 (<=4.0.1)
NPM3

Exclusions

Step 3 Select the appropriate clean dist file for the platform and click Install.

Removing a file system takes a few minutes, then the controller automatically reboots. Wait for the reboot to complete.

Note:

After reboot from a clean dist install, the controller requires default platform credentials and port (3011). The system passphrase is the default platform password. On the first commissioning of such controllers you are prompted to change the passphrase from the default value.

Step 4 Do one of the following:

To re-install the software versions to the controller, open a version of MultiSITE Supervisor that uses the same software version that you want on the controller, and use the platform Commissioning Wizard to install the desired software build.

If you have a backup dist file for the controller that was made when it had the desired prior N4 software version, use the Distribution File Installer to install it.

File Transfer Client

The File Transfer Client allows you to copy files and/or folders in both directions between your MultiSITE Supervisor PC and a remote platform. You can also use it to delete files and folders.

The File Transfer Client is useful to copy graphics images to a controller, or to copy a text file from a User Home folder on a remote controller (say, ~etc/system.properties) to your local PC, to allow editing. Then use the File Transfer Client to copy the edited version back to the controller's ~etc folder.

Note:

- Be careful when using the File Transfer Client, especially when copying files to a target platform, or when using the delete (X) control. In either direction, when transferring a file and an identically named file already exists or if deleting a file, a popup window confirms the action. After confirmation there is no Undo.
- 🛇 Do not use the File Transfer Client to copy modules to a controller, as "runtime profile types" are not applied, nor are module dependencies. Incorrect or missing modules may result. Always use the platform Software Manager to install (or uninstall) software modules on a controller.

Editing system.properties

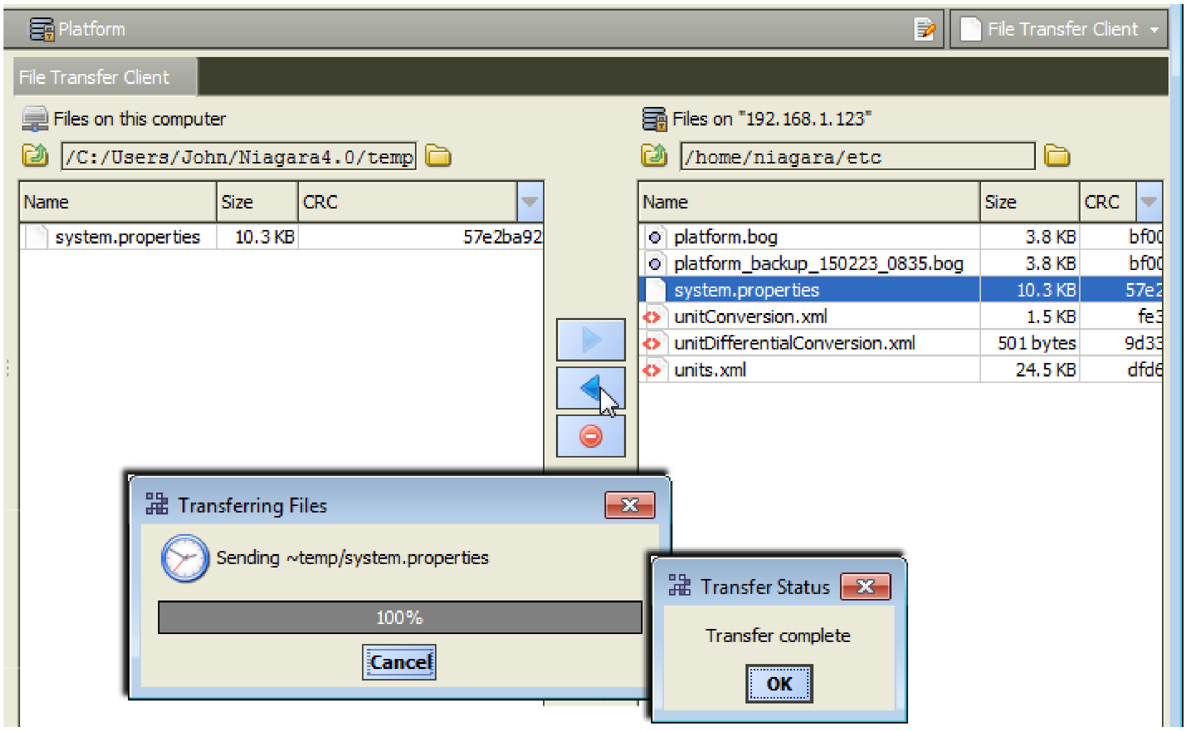
This procedure provides general steps for using the File Transfer Client to copy files between a Supervisor PC and a remote host.

Note:

- Editing, and especially activating system.properties entries is an operation for advanced users, with the possibility of undesirable results. Read all entries in this file carefully. Always save a backup copy of this file before editing it, and test the system after implementing a change.

Step 1 Connect to the platform and click Platform→File Transfer Client. The File Transfer Client window opens.

Figure 18: File Transfer Client window



/C:/Users/John/Niagara4.0/temp

Name	Size	CRC
system.properties	10.3 KB	57e2ba92

/home/niagara/etc

Name	Size	CRC
platform.bog	3.8 KB	bf0
platform_backup_150223_0835.bog	3.8 KB	bf0
system.properties	10.3 KB	57e2
unitConversion.xml	1.5 KB	fe3
unitDifferentialConversion.xml	501 bytes	9d33
units.xml	24.5 KB	dfd6

Transferring Files

Sending ~temp/system.properties

100%

Cancel

Transfer Status

Transfer complete

OK

The File Transfer Client provides a two-pane view.

- The left pane provides access to local (MultiSITE Supervisor PC) files.
- The right pane provides access to files on the remote platform.

Step 2 Click the navigation controls at the top of each pane to go to the appropriate location for source and target.

Step 3 Select one or more items on one side (as source) to copy to the other side (target), and click the appropriate transfer arrow.

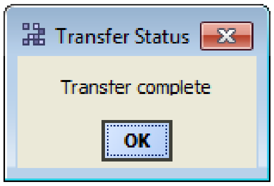
For local-to-remote transfer of a file containing encrypted, sensitive data, the File Transfer Client does not prompt you to enter a passphrase. Instead, the results of the transfer are one of the following:

This message displays when all files are transferred:

- Transfer completes successfully if the file is protected with a passphrase that matches the system passphrase
- Transfer fails in the following cases:
  – the file is protected with a passphrase that differs from the system passphrase
  – more than one protected file is included in the same transfer.

When finished, the system displays the following message.

Figure 19: Transfer complete



Transfer complete

A station must be restarted before changes to system.properties become effective.

Step 4 Stop the station using the platform Application Director, and wait for the station to stop completely, ensuring that it saves its database.

Step 5 From the Platform Administration view, select Reboot.

Allow sufficient time for the controller to reboot and station to start.

Step 6 Reconnect to the station with MultiSITE Supervisor to verify operation.

Lexicon Installer

The Lexicon Installer lets you install file-based sets of the text used by the software from your MultiSITE Supervisor PC to a remote platform.

Note:

In Niagara 4, usage of this view and file-based lexicon sets is typically not recommended. Instead, make one or more modules of customized lexicons using the Lexicon Module Builder, and install them in a remote platform using the Software Manager. Otherwise, issues may occur when accessing a host station using a browser.

Lexicons can also be installed as modules (.jar files), in which case you use the platform Software Manager (instead) for installation in remote platforms. In fact, "standard lexicons" are distributed as modules, using a module file name convention of:

niagaraLexiconLc-rt.jar

where Lc is the two-character language code, such as Fr for French and Es for Spanish. MultiSITE Supervisor provides a Lexicon Tool with a special Lexicon Module Maker view that you can use to modify or make new lexicon modules, from edited text-based lexicon files.

Lexicons typically have one of two uses, depending on job location:

- International locations provide non-English language support
- Domestic (U.S.) locations where you have modified the English (en) lexicon to change the wording used in default labels.

Beforehand, use the Lexicon Editor view of the Lexicon Tool in MultiSITE Supervisor to review and edit entries (or keys) in the individual lexicon files with localized values needed for language support.

Install lexicons to support additional languages

This step installs one or more text-based lexicon file sets in the host controller. Lexicons provide support for non-English languages. A locale code identifies each lexicon. For example, "fr" identifies the French lexicon and "de" the German lexicon. In some domestic (U.S.) installations, an English lexicon ("en") is added and configured to globally customize items, such as the property descriptions in MultiSITE Supervisor.

Prerequisites: The lexicon file(s) to install are in the !lexicons folder under your Niagara 4 Sys Home (niagara_home)

Note:

The recommendation for Niagara 4 is to skip this step. Instead, make one or more modules of customized lexicons and install them in the next (Select modules) step. Otherwise, issues may occur when using a browser to access of the hosted station.

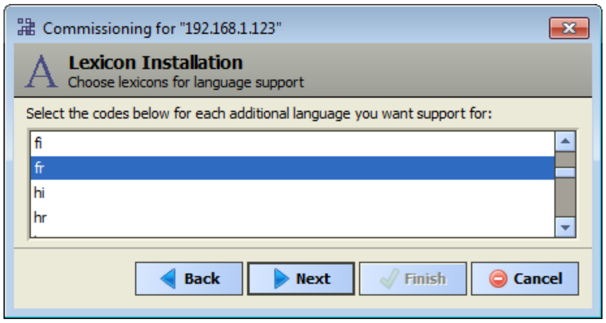
Step 1 Click the Lexicon Installer.

Any existing file-based lexicon sets (already installed in that platform) are listed in the view pane.

Step 2 Click a language code to select it, as shown below.

To install more than one lexicon, hold down the Ctrl key while you click.

Figure 20: Lexicon Installer



Commissioning for "192.168.1.123"

Lexicon Installation

Choose lexicons for language support

Select the codes below for each additional language you want support for:

fi
fr
hi
hr

Step 3 Click the Next button and follow the wizard, and click OK.

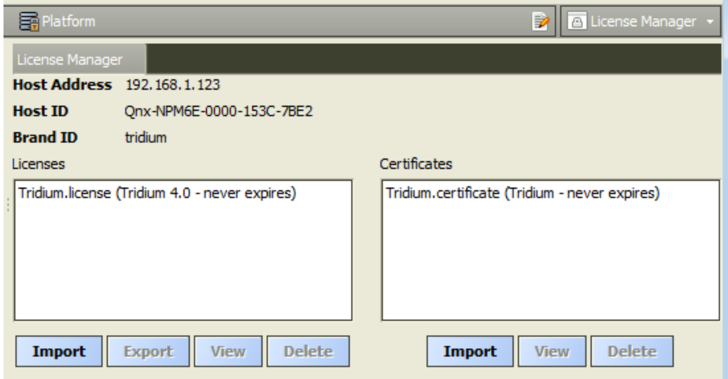
The selected lexicon directory or directories are installed in the remote platform. When all files are transferred, an Installation Complete window opens.

License Manager

The License Manager lets you install (import) licenses and certificates to a remote platform, sourced either from your MultiSITE Supervisor PC or the Niagara licensing server. You can also view the contents of licenses and certificates, and if desired, delete them from a remote platform.

The MultiSITE Supervisor management of licenses uses a structured local license database and utilization of a license archive file format. In addition, a MultiSITE Supervisor License Manager tool is available, which does not require a platform (or station) connection to use. See Chapter 5: License Tools and Files, for details about the contents (features) of license files.

Figure 21: License Manager lists existing licenses and certificates



Host Address 192.168.1.123
Host ID Qnx-NPM6E-0000-153C-7BE2
Brand ID tridium

Licenses
Tridium.license (Tridium 4.0 - never expires)

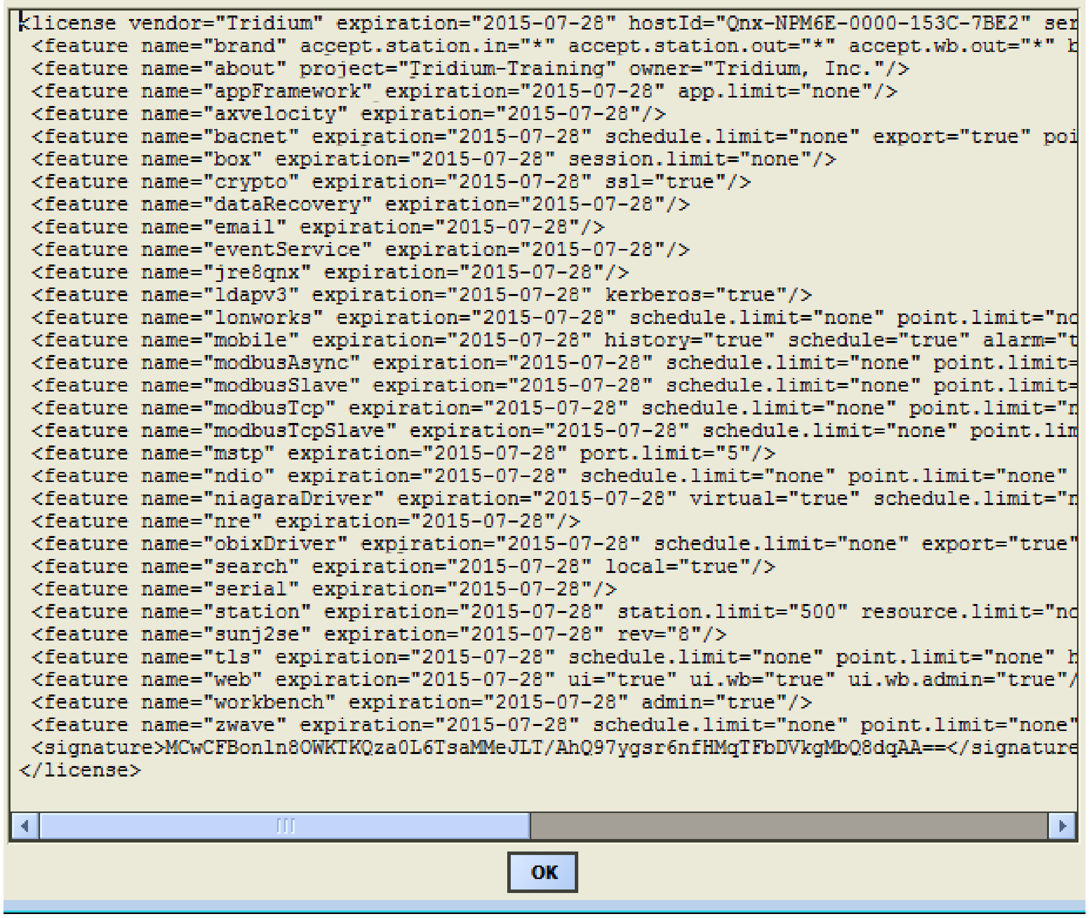
Certificates
Tridium.certificate (Tridium - never expires)

The License Manager lists any existing licenses and certificates (already installed in the platform). Below the left-hand license side of the License Manager, the following buttons (commands) display:

- Import: This installs a new license or certificate file. Typically, you import license files from either the online licensing server or from your local license database.
- Export: This saves a license file as a license archive (.lar) file.
- View: This opens an existing license file (clicking this button is the same as double-clicking an item).
- Delete: This removes an existing license file.

Click a license or certificate to select it, or double-click to view it in a window, as shown in the next figure.

Figure 22: Viewing a license in License Manager



```
<license vendor="Tridium" expiration="2015-07-28" hostId="Qnx-NPM6E-0000-153C-7BE2" ser
 <feature name="brand" accept.station.in="*" accept.station.out="*" accept.wb.out="*" b
 <feature name="about" project="Tridium-Training" owner="Tridium, Inc."/>
 <feature name="appFramework" expiration="2015-07-28" app.limit="none"/>
 <feature name="axvelocity" expiration="2015-07-28"/>
 <feature name="bacnet" expiration="2015-07-28" schedule.limit="none" export="true" poi
 <feature name="box" expiration="2015-07-28" session.limit="none"/>
 <feature name="crypto" expiration="2015-07-28" ssl="true"/>
 <feature name="dataRecovery" expiration="2015-07-28"/>
 <feature name="email" expiration="2015-07-28"/>
 <feature name="eventService" expiration="2015-07-28"/>
 <feature name="jre8qnx" expiration="2015-07-28"/>
 <feature name="ldapv3" expiration="2015-07-28" kerberos="true"/>
 <feature name="lonworks" expiration="2015-07-28" schedule.limit="none" point.limit="nc
 <feature name="mobile" expiration="2015-07-28" history="true" schedule="true" alarm="t
 <feature name="modbusAsync" expiration="2015-07-28" schedule.limit="none" point.limit=
 <feature name="modbusSlave" expiration="2015-07-28" schedule.limit="none" point.limit=
 <feature name="modbusTcp" expiration="2015-07-28" schedule.limit="none" point.limit="n
 <feature name="modbusTcpSlave" expiration="2015-07-28" schedule.limit="none" point.lim
 <feature name="mstp" expiration="2015-07-28" port.limit="5"/>
 <feature name="ndio" expiration="2015-07-28" schedule.limit="none" point.limit="none"
 <feature name="niagaraDriver" expiration="2015-07-28" virtual="true" schedule.limit="n
 <feature name="nre" expiration="2015-07-28"/>
 <feature name="obixDriver" expiration="2015-07-28" schedule.limit="none" export="true"
 <feature name="search" expiration="2015-07-28" local="true"/>
 <feature name="serial" expiration="2015-07-28"/>
 <feature name="station" expiration="2015-07-28" station.limit="500" resource.limit="nc
 <feature name="sunj2se" expiration="2015-07-28" rev="8"/>
 <feature name="tls" expiration="2015-07-28" schedule.limit="none" point.limit="none" h
 <feature name="web" expiration="2015-07-28" ui="true" ui.wb="true" ui.wb.admin="true"/
 <feature name="workbench" expiration="2015-07-28" admin="true"/>
 <feature name="zwave" expiration="2015-07-28" schedule.limit="none" point.limit="none"
 <signature>MCwCFBonln8OWKTKQza0L6TsaMMeJLT/AhQ97ygsr6nfHMqTFbDVkgMbQ8dqAA==</signature
</license>
```

A license and a certificate is 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. It is used for verifying the authenticity of license files. All hosts require a Tridium certificate. If third-party modules are installed, one or more additional certificates may be needed.

Note:

⃠ Do not delete an existing license or certificate without specific reason. This will likely render the controller inoperable until a proper license or certificate is reinstalled.

About the licensing server

The licensing server is an online database of licenses and certificates. As the final license authority, it contains the most current version of each host platform's license. This includes licenses for controllers, Supervisors, and Workstation-only applications.

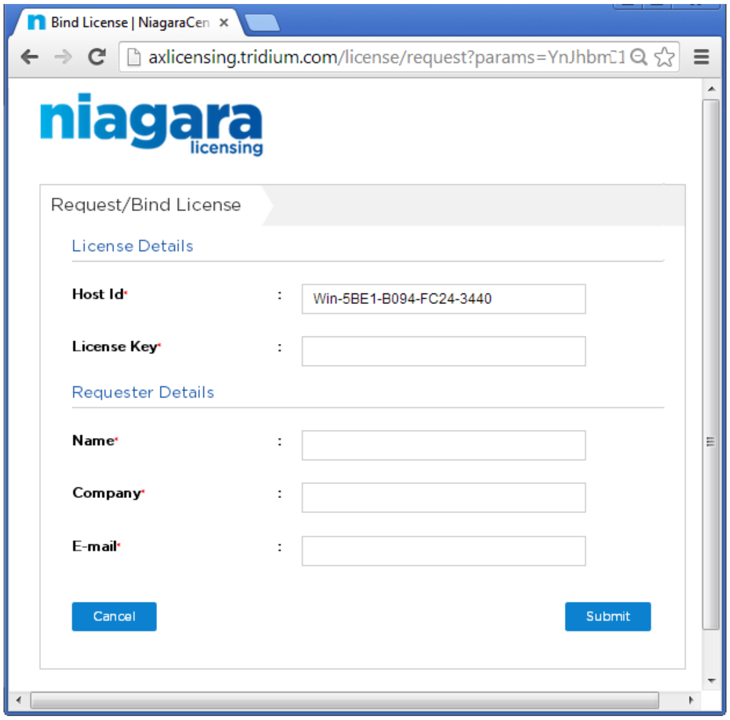
In addition to using the License Manager to access licenses via the licensing server, other MultiSITE Supervisor views use the licensing server to confirm that a feature is licensed. Examples include the MultiSITE Supervisor Local License Database tool and the Network License Summary view of the Licenses slot of the NiagaraNetwork's ProvisioningNwExt

Provided that your PC currently has Internet connectivity while running a platform connection to any host, the License Manager automatically retrieves and installs individual licenses.

You can also retrieve and install a license using the Import button, then selecting the license server option. As a side benefit, the system updates your local license database.

Note that if sourcing from the license server while platform-connected to a host that has not yet been assigned a license by the server (or has a pending license), a license request form opens in your computer's default browser, as shown below.

Figure 23: License request form in browser (from Workbench, Tools→Request License


Bind License | NiagaraCen
axlicensing.tridium.com/license/request?params=YnJhbm
niagara
licensing
Cancel
Submit

Request/Bind License

License Details

Host Id* : Win-5BE1-B094-FC24-3440

License Key* :

Requester Details

Name* :

Company* :

E-mail* :

This lets you submit a license request to the licensing server that includes the platform's Host ID. In this window, be sure to enter your name, and email address.

If you already received a License Key, a pending unbound license already exists on the licensing server. In this case, you can enter the license key along with the part number to activate that license, and make it immediately available.

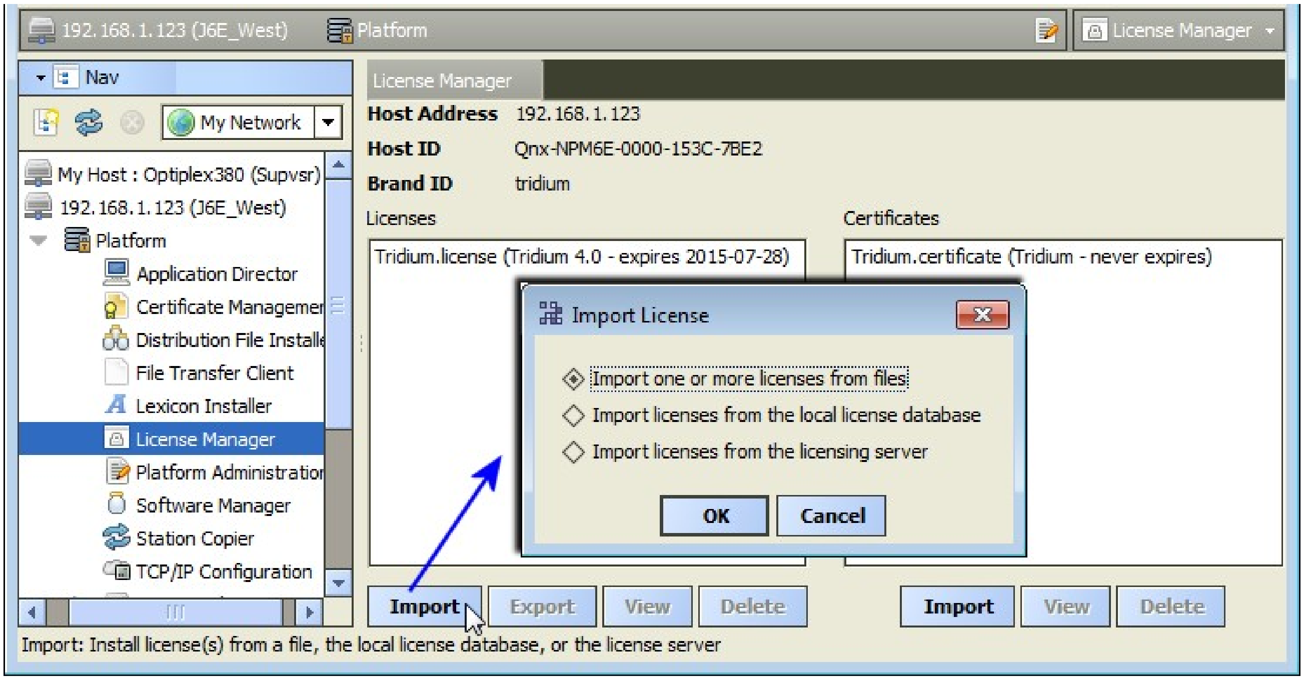
Upon approval, the system sends the host's license file, typically in a zipped format, by email back to the entered address. At that point, it is also available for automatic retrieval using the corresponding licensing server operations from various views, such as the License Manager, Workbench License Manager view, and so forth.

Import using License Manager

The ability to import a license using the License Manager is always available, and provides various options for installing a license file from local files, from the licensing server, or from your local license database.

If you choose Import from the License Manager, the Import License window asks you to select the location of the source license.

Figure 24: Import window from License Manager



Host Address 192.168.1.123

Host ID Qnx-NPM6E-0000-153C-7BE2

Brand ID tridium

Tridium.license (Tridium 4.0 - expires 2015-07-28)

Tridium.certificate (Tridium - never expires)

◈ Import one or more licenses from files

◇ Import licenses from the local license database

◇ Import licenses from the licensing server

Import: Install license(s) from a file, the local license database, or the license server

Select one of the following options (depending on scenarios, some options may be unavailable):

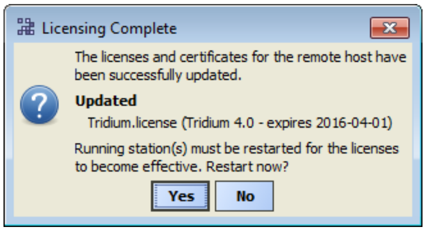
- Import one or more licenses from files: Always an available option, this opens a Select File window in which you can navigate to either a source license archive (.lar) file or an unzipped license file. When you select a license or license archive file, an attempt is made to install the license in the host platform.
- Import licenses from the local license database: This option is unavailable (grayed out) if the host's license file is not in your local license database, or if the license in your local license database already matches the currently installed license. With this option selected, the license is immediately installed in the remote host platform.
- Import licenses from the licensing server: Typically, this option is available if your MultiSITE Supervisor PC has Internet connectivity. When you select this option, the system searches the licensing server and installs the license.

Depending on the Import option chosen in the License Manager and the success of the import attempt, after you click OK, one of the following windows may open to signal completion.

- Licensing Complete: The license was successfully added, as shown below.

If a station is running on the host platform, this window informs you that the station must be restarted for the license(s) to become effective, and provides a Yes button to do this now. Or, you can select No and do this manually later.

Figure 25: Licensing Complete dialog



Licensing Complete

The licenses and certificates for the remote host have been successfully updated.

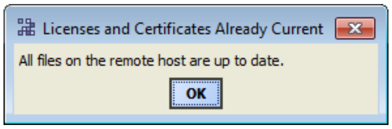
Updated

Tridium.license (Tridium 4.0 - expires 2016-04-01)

Running station(s) must be restarted for the licenses to become effective. Restart now?

- Licenses and Certificates Already Current: The license currently installed on the host already matches the source license (whether specifying any of the license import options). The following window opens.

Figure 26: License and Certificates Already Current

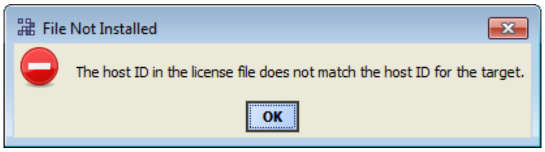


Licenses and Certificates Already Current

All files on the remote host are up to date.

- File Not Installed: No appropriate license (by host ID) was found in either the license file or the license archive specified when importing by file. The following window appears.

Figure 27: File Not Installed dialog



File Not Installed

The host ID in the license file does not match the host ID for the target.

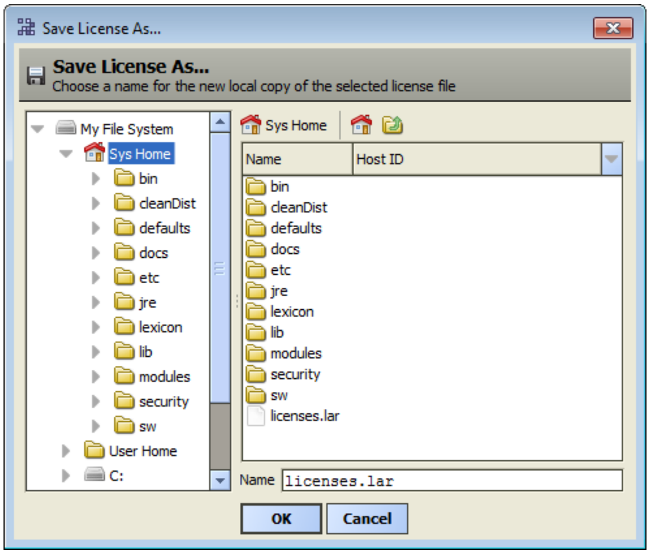
- (License Request Form, in browser): If importing from the license server and an existing license was not found for this host platform, a separate window (of your default browser) opens with a license request form, showing the host ID for this host.

Export using License Manager

The ability to export a license using the License Manager is always available if you have a license selected, to save locally as a license archive file.

With a license selected in the License Manager, the Export button opens a Save License As... window to save that license file locally on your MultiSITE Supervisor PC, as a license archive (.lar) file, as shown in the figure below.

Figure 28: Save License As dialog



Save License As...

Choose a name for the new local copy of the selected license file

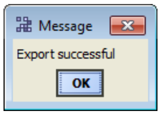
Name: licenses.lar

Note that you can use the License Manager’s Import command to install any exported license archive, or the equivalent Import File command in the License Manager view.

By default, the system saves a license archive file in the root of your Niagara release directory. If needed, use the window’s navigation controls to specify another target folder or drive. Before saving, you can also rename the license archive file, to make it more identifiable. For example, instead of: licenses.lar, you could rename it My6E.lar.

After exporting a license, a notification window opens, as shown below.

Figure 29: Exported license archive notification dialog



Export successful

Synchronizing with the Supervisor license database

The local Supervisor maintains a database that includes information about each host’s license. It is recommended to periodically interrogate each host and update this license database.

Prerequisites: You have a network of licensed hosts.

Step 1 Expand the ProvisioningNwExt in the Nav tree to see its Licenses node.

Step 2 Right-click Licenses and select Views→Supervisor License Manager.

The Supervisor License Manager window opens.

Step 3 Click Synchronize.

The system prompts with the option to Synch All Licenses?

Step 4 Click Yes and, at the Synchronization Complete prompt, click OK.

The Supervisor’s license database contains the license identifier for each host in the network.

Automating host licenses updates

This procedure uses the Niagara Network Job Builder to create a one-time provisioning job to automate the updating of one or more host licenses in a network.

Prerequisites: The BatchJobService and ProvisioningNwExt components are available under your NiagaraNetwork.

Step 1 Double-click ProvisioningNwExt.

The system displays the Niagara Network Job Builder view.

Step 2 In the top Initial steps to run only once pane, click the Add button.

Step 3 In the New Job Step popup window, click the Update Licenses step and click OK.

Step 4 In the lower Stations to include in the job pane, click the Add button,

Step 5 In the Add Device popup window, click to select the stations and click OK.

Step 6 To initiate the provisioning job, review your choices and click the Run Now button at the bottom of the Niagara Network Job Builder View.

The view changes to the Niagara Network Job View, where steps and results appear as they are executed.

The licenses for all selected hosts are up-to-date. To make updating licenses a regular automatic event, you need to create a job prototype.

Updating licenses from the Network License Summary

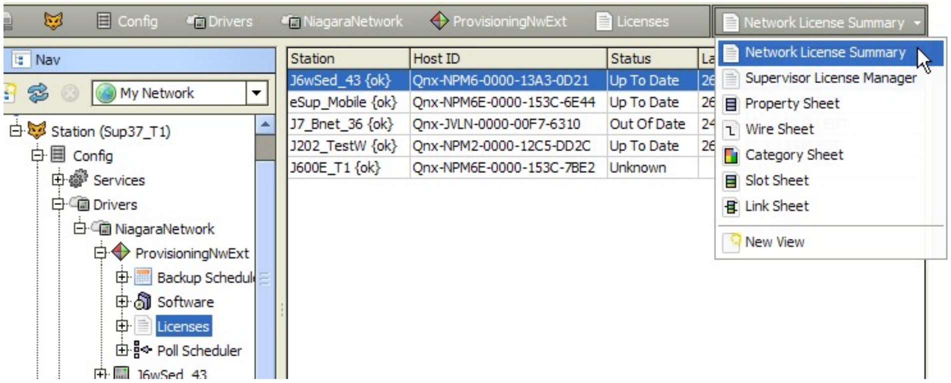
Rather than create a one-time provisioning job, you can update the license on one or more remote hosts using the Network License Summary.

Prerequisites: You have synchronized the Supervisor's license database with the host controllers in your network, purchased a license upgrade for each host, and the upgrades are available on the online licensing server.

Step 1 Select the Licenses slot on the ProvisioningNwExt.

The system displays the Network License Summary.

Figure 30: Network License Summary



Station	Host ID	Status	La
J6wSed_43 {ok}	Qnx-NPM6-0000-13A3-0D21	Up To Date	26
eSup_Mobile {ok}	Qnx-NPM6E-0000-153C-6E44	Up To Date	26
J7_Bnet_36 {ok}	Qnx-JVLN-0000-00F7-6310	Out Of Date	24
J202_TestW {ok}	Qnx-NPM2-0000-12C5-DD2C	Up To Date	26
J600E_T1 {ok}	Qnx-NPM6E-0000-153C-7BE2	Unknown	

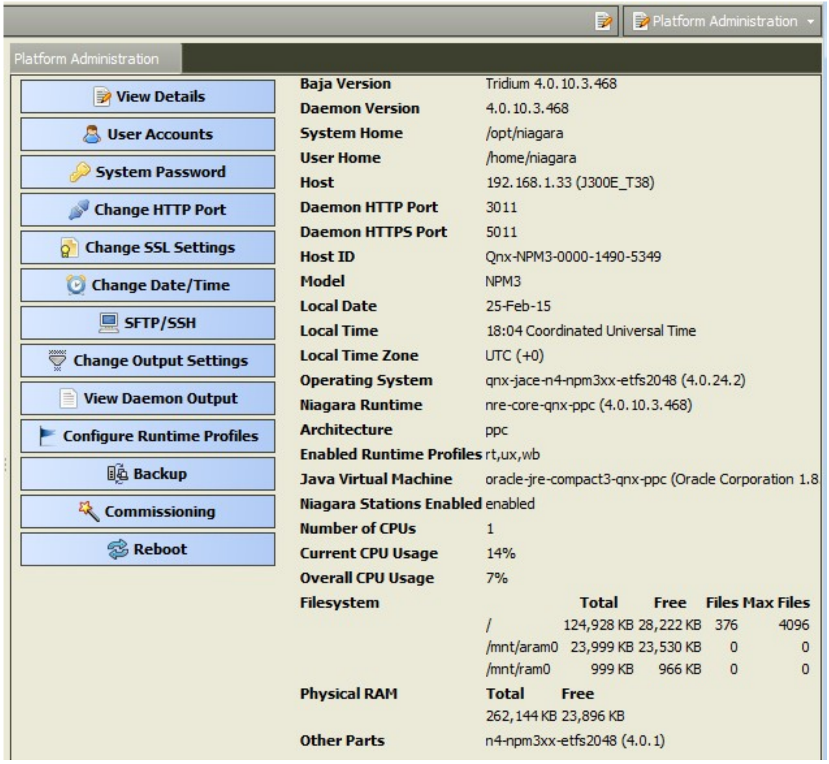
Step 2 Select one or more stations and click Update.

If a newer license is found (than that already installed), the system installs it in the remote host (s), updates the license(s) in the Supervisor's local license database, and resets the Last Updated timestamp to the time of the update.

Platform Administration

The Platform Administration view provides access to various platform daemon (and host) settings and summary information.

Figure 31: Platform Administration view



```
Baja Version              Tridium 4.0.10.3.468
Daemon Version            4.0.10.3.468
System Home               /opt/niagara
User Home                 /home/niagara
Host                      192.168.1.33 (J300E_T38)
Daemon HTTP Port          3011
Daemon HTTPS Port         5011
Host ID                   Qnx-NPM3-0000-1490-5349
Model                     NPM3
Local Date                25-Feb-15
Local Time                18:04 Coordinated Universal Time
Local Time Zone           UTC (+0)
Operating System          qnx-jace-n4-npm3xx-etfs2048 (4.0.24.2)
Niagara Runtime           nre-core-qnx-ppc (4.0.10.3.468)
Architecture              ppc
Enabled Runtime Profiles  rt,ux,wb
Java Virtual Machine      oracle-jre-compact3-qnx-ppc (Oracle Corporation 1.8
Niagara Stations Enabled  enabled
Number of CPUs            1
Current CPU Usage         14%
Overall CPU Usage         7%
Filesystem                                Total       Free  Files Max Files
                          /          124,928 KB  28,222 KB    376      4096
                          /mnt/aram0  23,999 KB  23,530 KB      0         0
                          /mnt/ram0      999 KB     966 KB      0         0
Physical RAM              Total       Free
                          262,144 KB  23,896 KB
Other Parts               n4-npm3xx-etfs2048 (4.0.1)
```

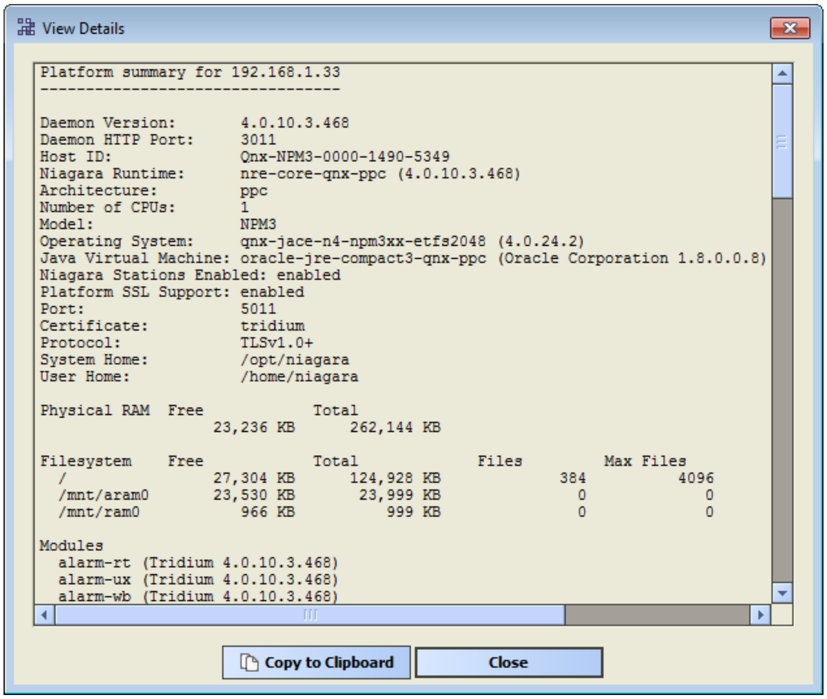
Available functions appear as buttons on the left side, and summary information is listed in the right side. Typical use is when commissioning a new controller, or to troubleshoot platform or host problems.

During a platform connection, upon first access to Platform Administration, a small delay occurs while downloading data about that platform’s installed modules. You may briefly see a Loading Modules window before the main view appears.

View Details

This selection from the main Platform Administration view provides platform summary data, available to the Windows clipboard. It includes all summary information shown in main Platform Administration view, plus installed modules, and so on. You access these details by double-clicking the View Details button in the NavContainerView.

Figure 32: View Details dialog in Platform Administration



```
Platform summary for 192.168.1.33
---------------------------------

Daemon Version:       4.0.10.3.468
Daemon HTTP Port:     3011
Host ID:              Qnx-NPM3-0000-1490-5349
Niagara Runtime:      nre-core-qnx-ppc (4.0.10.3.468)
Architecture:         ppc
Number of CPUs:       1
Model:                NPM3
Operating System:     qnx-jace-n4-npm3xx-etfs2048 (4.0.24.2)
Java Virtual Machine: oracle-jre-compact3-qnx-ppc (Oracle Corporation 1.8.0.0.8)
Niagara Stations Enabled: enabled
Platform SSL Support: enabled
Port:                 5011
Certificate:          tridium
Protocol:             TLSv1.0+
System Home:          /opt/niagara
User Home:            /home/niagara

Physical RAM  Free            Total
                   23,236 KB      262,144 KB

Filesystem    Free            Total                Files         Max Files
  /                27,304 KB      124,928 KB                384           4096
  /mnt/aram0       23,530 KB       23,999 KB                  0              0
  /mnt/ram0           966 KB          999 KB                  0              0

Modules
  alarm-rt (Tridium 4.0.10.3.468)
  alarm-ux (Tridium 4.0.10.3.468)
  alarm-wb (Tridium 4.0.10.3.468)
```

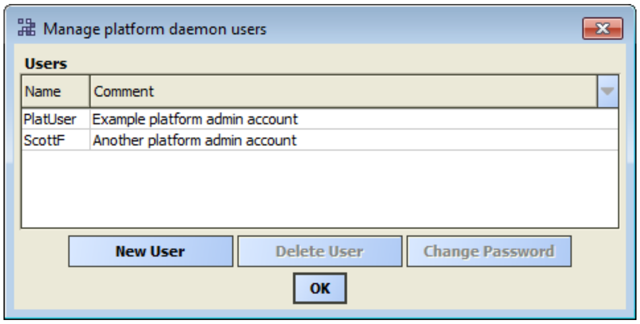
Included in the View Details window is a listing of all installed modules, lexicons, licenses, and certificates. Included is a station line, listing configuration for autostart and autorestart, and current status. Generally, information in this view is helpful when troubleshooting or asking for technical support. The following buttons are available:

- Copy to Clipboard: Puts all details in the window on your PC's Windows clipboard.
- Close: Exits the window. This is the same as Windows close control (contents copied remain on clipboard).

User Accounts

This selection from the main Platform Administration view is available on Niagara 4 controllers only. Unlike in NiagaraAX, the controller may have multiple platform administrator users (up to 20 maximum). All have the same full administrator permissions, can create additional users, and can change the password of their own accounts.

Figure 33: Example where two platform admin accounts have been created



Manage platform daemon users

Users

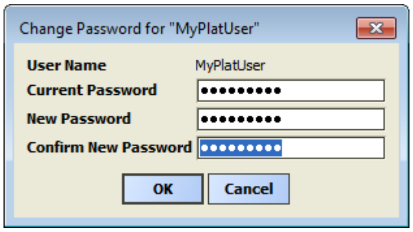
Name	Comment
PlatUser	Example platform admin account
ScottF	Another platform admin account

If you are commissioning a new unit, or a controller that has had a cleanDist file installed, only a well-known default platform admin account exists. Any unit with the default platform admin user is extremely susceptible to unauthorized intrusion. Therefore, before you can complete other commissioning tasks, the N4 Commissioning Wizard requires you to first replace the default platform user account in a wizard step.

Changing a password to access a remote platform

Changing the password is required to access any platform. This requires that you enter the current password, then enter the new password (twice) in the popup window. A strong password is required.

Figure 34: Change Password dialog



Change Password for "MyPlatUser"

User Name MyPlatUser

Current Password •••••••••

New Password •••••••••

Confirm New Password •••••••••

If you enter an incorrect current password, an Invalid login credentials error popup opens. After clicking OK you return back to the change password window above.

- If you are changing your password (used in your current platform session), your new credentials become immediately effective upon clicking OK. If you previously had Remember these credentials, selected in the Authentication login window, the cached credentials are automatically updated.

Note that any platform user can delete any other platform user except when:

- The user is active in the current platform session, or
- The user is the original platform user, meaning the one created in the Remove platform default user account step when using the Commissioning Wizard to commission the controller. Such users cannot be selected to delete.

Update Authentication

For Niagara 4 platforms, this Platform Administration view is available on Windows-based hosts only. You use it to specify the Windows users group for platform administrator access.

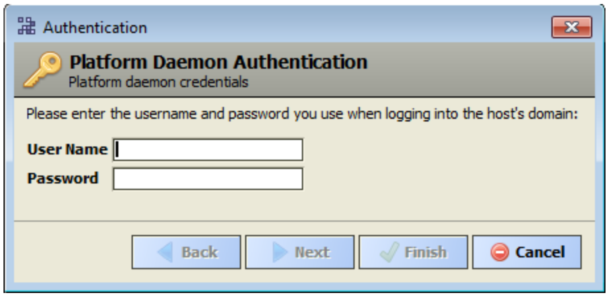
This function is also available in a platform connection to an AX host, to change the credentials for the single (digest) platform user. It is unavailable in a platform connection to an AX Windows host.

Unlike in NiagaraAX, authentication in Niagara 4 uses only basic (native Windows OS user) authentication for platform access—file/digest platform access is no longer an option. The platform User Manager view is also not available. Instead, you must use native Windows tools to create and manage Windows OS users and groups.

This theme also applies to the TCP/IP Configuration view for a Niagara 4 Windows host, which is available, but is read-only (allowing you to review current TCP/IP settings). Also, unlike in NiagaraAX, there is only one level of platform access for any Niagara 4 host—admin level. This level applies to Windows platforms as well as to controller platforms.

When you click Update Authentication on a Windows host, you see a login window, as shown below.

Figure 35: Login window for Update Authentication on Niagara 4 Windows platform



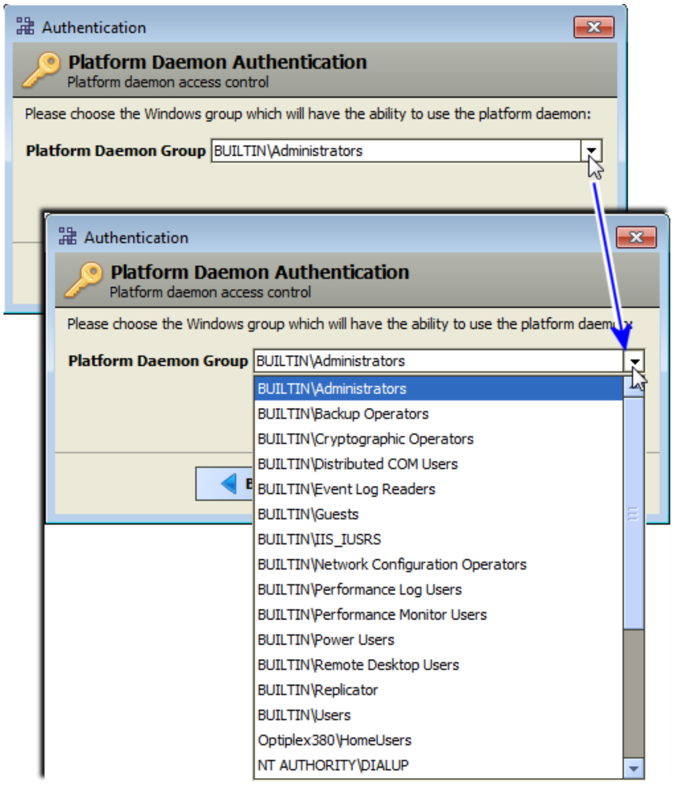
Please enter the username and password you use when logging into the host's domain:

User Name

Password

Use your standard Windows login credentials. If the host is on a Windows domain, log in using the credentials you use when logging in to that domain. This is necessary to limit the number of possible domain groups to only those groups in which you are a member. Such groups are selectable in the next window to choose the sole Windows users group for platform daemon access, as shown in the next figure.

Figure 36: Windows platform daemon group selection dialog



Authentication

Platform Daemon Authentication

Platform daemon access control

Please choose the Windows group which will have the ability to use the platform daemon:

Platform Daemon Group BUILTIN\Administrators

BUILTIN\Administrators
BUILTIN\Backup Operators
BUILTIN\Cryptographic Operators
BUILTIN\Distributed COM Users
BUILTIN\Event Log Readers
BUILTIN\Guests
BUILTIN\IIS_IUSRS
BUILTIN\Network Configuration Operators
BUILTIN\Performance Log Users
BUILTIN\Performance Monitor Users
BUILTIN\Power Users
BUILTIN\Remote Desktop Users
BUILTIN\Replicator
BUILTIN\Users
Optiplex380\HomeUsers
NT AUTHORITY\DIALUP

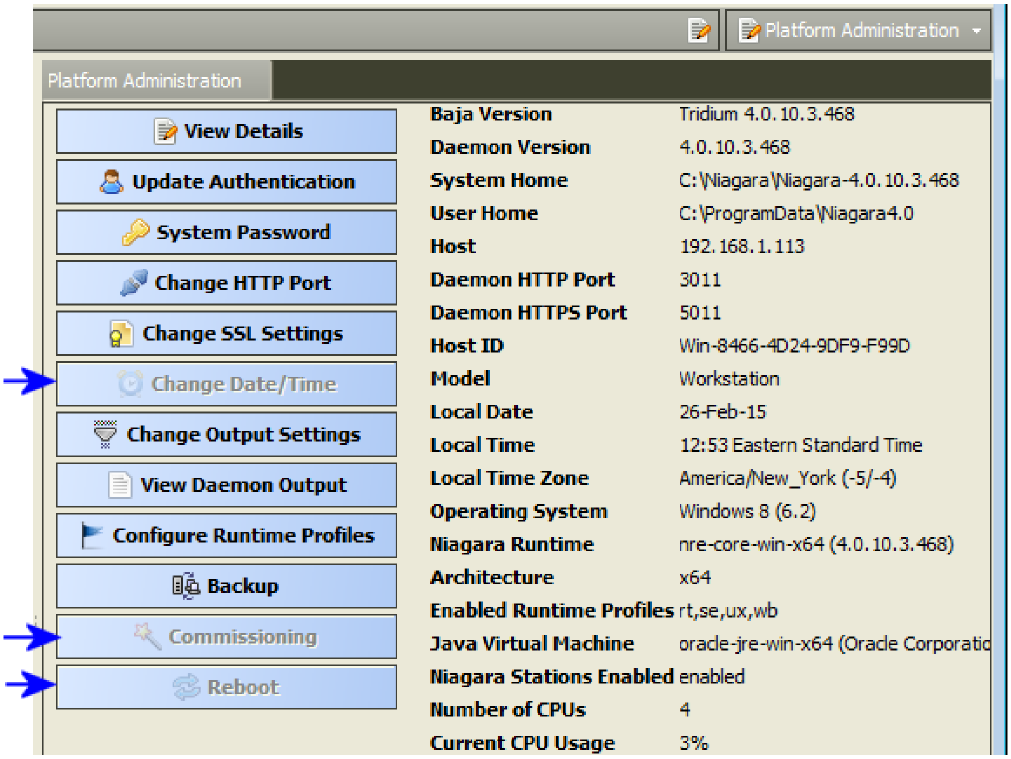
This window lets you select the one Windows users group that can make platform connections to this host. Groups include Windows built-in user groups (include “BUILTIN” or “NT AUTHORITY” prefix), as well as any locally-defined user groups. If the host has been added to a Windows domain, groups defined in that domain are also listed and available.

Note:

Domain groups are limited to only those in which the login user is a member.

When platform-connected to a Niagara 4 Windows host, some Platform Administration view buttons are unavailable, as shown in the figure below.

Figure 37: Platform Administration view in platform connection to remote Niagara 4 Windows host



Baja Version	Tridium 4.0.10.3.468
Daemon Version	4.0.10.3.468
System Home	C:\Niagara\Niagara-4.0.10.3.468
User Home	C:\ProgramData\Niagara4.0
Host	192.168.1.113
Daemon HTTP Port	3011
Daemon HTTPS Port	5011
Host ID	Win-8466-4D24-9DF9-F99D
Model	Workstation
Local Date	26-Feb-15
Local Time	12:53 Eastern Standard Time
Local Time Zone	America/New_York (-5/-4)
Operating System	Windows 8 (6.2)
Niagara Runtime	nre-core-win-x64 (4.0.10.3.468)
Architecture	x64
Enabled Runtime Profiles	rt,se,ux,wb
Java Virtual Machine	oracle-jre-win-x64 (Oracle Corporatio
Niagara Stations Enabled	enabled
Number of CPUs	4
Current CPU Usage	3%

As shown above, Change Date/Time, Commissioning, and Reboot are unavailable when the platform is connected to any Niagara 4 Windows host (remote or local). For a local platform connection, Configure Runtime Profiles is also unavailable.

Notes about station access to a Windows platform

- Station (Fox) and/or HTTP access of a station running on a Niagara 4 Windows platform prevents any date, time, or time zone host changes via the station’s PlatformServices (differing from NiagaraAX). In PlatformServices, this is reflected by the following:
  - Properties of the PlatformServiceContainer for System Time, Date, and Time Zone are read-only, as are those same properties in the System Date Time Editor view on PlatformServices.
  - The child NTP platform service (NtpPlatformServiceWin32) comes up as both disabled and read-only, and thus has no application.

You must make any necessary changes to these items through the Windows OS on the Niagara 4 host. However, note that access of a Niagara 4 station running on a QNX host (JACE) provides write ability to all such items, depending on the permissions of the user.

System Passphrase

All Niagara 4 platforms have a system passphrase (password), used to encrypt sensitive information, such as client passwords stored in BOG files and station databases (config.bog files) or station backup distribution (. dist) files. The passphrase increases security for the files that contain critical information. In various Workbench operations, you are prompted to enter the passphrase, such as when copying stations or restoring station backups in remote platforms.

Note:

This system passphrase functionality applies to a JACE-8000 controller, even if you downgrade the unit from N4 to AX. In this situation, configuring sensitive data must be accomplished via the MultiSITE Supervisor.

The following areas of the framework are affected by passphrase implementation:

- Provisioning
- Distribution File Installer
- File Transfer Client
- Station Copier
- Back up
- Commissioning
- Export Tags

The sensitive information in files is protected with encryption, either by encrypting the information within the file or by encrypting the whole file. How encryption is applied depends on the expected portability of the file. Files located under the daemon User Home (files that belong to the system) are encrypted using a strong, randomly generated key that exists only on that system. Files located under a MultiSITE Supervisor User Home (portable files that can be sent to many systems) are encrypted using a key derived from the user-defined system passphrase entered during software installation or when the system passphrase is changed.

Due to the different types of encryption that are used for the system or portable locations, when transferring files between the daemon User Home and another MultiSITE Supervisor User Home, you must use the MultiSITE Supervisor platform tools (Station Copier, File Transfer Client or Backup) which convert files to use the correct encryption key for the target location.

Note:

⃠ Do not use Windows Explorer to copy files between the daemon User Home and other User Homes, because without the proper encryption those files may not be readable.

- For system-to-portable transfers: You can get portable copies of files located under the daemon User Home by any of these methods:
  - Make a backup from the Platform Administration view
  - Make a backup from a running station
  - Use either Station Copier or File Transfer Client from the Platform Administration view

The resulting local, portable copies and backup files are protected with a passphrase.

- For portable-to-system transfers: Alternatively, when you use the Distribution File Installer to restore a backup .dist file, or Station Copier to transfer a station from your MultiSITE Supervisor directory to a controller, the file’s passphrase is validated and used to translate the data back into the proper system encryption format for use under the daemon User Home.

Note:

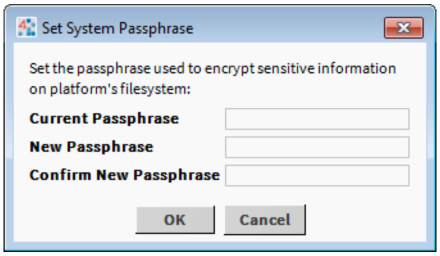
- It is very important to remember the system password and keep it safe. If you lose the system passphrase, you will lose access to encrypted data.

Update the system passphrase

To change the system passphrase on a Niagara 4 platform use either the Commissioning Wizard or the Platform Administration view as described here.

In the Platform Administration view, when you click System Password for any Niagara 4 platform (including a JACE-8000 downgraded to run AX-3.8U1), the Set System Password window opens.

Figure 38: Set System Password dialog



Set System Passphrase

Set the passphrase used to encrypt sensitive information on platform's filesystem:

Current Passphrase

New Passphrase

Confirm New Passphrase

A strong password is required (must match in both password fields). The characters you enter are obscured. Password rules are the same as for platform users. Use a minimum of 10 characters, with the following:

- At least one UPPER CASE character.
- At least one lower case character.
- At least one digit (numeral).

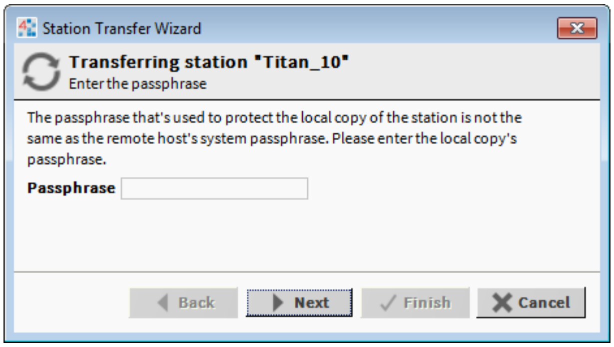
An error popup reminds you if you attempt to enter a password that does not meet minimum rules.

System passphrase usage in backups and station copies

The system passphrase is required when using either the Distribution File Installer to restore a backup .dist file, or the Station Copier to transfer a local file. Note the following:

- If the file passphrase and system passphrase are the same, the station copy proceeds without prompting for a passphrase.
- If the passphrase for the bog file is not the same as the passphrase for the target host platform, then you are prompted to enter the bog file’s passphrase, as shown below.

Figure 39: Station Transfer Wizard prompt for bog file passphrase



Station Transfer Wizard

Transferring station "Titan_10"

Enter the passphrase

The passphrase that's used to protect the local copy of the station is not the same as the remote host's system passphrase. Please enter the local copy's passphrase.

Passphrase

The above dialog is prompting you to enter the bog file’s passphrase.

Note:

- If you do not know the passphrase for a BOG file, you can edit it offline.
- If you do not know the passphrase for a .dist file you cannot install it.

Editing BOG files offline

Files created in MultiSITE Supervisor initially have no passphrase at all since the files do not yet contain sensitive data. You can add passphrase protection to offline BOG files by clicking the Bog File Protection icon in the toolbar.

If you change or add a passphrase value and then attempt to save, you are prompted to enter the file passphrase. You can save only if you enter the correct passphrase or add a new one.

If a BOG file is protected with an unknown passphrase, you can use the MultiSITE Supervisor toolbar icon to Unlock (force-remove) the passphrase, making the file unprotected, or “force-change” the passphrase to enter a new value. Choosing either of these options clears any sensitive data in the file.

Note:

- It is important to remember the system password and keep it safe. If you lose the system passphrase, you will lose access to encrypted data.
- When you Unlock (force-remove) or Change (force-change) the passphrase on a BOG file, it results in the loss of the sensitive data in the file.

System passphrase usage in JACE-8000

The JACE-8000 makes additional use of its system passphrase, to encrypt sensitive information on its removable microSD flash drive, as well as when writing backup images to a USB flash drive. The passphrase is assigned as the file passphrase for portable copies of backups and station copies.

Note:

The system passphrase default value is the same as the default platform password for controllers that you have just converted from NiagaraAX, and controllers on which you have just installed a clean dist. On the first commissioning of such controllers you are prompted to change the passphrase from the default value.

When inserting a JACE-8000 SD card into a replacement unit, note the following:

- If the replacement unit is preconfigured with the same system passphrase, the unit starts.
- If the replacement unit has a different system passphrase, the unit will not boot, and the status LED flashes every second. To resolve, you must make a serial connection and, when prompted, select either: Update the system passphrase, or Remove all encrypted data.

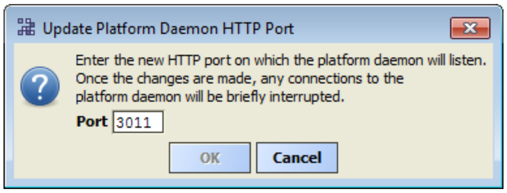
Change HTTP Port

This function on the Platform Administration view lets you change the HTTP port monitored by the host's platform daemon for regular platform client connections (connections that are not secure). By default, port 3011 is monitored for such connections. This differs from any port used for station (Foxs) connections that are secure.

Note:

- If there is a firewall on the host (or its network), before changing this port, make sure that the firewall will allow traffic to the new port.

Figure 40: Update Platform Daemon HTTP Port dialog



Update Platform Daemon HTTP Port

Enter the new HTTP port on which the platform daemon will listen. Once the changes are made, any connections to the platform daemon will be briefly interrupted.

Port 3011

If needed, you can change the daemon monitored port to another HTTP port. You may choose to do this for specific firewall reasons, or perhaps for additional security. As shown in the figure above, you can type in the new port number in the Port field, which enables the OK button.

When you click OK, the platform daemon restarts, and your platform connection reopens (this does not affect the operation of any running station). If previously connected on the port without security, the platform icon displays in the Nav tree with the new HTTP port number (:n) in parenthesis.

Note:

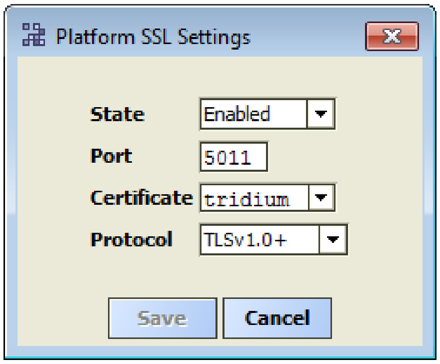
Before closing the host, which removes it from the Nav tree, carefully note the new (non-default) port number you entered. You must specify the port number the next time you open a platform using a connection that is not secure. To check this port number in a station running on the host, open Config→Services→PlatformServices property sheet.

Change TLS Settings

This function on the Platform Administration view configures a secure (TLS) platform connection, as well as change related secure platform connection (platformtls) properties.

The figure below shows the Platform SSL Settings window with default values.

Figure 41: Platform TLS Settings with default values (enabled)

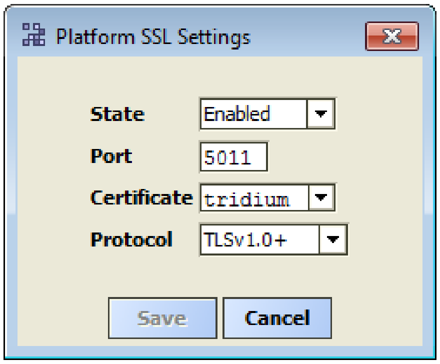


Platform SSL Settings

State: Enabled
Port: 5011
Certificate: tridium
Protocol: TLSv1.0+

The figure below shows an example window for a controller enabled for platform TLS (only). In this example, the controller uses a signed certificate with alias controller3 (previously imported), and the port and protocol settings left at defaults.

Figure 42: Example settings for a controller enabled for TLS, with a signed certificate



Platform SSL Settings

State: Enabled
Port: 5011
Certificate: tridium
Protocol: TLSv1.0+

When you click Save after making any changes, the changes are immediately applied. Often this means that your current platform connection will close, and then open in MultiSITE Supervisor.

For example if you change State from Tls Only to Disabled, your secure connection closes and opens again as a regular platform connection without security. Or, if while securely connected, you change the Port from (default) 5011 to another port number, your reopened platformtls connection uses this new port, shown in parentheses (nnnn) to indicate that a port other than the default is being used.

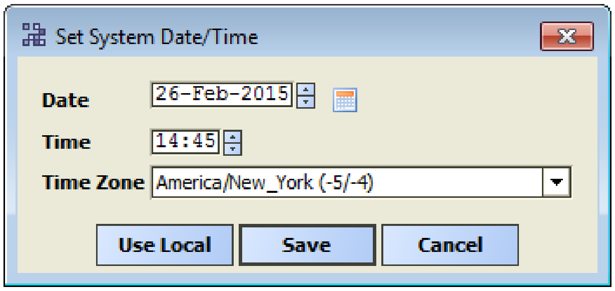
Note:

Before closing the host (removing it from the Nav tree), carefully note the new secure platform port number you entered. In the future you must specify that port number whenever making a secure connection to this platform.

Change Date/Time

This selection from the main Platform Administration view lets you change the date and time in the platform, as well as specify its time zone.

Figure 43: Set System Date/Time window



Set System Date/Time

Date: 26-Feb-2015

Time: 14:45

Time Zone: America/New_York (-5/-4)

Typically, if your MultiSITE Supervisor PC's current date/time settings are accurate, you click the Use Local button to synchronize the remote host's date, time, and time zone with your MultiSITE Supervisor PC. Upon Save, the remote host will have the identical settings.

Note:

To keep time synchronized across multiple platforms, configure the NtpPlatformService in the PlatformServices of the station running on each platform, as appropriate.

The Save button becomes available after you change one or more fields in the window, or when you click Use Local. Upon Save, any change is processed by the host's operating system.

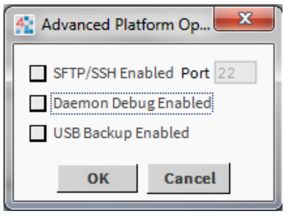
- To set the date, click in a day-month-year position to select, then click up/down controls, or click and type in numerals directly, or click the calendar icon for a popup dialog to select the date from a calendar.
- To set the time, click in a hour or minute position to select, then click up/down controls, or click and type in numerals directly.
- Select the time zone from the drop-down list.

Advanced Platform Options

This Platform Administration view selection appears for JACE platforms only, to enable, disable, or configure certain settings and properties.

For Windows-based hosts, you can use Windows "Remote Desktop Connections" for SFTP/SSH.

Figure 44: Advanced Platform Options



Advanced Platform Op...

☐ SFTP/SSH Enabled Port 22

☐ Daemon Debug Enabled

☐ USB Backup Enabled

Note:

This replaces an FTP/Telnet selection available for QNX-based platforms running NiagaraAX, which are both inherently less secure services.

This window displays the following options:

- SFTP/SSH Enabled Port

Use this to enable, disable, or configure SFTP (Secure File Transfer Protocol) or SSH (Secure Shell Protocol) access. For Windows-based hosts, you typically use Windows > Remote Desktop Connections instead.

In the factory-shipped state, a Niagara 4 controller has the SFTP and SSH service disabled. This may be best, especially if the platform is exposed to the public Internet. However, in some cases you may wish to temporarily enable the single port shared by these services, perhaps to facilitate debugging.

SSH access to a controller provides system shell access, providing (after login using platform credentials) the same menu as serial shell access to its RS-232 port.

Note:

- Even SFTP and SSH pose security risks. Before enabling, it is strongly recommended that you configure for platform TLS only, and keep this function disabled.

You can also change the TCP/IP port shared by these services from the well-known port to some other port. However, be sure that any firewalls being used on your network will allow traffic to that port.

- Daemon Debug Enabled check box

Enables a QNX webserver to accept incoming browser connections on: 3011 or :5011.

- USB Backup Enabled

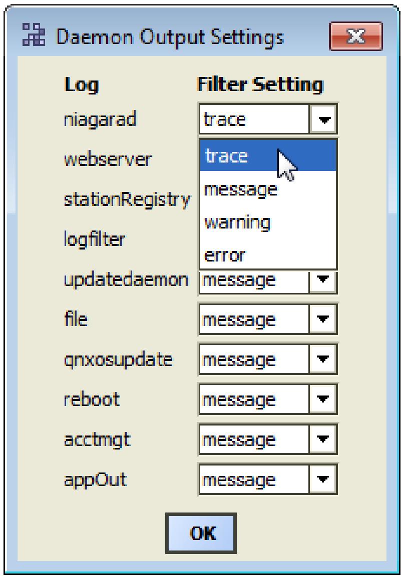
Enables or disables USB Backup for those platforms that have USB backup capability.

Change Output Settings

This function from the main Platform Administration view lets you adjust (tune) the amount and content of the platform daemon output.

You do this by changing the log filter settings of the various daemon processes.

Figure 45: Daemon Output Settings window for a JACE controller



Daemon Output Settings

Log	Filter Setting
niagarad	trace
webserver	
stationRegistry	
logfilter	
updatedaemon	message
file	message
qnxosupdate	message
reboot	message
acctmgt	message
appOut	message

Logs

By default, all daemon processes have a message log filter level, and include the following:

- niagarad — Log for the platform daemon (niagarad) process, with high level entries like niagarad starting, baja home = ..., niagarad stopping.
- webserver — Log for HTTP server for incoming platform client connections. Entries are often generic, before the daemon hands off to the appropriate platform servlet.
- stationregistry — Log for platform daemon management of stations, including startup, shutdown, and watchdog actions.
- logfilter — Logs changes to daemon log states, meaning it tracks the changes made in this window.
- updatedaemon — Log for handling MultiSITE Supervisor requests for current platform daemon configuration, used mainly by the Platform Administration view.
- file — Logs requests made to the platform daemon's file servlet, used in platform views like the File Transfer Client, Commissioning Wizard, Software Manager, Station Copier, and so on. Many different things can print on this log, such as request for file xxx, and wrote file xxx.
- qnxosupdate — Log for the OS upgrade servlet created by the platform daemon. MultiSITE Supervisor uses this servlet to upgrade the QNX OS in the host JACE when using the Commissioning Wizard or Distribution File Installer. Entries here can reflect a problem when updating the QNX OS, such as os crc isn't right, and waitpid when launching osupdate command failed.
- reboot — Log for the reboot servlet, one of the servlets the platform daemon manages.
- appOut — Log for the thread managing buffers associated with station output, making that output visible in the Application Director view. Entries may reflect buffer size changes (available in Application Director interface), or if a problem occurs streaming the output to MultiSITE Supervisor.

Filter Settings

For any item, use the Filter Settings drop-down to select one of the following:

- Trace: Returns all message activity (verbose). This includes all transactional messages, which may result in too many messages to be useful. Be careful using Trace.
- Message: (Default) Returns informational "MESSAGE"s, plus all "ERROR" and "WARNING" types.
- Warning: Returns only "ERROR" and "WARNING" type messages (no informational "MESSAGE"s).
- Error: Returns only "ERROR" type messages (no "WARNING" or informational "MESSAGE"s).

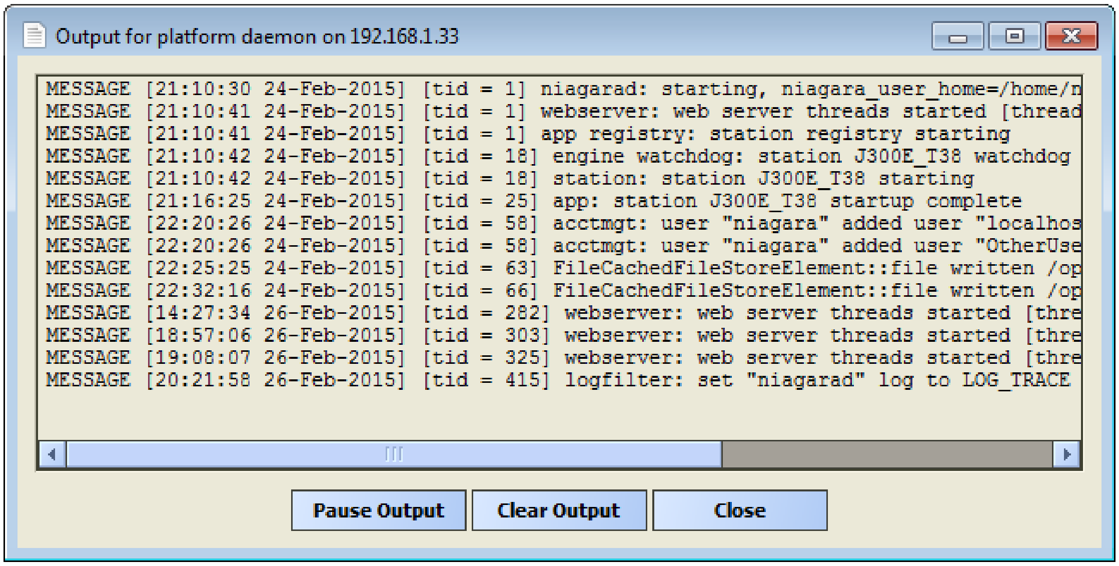
View Daemon Output

This selection from the main Platform Administration view lets you examine standard output from the host's platform daemon in real time. It is available for troubleshooting purposes.

Note:

Output is different from the output of a running station, as seen in the Application Director.

Figure 46: Example Output for platform daemon



```
MESSAGE [21:10:30 24-Feb-2015] [tid = 1] niagarad: starting, niagara_user_home=/home/n
MESSAGE [21:10:41 24-Feb-2015] [tid = 1] webserver: web server threads started [thread
MESSAGE [21:10:41 24-Feb-2015] [tid = 1] app registry: station registry starting
MESSAGE [21:10:42 24-Feb-2015] [tid = 18] engine watchdog: station J300E_T38 watchdog
MESSAGE [21:10:42 24-Feb-2015] [tid = 18] station: station J300E_T38 starting
MESSAGE [21:16:25 24-Feb-2015] [tid = 25] app: station J300E_T38 startup complete
MESSAGE [22:20:26 24-Feb-2015] [tid = 58] acctmgt: user "niagara" added user "localhos
MESSAGE [22:20:26 24-Feb-2015] [tid = 58] acctmgt: user "niagara" added user "OtherUse
MESSAGE [22:25:25 24-Feb-2015] [tid = 63] FileCachedFileStoreElement::file written /op
MESSAGE [22:32:16 24-Feb-2015] [tid = 66] FileCachedFileStoreElement::file written /op
MESSAGE [14:27:34 26-Feb-2015] [tid = 282] webserver: web server threads started [thre
MESSAGE [18:57:06 26-Feb-2015] [tid = 303] webserver: web server threads started [thre
MESSAGE [19:08:07 26-Feb-2015] [tid = 325] webserver: web server threads started [thre
MESSAGE [20:21:58 26-Feb-2015] [tid = 415] logfilter: set "niagarad" log to LOG_TRACE
```

Depending on the log filter settings set in platform administration's Daemon Output Settings window, the activity level in the output window varies. Output is non-modal, meaning that you can leave this window open and still do other MultiSITE Supervisor operations (including change output settings).

As needed, use the scroll bars to navigate through messages, which have headings "TRACE," "MESSAGE," "WARNING," or "ERROR," depending on message type. Each message includes a timestamp and a thread id number.

Use the Windows copy shortcut (Ctrl + C) to copy text of interest to the Windows clipboard.

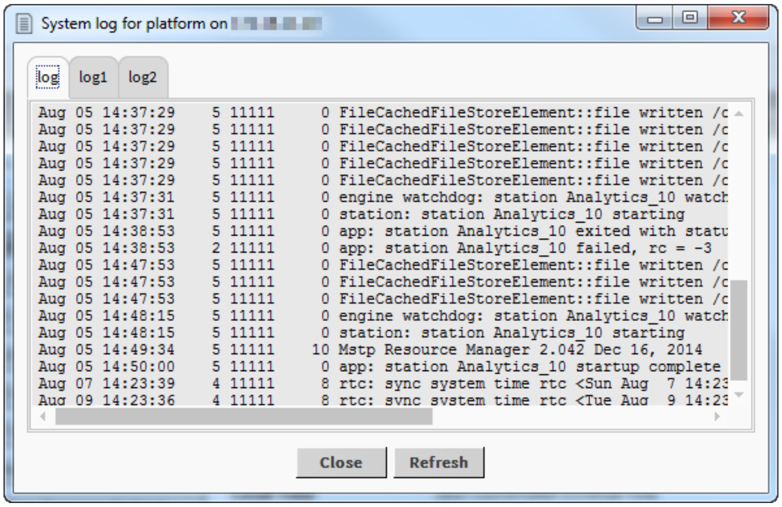
- Click Pause Output to freeze the output from updating further (no longer in real time).
- When you freeze the output, the button changes to Load Output. This means that daemon messages are still collected.
- When you click Load Output, the display loads the collected messages and continues again in real time.
- Click Clear Output to clear all collected messages from the current daemon output window. This not a destructive clear, as another (or new) daemon output window retains daemon messages.

View System Log

Starting in Niagara 4.0, this selection from the main Platform Administration view is available on Niagara 4 controllers only. In AX releases, JACE system logs were accessible only through the QNX Diagnostic Platform view (accessible via browser) or through the station platform diagnostic Spy pages. Since the station no longer provides access to platform logs, starting in Niagara 4.0 the logs are accessed directly from the controller Platform Administration view via the View System Log button. This option provides an easy and direct method for retrieving Niagara 4 system logs for diagnostic purposes.

Clicking the View System Log button launches the System log for platform <IPaddress> window, as shown below. This window contains three tabs for viewing various system logs.

Figure 47: System log for platform <IPaddress> window



System log for platform on [redacted]

```
Aug 05 14:37:29    5 11111     0 FileCachedFileStoreElement::file written /c
Aug 05 14:37:29    5 11111     0 FileCachedFileStoreElement::file written /c
Aug 05 14:37:29    5 11111     0 FileCachedFileStoreElement::file written /c
Aug 05 14:37:29    5 11111     0 FileCachedFileStoreElement::file written /c
Aug 05 14:37:29    5 11111     0 FileCachedFileStoreElement::file written /c
Aug 05 14:37:31    5 11111     0 engine watchdog: station Analytics_10 watch
Aug 05 14:37:31    5 11111     0 station: station Analytics_10 starting
Aug 05 14:38:53    5 11111     0 app: station Analytics_10 exited with statu
Aug 05 14:38:53    2 11111     0 app: station Analytics_10 failed, rc = -3
Aug 05 14:47:53    5 11111     0 FileCachedFileStoreElement::file written /c
Aug 05 14:47:53    5 11111     0 FileCachedFileStoreElement::file written /c
Aug 05 14:47:53    5 11111     0 FileCachedFileStoreElement::file written /c
Aug 05 14:48:15    5 11111     0 engine watchdog: station Analytics_10 watch
Aug 05 14:48:15    5 11111     0 station: station Analytics_10 starting
Aug 05 14:49:34    5 11111    10 Mstp Resource Manager 2.042 Dec 16, 2014
Aug 05 14:50:00    5 11111     0 app: station Analytics_10 startup complete
Aug 07 14:23:39    4 11111     8 rtc: sync system time rtc <Sun Aug  7 14:23
Aug 09 14:23:36    4 11111     8 rtc: sync system time rtc <Tue Aug  9 14:23
```

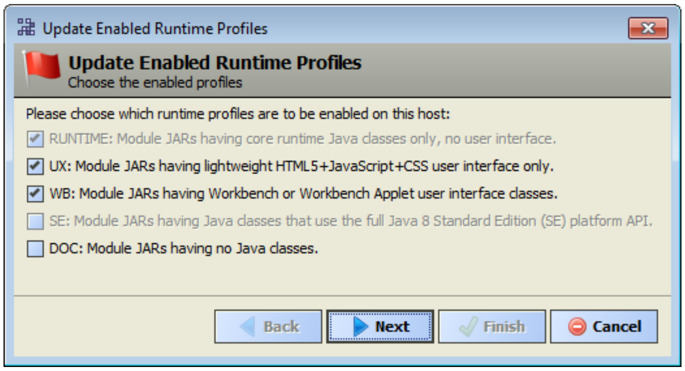
Configure Runtime Profiles

This selection from the Platform Administration view lets you globally change the runtime profile types for software modules on the connected platform. It is similar to the former module filter setting for NiagaraAX hosts, in that it affects the file space consumed by installed modules.

Note:

Typically, enabled runtime profiles are set once during initial commissioning, and then never changed.

Figure 48: Update Enabled Runtime Profiles window



Update Enabled Runtime Profiles

Update Enabled Runtime Profiles
Choose the enabled profiles

Please choose which runtime profiles are to be enabled on this host:

- ☑ RUNTIME: Module JARs having core runtime Java classes only, no user interface.
- ☑ UX: Module JARs having lightweight HTML5+JavaScript+CSS user interface only.
- ☑ WB: Module JARs having Workbench or Workbench Applet user interface classes.
- □ SE: Module JARs having Java classes that use the full Java 8 Standard Edition (SE) platform API.
- □ DOC: Module JARs having no Java classes.

The figure above shows typical settings for controllers in the initial Niagara 4 release.

- For any Windows-based host (providing it has a hard drive for file storage), you typically want all runtime profiles enabled, including DOC if it hosts MultiSITE Supervisor.
- For a JACE controller, with more limited flash-based file storage, in certain scenarios you may wish to change the enabled runtime profiles. Selection produces the window above.

Note:

For N4.0, the selection of UX automatically includes WB, and vice-versa.

Runtime profiles for modules

Software modules in Niagara 4 are distributed with a “runtime profile” type, designated by a suffix on the module’s JAR file name. In this refactoring of modules, many now often have multiple runtime profiles.

For example, the alarm module is distributed as three separate .jar files: alarm-rt, alarm-se, and alarm-wb. The runtime profile describes each JARs contents based on what systems are able to use them, where rt module JARs are a baseline among all Niagara 4 platforms.

This differs from NiagaraAX software modules, where a single module file (alarm.jar for example) holds all possible content. At installation time, AX platform tools can strip content from each JAR, based on the platform’s module content filter. In Niagara 4, each .jar file is digitally signed. This security measure ensures that the content cannot be changed at commissioning time. Therefore, Niagara 4 has more software module JARs than didNiagaraAX.

The following table lists the types of software module runtime profile types in Niagara 4. Only a very few modules do not have the –rt extension. One of those is baja.jar.

Runtime Profile	Example module name	Minimum JRE Version (1) Dependencies	Description
rt	alarm-rt	Java 8 compact3	Module JARs for data modeling and communications. These have core runtime Java classes only, with no user interface. This is the largest runtime profile group.
ux	webchart-ux	Java 8 compact3	Module JARs for BajaUX, any Java classes implementing lightweight HTML5, JavaScript, CSS user interface interaction, also theme modules.
wb	report-wb	Java 8 SE or Java 8 compact3	Module JARs with Java classes for Workbench or Workbench applet (WbApplet) user interface; views, field editors, widgets, and so on. Includes Hx and HTML5 Hx views.
se	test-se	Java 8 SE	Module JARs with Java classes that use the full Java 8 Standard Edition (SE) platform API. Currently, these can run on Windows-based hosts only.
doc	platformguidedoc	not applicable	Module JARs without Java code (classes), typically for documentation.
(1) JACE controllers use a “Java 8 compact3” compliant VM, whereas Windows-based hosts use the full Java 8 Standard Edition (SE) VM.			

Currently, the runtime profile type rt is by far the most common of Niagara 4 software JARs. An inventory of module JAR files by type in one Beta build !/modules folder (4.0.11.0) yielded counts of:

- *-rt: 378
- *-ux: 17
- *-wb: 116
- *-se: 6
- *-doc: 20

Where the majority of modules with two runtime profiles had both rt and wb, with only a few modules having three runtime profiles, as follows:

- alarm: rt, wb, se
- hierarchy: rt, ux, wb
- history: rt, ux, wb
- platCrypto: rt, se, wb
- search: rt, ux, wb
- seriesTransform: rt, ux, wb

Niagara 4 module refactoring was done for several reasons, such as the following:

- Niagara 4 software module files are digitally-signed, to improve security. This does not allow for module files to be installed with removed content during commissioning.
- To simplify dependencies between different modules.

Results from a change in enabled runtime profiles

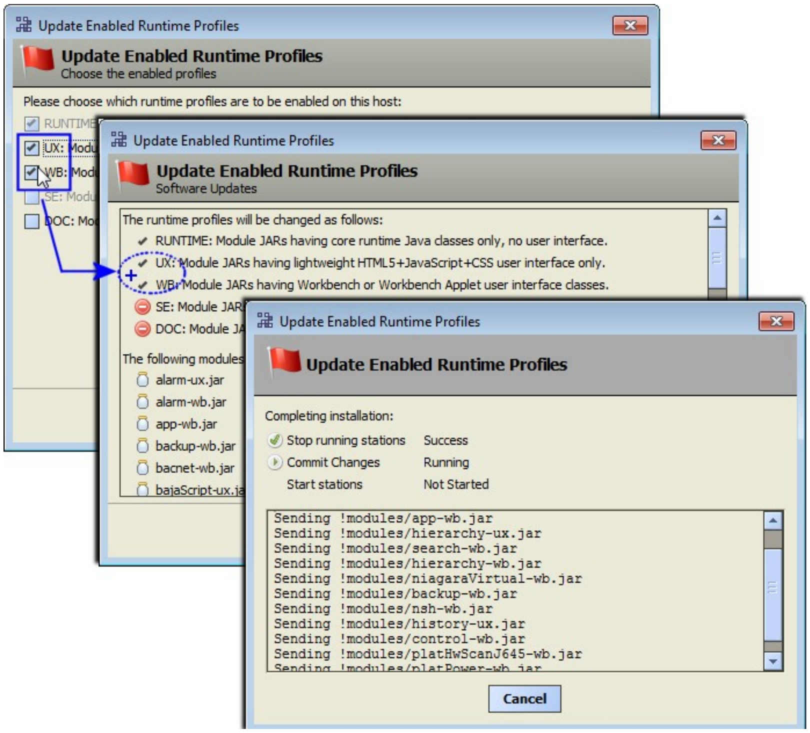
Depending on how you change enabled runtime profile, operations on the platform vary:

- If you enable additional profiles (say, go from “rt” only to “rt”, “ux” and “wb” on a controller), additional modules will need to be installed, and these are listed in a confirmation window with a Finish button. Upon confirming, any running station is stopped, the modules are installed, and the station is restarted.
- If you disable currently enabled runtime profiles (say, from “rt”, “ux” and “wb” to just “rt”) some modules will need to be uninstalled, as they are no longer supported. These modules are listed in a confirmation dialog with a Finish button. Upon confirming, any running station is stopped, the modules are uninstalled, and the station is restarted.

Note:

Niagara 4 does not permit disabling currently enabled runtime profiles to only rt” and “ux.

Figure 49: Dialog example after enabling more runtime profiles



Update Enabled Runtime Profiles

Update Enabled Runtime Profiles
Choose the enabled profiles

Please choose which runtime profiles are to be enabled on this host:

☑ RUNTIME
☑ UX: Modu
☑ WB: Mod
□ SE: Modu
□ DOC: Mo

Update Enabled Runtime Profiles

Update Enabled Runtime Profiles
Software Updates

The runtime profiles will be changed as follows:

✓ RUNTIME: Module JARs having core runtime Java classes only, no user interface.
✓ UX: Module JARs having lightweight HTML5+JavaScript+CSS user interface only.
✓ WB: Module JARs having Workbench or Workbench Applet user interface classes.
⊖ SE: Module JAR
⊖ DOC: Module JA

The following modules
alarm-ux.jar
alarm-wb.jar
app-wb.jar
backup-wb.jar
bacnet-wb.jar
bajaScript-ux.ja

Update Enabled Runtime Profiles

Update Enabled Runtime Profiles

Completing installation:

✓ Stop running stations	Success
Commit Changes	Running
Start stations	Not Started

```
Sending !modules/app-wb.jar
Sending !modules/hierarchy-ux.jar
Sending !modules/search-wb.jar
Sending !modules/hierarchy-wb.jar
Sending !modules/niagaraVirtual-wb.jar
Sending !modules/backup-wb.jar
Sending !modules/nsh-wb.jar
Sending !modules/history-ux.jar
Sending !modules/control-wb.jar
Sending !modules/platHwScanJ645-wb.jar
Sending !modules/platPower-wb.jar
```

Configure NRE Memory

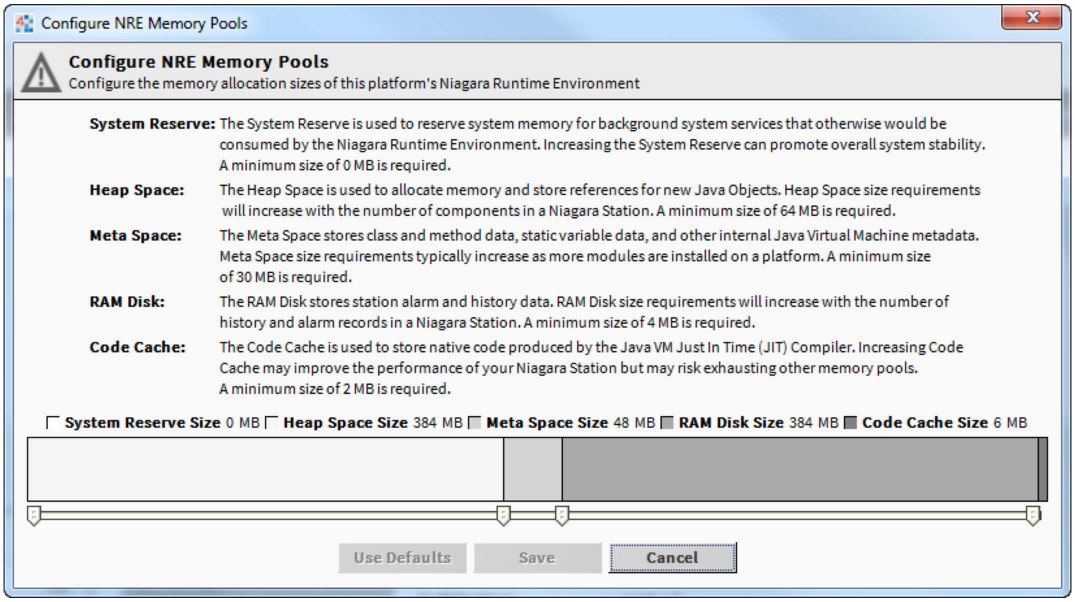
In Niagara 4.1 and later, this selection from the main Platform Administration view is available on Niagara 4 controllers only. You can use this to manually configure a controller's NRE memory pool settings to improve system performance. Depending on how the station is programmed, you may need to adjust the allocations. However, there is a fine balance between these memory pool settings. Since there is a finite amount of memory available, increasing one allocation decreases another.

In Niagara 4.2, the functionality changed slightly to include System Reserve space in the NRE memory pool settings.

Note:

- Configuring a controller with insufficient memory allocations could prevent the station from starting or could cause the station to fail and restart.

Figure 50: Configure NRE Memory Pools dialog



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 30 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.

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.

□ **System Reserve Size** 0 MB □ **Heap Space Size** 384 MB ▨ **Meta Space Size** 48 MB ▨ **RAM Disk Size** 384 MB ■ **Code Cache Size** 6 MB

The descriptions shown in the dialog include recommended allocation sizes. Additional details about the types of memory pools are described here:

- System Reserve, new in Niagara 4.2, allows you to allocate additional free operating system space. By default, this is set to 0 Mb. The reason you might reserve additional free operating system space is if additional system RAM is needed when any new thread is spawned by the station or Niagara daemon for native stack and overhead.
  Note that if you adjust the System Reserve allocation, you must restart the station for the new configuration to become effective.

- Heap Space is where the station runs. As your program grows it requires more memory (heap). Altering the Heap Space inversely affects the Meta Space. Increasing the allocation for Heap Space decreases the Meta Space.
  Note that if you adjust the Heap Space allocation, you must restart the station for the new configuration to become effective.

- Meta Space holds all of the Java classes that are loaded from the modules. As you install more drivers, this increases the number of Jar files holding the classes. So, you may need to increase the allotted Meta Space. This in turn reduces Heap Space. So you are balancing increasing the size of the station (which may require more jar files if new classes are loaded due to a driver install) and also managing the size of the Meta Space. Note that Meta Space can be increased by decreasing the allocation for either the Heap Space or the Ram Disk (or both). Altering Meta Space inversely affects the Heap space.
  Note that if you adjust the Meta Space allocation, you must reboot the controller for the new configuration to become effective.

- Ram Disk holds the histories and alarms. As a best practice, you should limit the amount of histories and alarms data held on a controller to a few days' worth of data, and archive the remainder to the supervisor. Altering Ram Disk inversely affects the Meta Space. Increasing the Ram Disk allocation decreases the allocation for Meta Space.
  Note that if you adjust the Ram Disk allocation, you must reboot the controller for the new configuration to become effective.

- Code Cache holds code that has already been compiles. Java functions with a JIT (Just-In-Time) compiler. As Java executes classes it compiles code "on the fly". Saving code that it has already compiled to the Code Cache eliminates the need to compile it again on the fly. Code that is used most often is cached. However, since there is a limited amount of memory available to cache code, it continues using the compiler as the station is running. If you adjust the memory allocation to allow a significant amount of space for code caching the station will run faster, but the risk is robbing too much memory from the Heap Space and Meta Space resulting in the station being able to run at all. Altering the Code Cache inversely affects the Ram Disk space.

Note:

If you adjust the Code Cache allocation, you must reboot the controller for the new configuration to become effective.

Backup

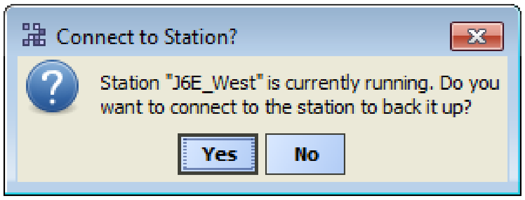
This selection from the Platform Administration view performs a complete backup of the connected controller, saved as a .dist file on your PC. The backup dist contains the entire station folder plus the specific NRE config used by platform, including license(s) and certificate(s). The dist also contains pointers to the appropriate NRE co re, Java VM, modules, and OS. If ever needed, you restore a backup dist using the platform Distribution File Installer view.

The backup dist file also contains the TCP/IP configuration of the host. When restoring the backup, you can select to restore these settings, or retain the TCP/IP settings currently in use by the target host.

You can perform a backup with a station running on the target host, or when no station is running.

- If the controller is running a station, a confirmation window opens to connect to it, as shown below.

Figure 51: Backup with station running, station connection



Connect to Station?

Station "J6E_West" is currently running. Do you want to connect to the station to back it up?

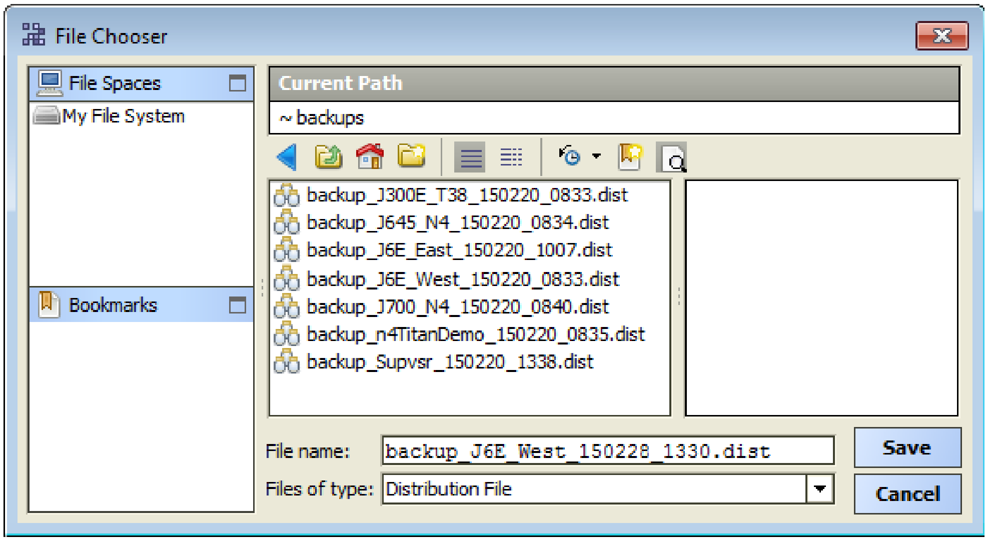
Due to our policy of continuous product innovation, some specifications may change without notification.

This routine uses that station's BackupService to perform an online backup. (If the station is not already open in MultiSITE Supervisor, you must log on as a station user.)

- If no station is running on the controller, the platform daemon performs its own offline backup.

After station logon and connection to the station (or if no station is running), the File Chooser opens, as shown below. Navigate to a target location to save the backup file, and to rename it if desired.

Figure 52: File Chooser to select target folder and dist file name



~ backups

backup_J300E_T38_150220_0833.dist
backup_J645_N4_150220_0834.dist
backup_J6E_East_150220_1007.dist
backup_J6E_West_150220_0833.dist
backup_J700_N4_150220_0840.dist
backup_n4TitanDemo_150220_0835.dist
backup_Supvsr_150220_1338.dist

File name: backup_J6E_West_150228_1330.dist

Files of type: Distribution File

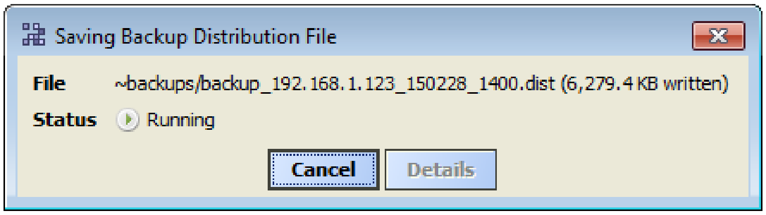
By default, the Backup function automatically creates (if not already present) a backups subdirectory under your MultiSITE Supervisor User Home. The default file name for a backup file uses a format of: backup_station-Name_YYMMDD_HHMM.dist

For example, "backup_J6E_West_180228_1330.dist" for a backup made of station "J6E_West" on February 28, 2018 at 1:30 pm.

After you click Save, the backup starts.

- If the station is running, a Fox Backup job is performed. A notification popup opens in the lower right of your display when the backup is done. This job is recorded in the station's BackupService and is visible in that component's BackupManager view. Details are also available by accessing the job in the station's Job Service Manager.
- If doing an offline backup (no station running), the platform daemon provides another progress window during the backup to a dist file, as shown below.

Figure 53: Backup from Platform Administration, no station running

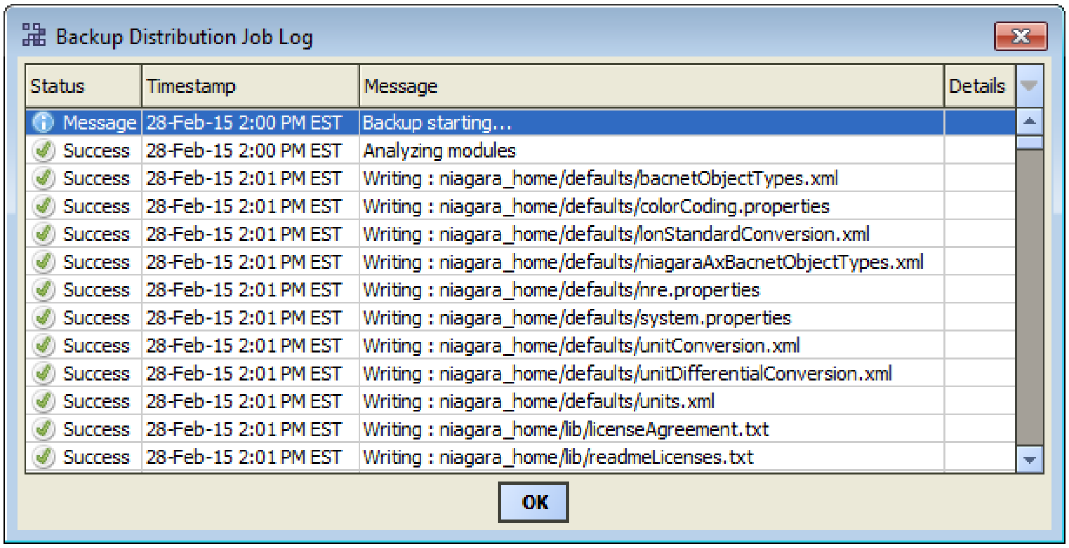


File ~backups/backup_192.168.1.123_150228_1400.dist (6,279.4 KB written)

Status Running

Upon completion, you can click Close to return to the Platform Administration view, or click Details to see another popup with a log of actions performed in the backup, as shown below.

Figure 54: Available Details from backup using platform daemon (no station running)



Backup Distribution Job Log

Status	Timestamp	Message	Details
Message	28-Feb-15 2:00 PM EST	Backup starting...	
Success	28-Feb-15 2:00 PM EST	Analyzing modules	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/bacnetObjectTypes.xml	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/colorCoding.properties	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/lonStandardConversion.xml	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/niagaraAxBacnetObjectTypes.xml	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/nre.properties	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/system.properties	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/unitConversion.xml	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/unitDifferentialConversion.xml	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/defaults/units.xml	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/lib/licenseAgreement.txt	
Success	28-Feb-15 2:01 PM EST	Writing : niagara_home/lib/readmeLicenses.txt	

Commissioning

This selection from the Platform Administration view launches the Commissioning Wizard, an ordered sequence of various platform steps.

Note:

The Commissioning Wizard is intended for a remote controller only. This button is unavailable whenever you are connected to any Windows platform.

Typically, you use the Commissioning Wizard for the following:

- The initial installation and startup of a controller.
- To upgrade a controller.

Note:

- For any AX-3.6U4 station with CryptoService that you attempt to upgrade to AX-3.8U1, once you commission the controller, the station will fail to start after the "successful" upgrade. The same is true if you attempt to move an AX-3.6U4 supervisor to an AX-3.8U1 station and start it. As a preparatory step, manually remove CryptoService from the station’s Services directory before attempting to commission it.
- Non-portable password encoding in AX-3.6 and AX-3.7 stations prevents upgrading those stations to AX-3.8 installations without first converting the passwords to a portable encoding format. Update release AX-3.8U1 provides the “plat makeportable” command, which converts such passwords to a portable format.

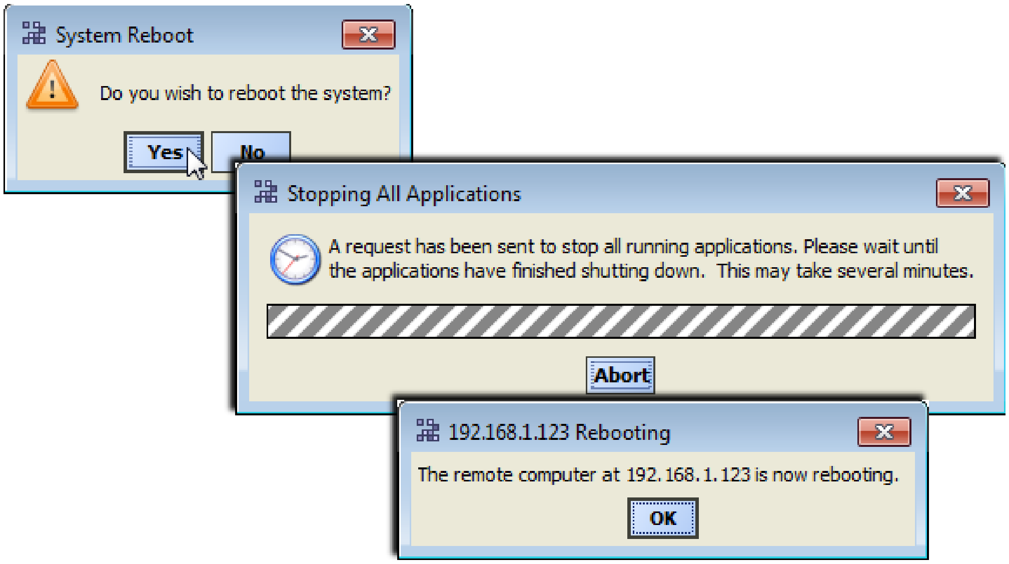
Reboot

This selection from the Platform Administration view reboots the host of a connected platform.

Note:

In Niagara 4, reboot is available only for remote platforms. Reboot is always unavailable whenever you are connected to any Windows platform, either local or remote.

Figure 55: Reboot performs operating system reboot



System Reboot

Do you wish to reboot the system?

Stopping All Applications

A request has been sent to stop all running applications. Please wait until the applications have finished shutting down. This may take several minutes.

192.168.1.123 Rebooting

The remote computer at 192.168.1.123 is now rebooting.

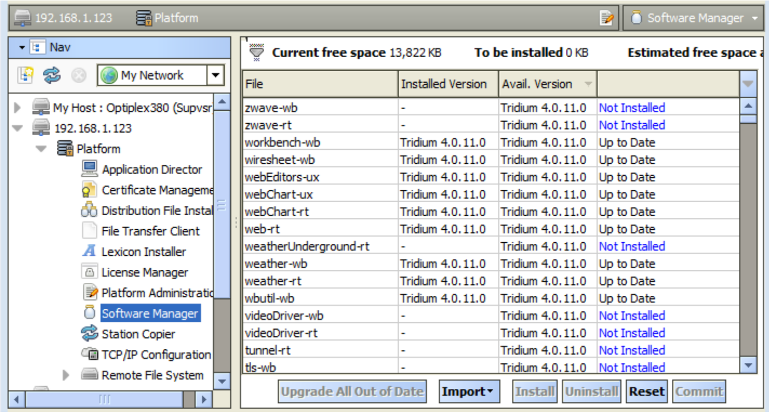
As shown above, a confirmation window opens, after which the daemon attempts to stop any running station before issuing the final reboot. A reboot restarts the QNX OS, Java VM, platform daemon, and finally the station (if it is configured to “Auto-restart”).

When the platform reboots, your MultiSITE Supervisor platform connection to it is dropped. Depending on the platform type, it may take from several seconds to a couple of minutes before you can connect again.

Software Manager

As shown in the figure below, the Software Manager is one of several platform views. This view lets you install, uninstall, or simply review all software modules installed in a remote platform. By default, this view compares the platform's modules against your locally available modules, meaning the most current modules in the software database on your PC.

Figure 56: Software Manager compares remotely installed modules to locally available modules



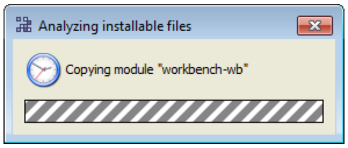
Current free space 13,822 KB **To be installed** 0 KB **Estimated free space a**

File	Installed Version	Avail. Version	
zwave-wb	-	Tridium 4.0.11.0	Not Installed
zwave-rt	-	Tridium 4.0.11.0	Not Installed
workbench-wb	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
wiresheet-wb	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
webEditors-ux	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
webChart-ux	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
webChart-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
web-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
weatherUnderground-rt	-	Tridium 4.0.11.0	Not Installed
weather-wb	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
weather-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
wbutil-wb	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
videoDriver-wb	-	Tridium 4.0.11.0	Not Installed
videoDriver-rt	-	Tridium 4.0.11.0	Not Installed
tunnel-rt	-	Tridium 4.0.11.0	Not Installed
tls-wb	-	Tridium 4.0.11.0	Not Installed

The first time you run the Software Manager, it copies modules from your Sys Home !/modules folder into a build-named subfolder in your "software database" (!/sw), for example !/sw/4.0.11.0.

Note that this can take several seconds, a popup window, similar to the one below, appears.

Figure 57: Copying modules into your software database



Copying module "workbench-wb"

Note that copying also occurs whenever you "import" software into your local software database. Then every time you access the Software Manager, it rebuilds the modules list, reflecting the latest revision of your available modules, as well modules currently installed in the opened platform.

Software Manager notes

The Niagara 4 Software Manager operates like it did in NiagaraAX, noting that Niagara 4 software module files now have separate runtime profiles. Apart from that difference, note that the following still applies:

- Only software modules are shown, versus all "installable parts" including dist files, etc. As in later releases of NiagaraAX, "standard lexicons" are distributed in Niagara 4 builds as modules, named (by convention) as niagaraLexiconLc-rt.jar (where Lc is a two-character language code).
- Module statuses of "Out of Date" and "Not Installed" can include "Requires Commissioning" too, for example "Out of Date (Requires Commissioning)". You cannot install such modules without first commissioning (upgrading) the controller, using the Commissioning Wizard.
- In some cases you can install a new module or modules without rebooting the controller, with its station kept running. This does not apply if upgrading (or downgrading) an existing module on the controller.
- If needed, you can install an earlier Niagara 4 version of a module, versus its latest "Available" version, provided earlier versions are in your MultiSITE Supervisor's software database.

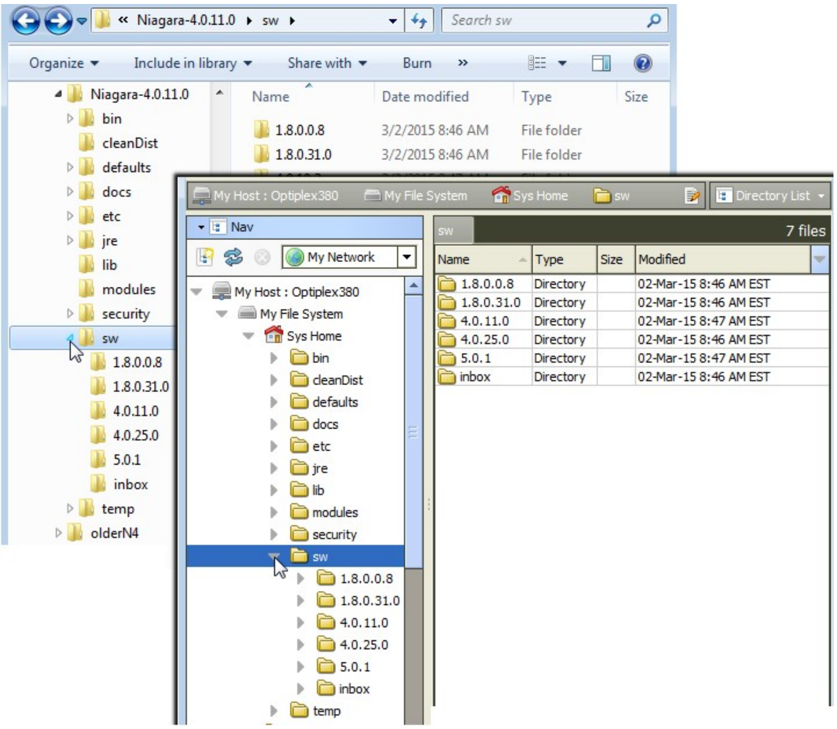
These changes are described and noted in other sections of this document, and are summarized here only to assist if you are already familiar with previous MultiSITE Supervisor versions.

About your software database

The software database for your MultiSITE Supervisor is located under the Sys Home sw subdirectory. If MultiSITE Supervisor was installed using the use as an installation tool option, this directory contains several subdirectories for various distribution (.dist) files, with each subdirectory named using version numbers.

You can see your sw subdirectory structure using either Windows Explorer, or in the MultiSITE Supervisor Nav tree, My File System, Sys Home as shown below.

Figure 58: Software database (everything under sw)



Name	Date modified	Type	Size
1.8.0.0.8	3/2/2015 8:46 AM	File folder	
1.8.0.31.0	3/2/2015 8:46 AM	File folder	

sw 7 files

Name	Type	Size	Modified
1.8.0.0.8	Directory		02-Mar-15 8:46 AM EST
1.8.0.31.0	Directory		02-Mar-15 8:46 AM EST
4.0.11.0	Directory		02-Mar-15 8:47 AM EST
4.0.25.0	Directory		02-Mar-15 8:46 AM EST
5.0.1	Directory		02-Mar-15 8:47 AM EST
inbox	Directory		02-Mar-15 8:46 AM EST

Note:

Numbers of subdirectories and version number names in your sw subdirectories will be different; this is only a simple example.

⊘ Do not manually create or rename subdirectories in this area for proper operation. Instead, let the Software Manager automatically administer this database.

For example, in the Niagara 4.0 installation (4.0.11.0), shown above, the software database has several versioned subdirectories, which are described in this example as follows:

- 1.8.0.0.8: Reflects the version of dist files for the Oracle Java 8 “compact3” JRE for JACE controllers (2 files, one for PPC processor JACE controllers, one for ARM processor JACE-8000).
- 1.8.0.31.0: Reflects the version of dist files for the Oracle Java 8 “Standard Edition” JRE for Windows platforms (2 files, one for 64-bit Windows, one for 32-bit Windows).
- 4.0.11.0: Reflects the current Niagara release, by build number. This contains numerous Niagara nre “config” and “core” dist files, installed by the “installation tool” MultiSITE Supervisor installation option. Also, after the Software Manager is first used, the contents of the build’s modules directory (module .jars) are automatically copied here too.
- 4.0.25.0: Reflects version of dist files for QNX operating system for controllers, with four different dist files.
- 5.0.1: Reflects a version of a few “prototype” MultiSITE Supervisor help modules.

- inbox: Provides a means for you to copy any installable file here, and have the Software Manager automatically create a proper "versioned" subdirectory for it. Or, if the correct subdirectory already exists, the Software Manager will copy the inbox file(s) there.

As an equivalent to the inbox feature, you can use the Import button at the bottom of the Software Manager to add to your software database. For details, see the "Software Import" section.

When you add different-versioned installable files, the number of different subdirectories under your sw directory will continue to increase. By default, the Software Manager displays only the most recent version of any module as the Avail. Version.

Note:

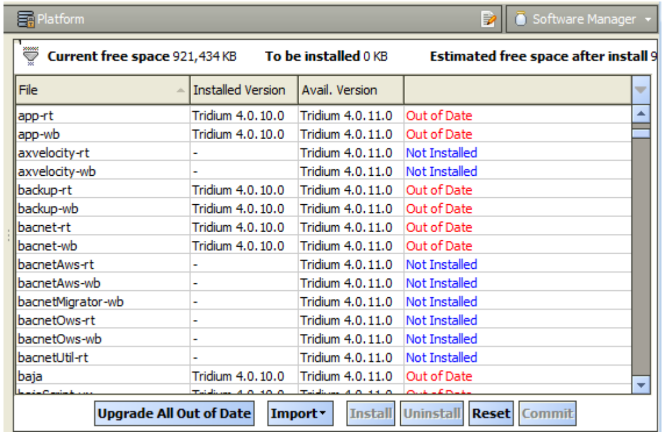
You can select to install an older version of any module listed in the Software Manager, if available in your software database. See the section "Right-click option to install earlier version".

Note that older software files (modules, dists) are also useful in your software database when restoring a backup dist for a JACE, if the backup was made using a previous software release. You use the platform Distribution File Installer to restore a backup.

Default module listing and layout

By default, the Software Manager lists all the JACE's out-of-date modules at the top of the table, and then the uninstalled modules, and lastly the up-to-date modules (sorted alphabetically). See the figure below.

Figure 59: Software Manager default listing



Current free space 921,434 KB **To be installed** 0 KB **Estimated free space after install** 9

File	Installed Version	Avail. Version	
app-rt	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date
app-wb	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date
axvelocity-rt	-	Tridium 4.0.11.0	Not Installed
axvelocity-wb	-	Tridium 4.0.11.0	Not Installed
backup-rt	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date
backup-wb	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date
bacnet-rt	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date
bacnet-wb	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date
bacnetAws-rt	-	Tridium 4.0.11.0	Not Installed
bacnetAws-wb	-	Tridium 4.0.11.0	Not Installed
bacnetMigrator-wb	-	Tridium 4.0.11.0	Not Installed
bacnetOws-rt	-	Tridium 4.0.11.0	Not Installed
bacnetOws-wb	-	Tridium 4.0.11.0	Not Installed
bacnetUtil-rt	-	Tridium 4.0.11.0	Not Installed
baja	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date

- Out of Date modules are older than what you have in your PC software database.
- Not Installed modules do not exist on the platform, but are in your PC software database.
- Up to Date modules are the same (or possibly newer) than that in your PC software database.

Note:

Both "out of date" and "not installed" modules may also show a "Requires Commissioning" status. This indicates you must upgrade the JACE first, before installing that module version. As needed, you can scroll down the table or click on headers of table columns to resort alphabetically.

Software Manager table columns

The Software Manager lists modules using four columns, from left-to-right, labeled as follows:

- File — File name of locally available module file, or blank if the module is on the remote host only.
- Installed Version — Version of the module installed in the remote host, or blank if not installed.
- Avail. Version — Latest version of locally available module, or blank if the software is on the remote host only.
- <unlabeled> — Status of the module in the remote JACE platform. For each module, status is one of the following:
  - Not Installed — Module is not in remote platform, but is available locally. Blue text is used for this status.
  - Not Installed (Requires Commissioning) — Module is not in remote platform, but is available locally. Blue text is also used for this status.

Dependencies prevent you from installing it, unless you first upgrade the JACE, using the Commissioning Wizard.

  - Up to Date — Module is installed in the remote platform, and is equal to (or higher) than locally available module version.
  - Out of Date — Module is installed in remote platform, and is older than your local version. Red text is used for this status.
  - Out of Date (Requires Commissioning) — Module is installed in remote platform, and is older than your local version shown. Red text is also used for this status.

Dependencies prevent you from installing it, unless you first upgrade the JACE, using the Commissioning Wizard.

  - Not Available Locally — Module installed in remote platform is not in your software database.
  - Cannot Install — Local module is unreadable or has a bad manifest; you cannot install it.
  - Bad Target — Remotely installed module is unreadable or has a bad manifest, and is therefore unusable by a station. Software in this state should probably be fixed, since it could cause the station to not work correctly.
  - Downgrade to <version> — Remotely installed software is intended to be replaced with a module having a lower version.
  - Install <version> — Module is intended to be installed; it does not currently exist on the remote platform.
  - Re-Install <version> — Remotely installed module is intended to be replaced with a module having a the same version.
  - Uninstall <version> — Remotely installed module is intended to be uninstalled.
  - Upgrade to <version> — Remotely installed module is intended to be replaced with a module having a higher version.

Note:

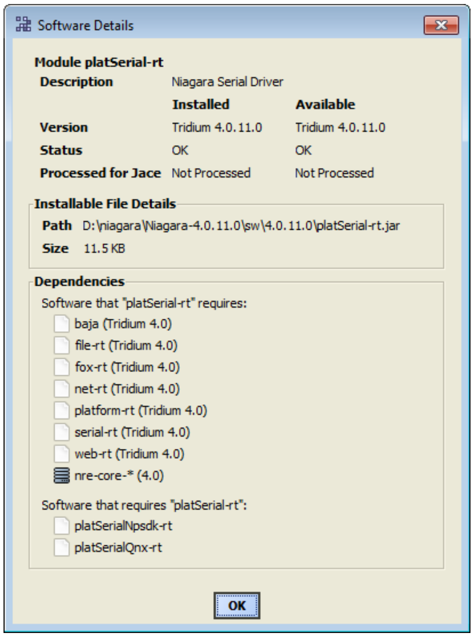
“Intended” status values like “Install <version>” reflect un-committed actions made during your Software Manager session. Blue text is used to list these statuses.

You can also view software details about any item in the table. In addition, you can filter (reduce) the number of software items listed, based on text included in file name or the software’s status values. See “Filtering displayed software” for more details.

Software Details

From the Software Manager, double-click any module to see a popup dialog with details.

Figure 60: Software Details dialog from Software Manager



Software Details

Module platSerial-rt

Description	Niagara Serial Driver	
	Installed	**Available**
Version	Tridium 4.0.11.0	Tridium 4.0.11.0
Status	OK	OK
Processed for Jace	Not Processed	Not Processed

Installable File Details

Path D:\niagara\Niagara-4.0.11.0\sw\4.0.11.0\platSerial-rt.jar

Size 11.5 KB

Dependencies

Software that "platSerial-rt" requires:

- baja (Tridium 4.0)
- file-rt (Tridium 4.0)
- fox-rt (Tridium 4.0)
- net-rt (Tridium 4.0)
- platform-rt (Tridium 4.0)
- serial-rt (Tridium 4.0)
- web-rt (Tridium 4.0)
- nre-core-* (4.0)

Software that requires "platSerial-rt":

- platSerialNpsdk-rt
- platSerialQnx-rt

Details include a brief module description, comparisons between installed and available module, module file and size, and whatever module dependencies exist, by part names. Dependencies are listed for both cases: what software is required by this module, plus software that is dependent on this module.

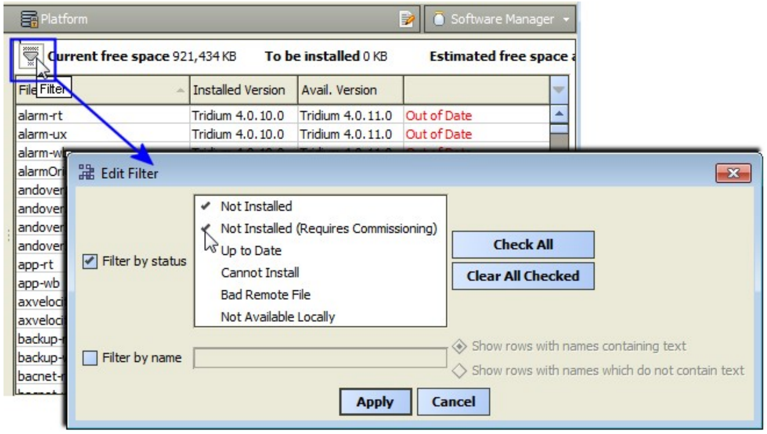
Note:

Essentially, dependency details are for information only. When installing modules from the Software Manager, all dependent modules are automatically included when you select a module to install.

Filtering displayed software

By default, the Software Manager lists all remotely installed and locally available modules, which can produce a very large table. A filter control provides an Edit Filter dialog, in which you select items for listing, thereby filtering undesired items. See the following figure.

Figure 61: Filter control and dialog to limit displayed modules



File	Installed Version	Avail. Version	
alarm-rt	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date
alarm-ux	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date

☑ Filter by status

- ✓ Not Installed
- ✓ Not Installed (Requires Commissioning)
- Up to Date
- Cannot Install
- Bad Remote File
- Not Available Locally

□ Filter by name

◇ Show rows with names containing text

◇ Show rows with names which do not contain text

You can use either “Filter by status” or “Filter by name”, or a combination of the two.

Filter by status

Modules with an “Out of Date” or “Out of Date (Requires Commissioning)” status always appear in the Software Manager. Modules with any with uncommitted (intended) status values, such as “Install,” “Uninstall,” and so on, also appear.

When you enable filter by status, you can check other statuses to include (or clear to omit) the listing of associated items in the table, as follows:

- Not Installed — Modules on your PC that can be installed, but are not in the remote platform.
- Not Installed (Requires Commissioning) — Modules on your PC, but not in the remote platform. The remote JACE must be upgraded (using Commissioning Wizard) first.
- Up to Date — Modules on your PC and in the remote platform, where the software is not older.
- Cannot Install — Local module is unreadable or has bad manifest, you cannot install it.
- Bad File — Remote module is unreadable or has bad manifest.

Note:

With status filtering enabled, you can also simply “check all” and “clear all checked.”

- If all status items are cleared, only “Out of Date” and uncommitted status modules appear.
- If all status items are checked, the display is similar to disabled status filtering, except “non-module” items are not listed.

Filter by name

Name filtering lets you include or exclude items based on character string portion of module File name. When enabled (checked), you can type in a string of characters, and then check one of the following:

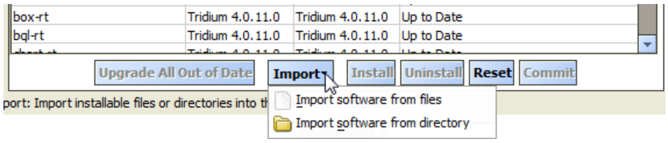
- Show rows with names containing text: Only items with file name containing this string.
- Show rows with names which do not contain text: Only items with file name that does not contain this string.

This feature can be useful to filter many modules with common name characters, for example “lon” or “doc” part-named modules.

Software Import

As shown below, an Import button at the bottom of the Software Manager provides two menu choices for you to add new (or earlier) installable software files (module .jars, .dists) in your software database. See the next section, “Import vs. copy into modules”.

Figure 62: Import choices to bring in file(s) or entire folders



box-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
bql-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date

port: Import installable files or directories into th

The two import options are the following:

- Import software from files: This produces the standard File Chooser dialog, in which you navigate to the proper location and select one or more software files for import.
- Import software from directory: This produces the standard Directory Chooser dialog, in which you navigate to the proper location and select a directory, for inclusion of any contained software files. For example, you might do this for an earlier installed software build, selecting its “sw” folder, or a portion thereof.

Upon import, the software list is again rebuilt by the Software Manager (popup dialogs appear while software files are copied). Afterwards, any modules that are newer-versioned, or that did not previously exist, will now be represented by default in the software table.

If imported modules are earlier versions, they are also available for installation in the Software Manager. See the section, “Right-click option to install earlier version” for more details.

Import vs. copy into modules

When receiving updated or new module jar files, you have two basic options when copying them to your MultiSITE Supervisor PC, as follows:

1. Copy directly into your !/modules directory. This makes the module(s) available in your MultiSITE Supervisor environment, and also available to install in other remote platforms (when the installer runs, the module(s) are also copied into your software database, available for installation). This is the typical choice.

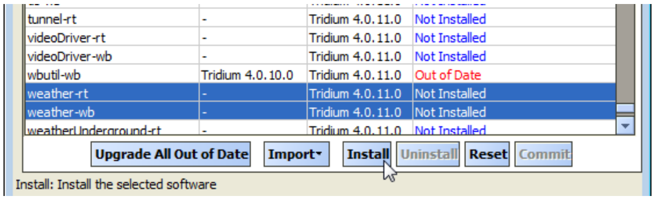
2. Copy into your !/sw/inbox directory (or, use the equivalent software Import option in the Software Manager). In this case, the module(s) are not used in your MultiSITE Supervisor environment, but are available in your software database for installation in remote platforms.

This would be the choice where you want to keep using a newer (or older) version of the received module (s) in your MultiSITE Supervisor environment. A scenario that is applicable here is that if you received older versions of modules, perhaps needed to restore an older backup dist file in a certain remote platform.

Software actions

As needed, from the Software Manager you can take actions on modules, such as install, uninstall, upgrade, downgrade, and re-install. You flag intended actions on software items using action buttons near the bottom of the Manager's view pane, as shown below. Action buttons become enabled when you have one or more items selected.

Figure 63: Software Manager action buttons



tunnel-rt	-	Tridium 4.0.11.0	Not Installed
videoDriver-rt	-	Tridium 4.0.11.0	Not Installed
videoDriver-wb	-	Tridium 4.0.11.0	Not Installed
wbutil-wb	Tridium 4.0.10.0	Tridium 4.0.11.0	Out of Date
weather-rt	-	Tridium 4.0.11.0	Not Installed
weather-wb	-	Tridium 4.0.11.0	Not Installed
weatherUnderground-rt	-	Tridium 4.0.11.0	Not Installed

Install: Install the selected software

Reset button

When you reset, all flagged module changes (since the last commit) are cleared.

Commit button

Use this button to actually launch the flagged changes.

When you choose Commit, one of these two things happens:

- If upgrading (or downgrading) modules, a confirmation popup dialog appears, telling you the station must be stopped and the host rebooted. After the software operation completes, the host is rebooted.

Note:

Before committing, make sure that controlled equipment that might be adversely affected by the JACE's station stopping and then host rebooting (from software changes) is put in a manually controlled state.

- In many cases, if only installing new module(s), meaning modules not previously installed, the station continues running on that platform. The software is immediately installed.

Upgrading out-of-date modules

Whenever one or more local modules are newer than in the modules in an opened platform, the Software Manager enables an Upgrade All Out of Date button. This allows you to flag all out-of-date modules to be upgraded. Unlike other action buttons, specific item(s) do not need selection first.

The platform is configured and running.

Step 1 Open a secure platform connection to a target controller.

Step 2 Expand the Platform container in the Nav tree and double-click the Software Manager container.

The Software Manager compares the modules on the Supervisor platform with the modules in each open platform. If a module on the Supervisor side is newer than its equivalent on the controller side, the Software Manager enables the Upgrade All Out of Date button.

Step 3 Click the Upgrade All Out of Date button.

The status of all out-of-date modules changes to Upgrade to version, where version is the latest version available.

Due to our policy of continuous product innovation, some specifications may change without notification

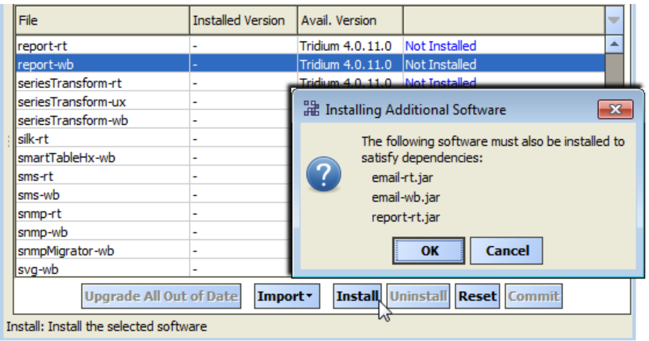
Install button

This button is available in the Software Manager when you have one or more modules selected with a status of "Not Installed." When you click it, the status of the selected modules changes to "Install <version>," and if selected again, the button changes to Cancel Install.

Note:

If a selected module has dependencies on modules not already installed (or also flagged to install), a dialog appears explaining additional software is needed, as shown below. After you click OK from this dialog, the additional modules are flagged, the status of all affected modules changes to "Install <version>".

Figure 64: Installing Additional Software dialog



File	Installed Version	Avail. Version	
report-rt	-	Tridium 4.0.11.0	Not Installed
report-wb	-	Tridium 4.0.11.0	Not Installed
seriesTransform-rt	-	Tridium 4.0.11.0	Not Installed
seriesTransform-ux	-		
seriesTransform-wb	-		
silk-rt	-		
smartTableHx-wb	-		
sms-rt	-		
sms-wb	-		
snmp-rt	-		
snmp-wb	-		
snmpMigrator-wb	-		
svg-wb	-		

Installing Additional Software

The following software must also be installed to satisfy dependencies:

email-rt.jar
email-wb.jar
report-rt.jar

Install: Install the selected software

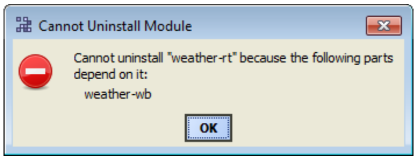
Uninstall button

This button is available in the Software Manager when you have one or more installed modules selected (status of either "Up to Date" or "Out of Date"). If the selected module(s) are not dependencies of other installed modules, when you click Uninstall, the module(s) status changes to "Uninstall <version>," and the button changes to Cancel Uninstall.

Note:

If other installed modules have dependencies on one or more modules you selected, a dialog appears explaining that the uninstallation cannot occur, as shown below. You can then decide if you want to reflag another uninstall, selecting also all modules that are dependent.

Figure 65: Cannot Uninstall dialog



Cannot Uninstall Module

Cannot uninstall "weather-rt" because the following parts depend on it:

weather-wb

Re-Install/Upgrade/Downgrade button

In the Software Manager, when you have one or more installed software items selected, the "Install" button changes to show one of these options.

- Re-Install appears if the installed item is the same version as your locally available one.
- Upgrade appears if the installed item is an earlier version than your locally available one.
- Downgrade appears if the installed item is a newer version than your locally available one.

When you click this button, the software's status correspondingly changes to either "Re-Install <version>", "Upgrade <version>", or "Downgrade <version>", and the button changes to Cancel <action>, for example: Cancel Re-Install.

Commit and Reset button

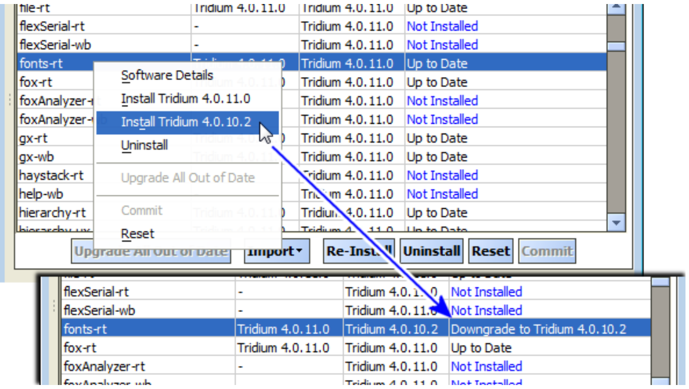
In the Software Manager, when you have one or more pending actions in place on software items, the Commit button is available. This is how you initiate the software action.

At any time before you commit, you can also click the Reset button. This removes all pending actions in place on software items, and makes the Commit button unavailable again.

Right-click option to install earlier version

In addition to button-based software actions in the Software Manager, you can also select an earlier version of a module to install, providing one is in your local software database.

Figure 66: Right-click option to install earlier module version in Software Manager



file-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
flexSerial-rt	-	Tridium 4.0.11.0	Not Installed
flexSerial-wb	-	Tridium 4.0.11.0	Not Installed
fonts-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
fox-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
foxAnalyzer-r	[illegible]	Tridium 4.0.11.0	Not Installed
foxAnalyzer-w	[illegible]	Tridium 4.0.11.0	Not Installed
gx-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
gx-wb	Tridium 4.0.11	Tridium 4.0.11.0	Up to Date
haystack-rt	[illegible]	Tridium 4.0.11.0	Not Installed
help-wb	[illegible]	Tridium 4.0.11.0	Not Installed
hierarchy-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date

flexSerial-rt	-	Tridium 4.0.11.0	Not Installed
flexSerial-wb	-	Tridium 4.0.11.0	Not Installed
fonts-rt	Tridium 4.0.11.0	Tridium 4.0.10.2	Downgrade to Tridium 4.0.10.2
fox-rt	Tridium 4.0.11.0	Tridium 4.0.11.0	Up to Date
foxAnalyzer-rt	-	Tridium 4.0.11.0	Not Installed

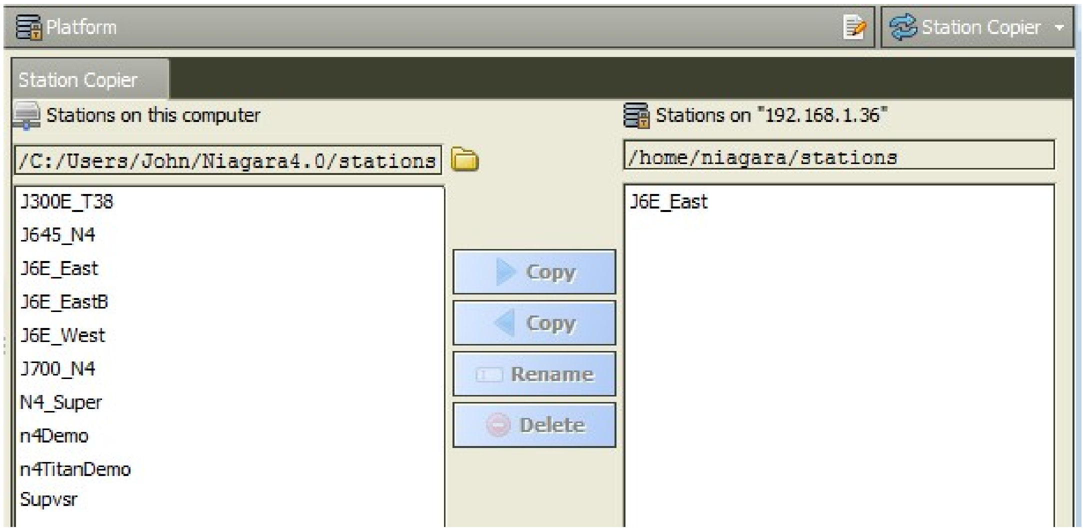
Simply right-click a module row, and from the shortcut menu select any Install vendor 4.n.nn items as shown here. Note if downgrading to an earlier module, a host reboot/station restart will result after you commit.

Station Copier

The Station Copier is one of several platform views. You use it to install a station in any Niagara 4 platform (remote or local), as well as make a copy in your User Home of any running station (remote or local). You can also use Station Copier to rename and delete stations, either locally or remotely.

You see this view even when opening a local platform connection at your Supervisor computer as well as when opening a remote Niagara host. The following figure shows the Station Copier in a platform connection to a controller.

Figure 67: Example Station Copier view for remote platform



/C:/Users/John/Niagara4.0/stations

J300E_T38
J645_N4
J6E_East
J6E_EastB
J6E_West
J700_N4
N4_Super
n4Demo
n4TitanDemo
Supvsr

/home/niagara/stations

J6E_East

As shown above, the Station Copier view is split into two main areas:

- Stations on your MultiSITE Supervisor PC, typically your User Home (left)
- Station in the daemon User Home of the opened platform (right)

By default, content of your User Home station's folder is shown on the left side. If you have station folders located elsewhere, click the folder icon for a Change Directory window, and point the Station Copier there. That changed location is used the next time you access the Station Copier.

Installing a station

Station installation usually involves copying an existing station from a MultiSITE Supervisor user home to a target controller platform. The procedure uses the Station Transfer Wizard.

Prerequisites: The following conditions must be met:

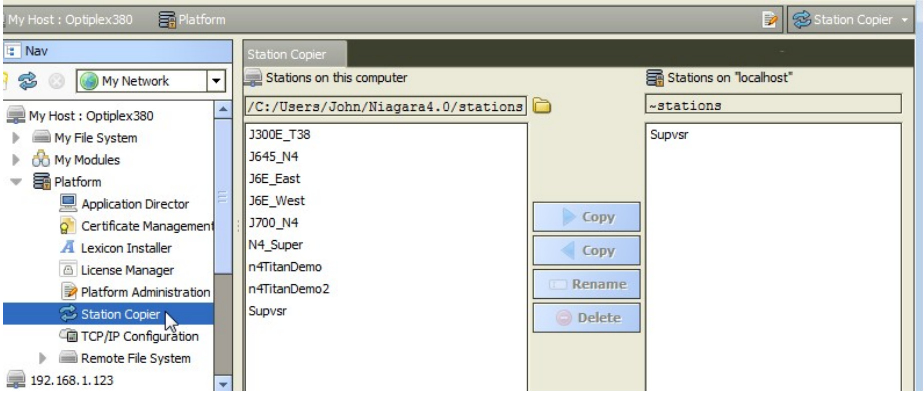
- All hardware (PC or controller) has been installed and connected.
- The controller has been commissioned and network communication configured.
- The station you wish to install exists in a MultiSITE Supervisor user home.
- You are prepared to answer the Station Transfer Wizard questions.

This topic is part of configuring a station for the first time or upgrading a station from a previous version of Niagara. The Station Copier is a platform service.

Step 1 Open a secure platform connection to the target controller, the one on which you wish to install the station.

Step 2 Expand the Platform container in the Nav tree and double-click the System Copier.

Figure 68: Example Station Copier view at local Supervisor host



Step 3 On the left side (MultiSITE Supervisor user home), select the station and click the Copy button that points to the right side of the window.

The Station Copier displays “Loading module information” and, if all needed modules are available, launches the Station Transfer Wizard.

If any module needed by the station has a dependency that requires the controller (platform) to be commissioned (commissioning upgrades core software or the operating system), the station installation stops immediately, displays a message, and provides the option to start the Commissioning Wizard instead. The need to commission a controller arises if you are installing a brand new controller or upgrading a controller from NiagaraAX to Niagara 4.0 and forgot to run the Commissioning Wizard.

Step 4 Follow the wizard prompts clicking Next or Back as necessary.

If the station is running, the wizard informs that it will stop and restart the station.

Step 5 Review all the changes you selected and click Finish.

The wizard displays installation progress in the Transferring station window.

Step 6 To complete the operation, click Close.

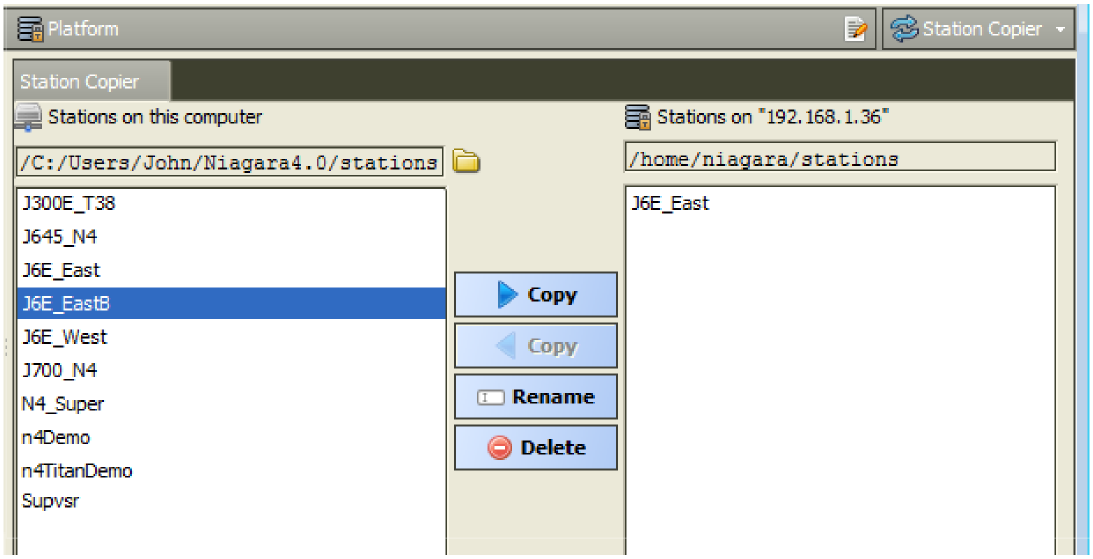
The Station Copier prompts you to open the Application Director now.

Step 7 To view the station log, click Yes.

Station copy direction

The copier works in either direction. In other words, click a station on one side (to copy to the other side). When you click a station, the station is selected (highlighted) and the appropriate Copy button, by direction, becomes enabled to clarify the source and target. See the figure below.

Figure 69: Copy direction by station side selection



/C:/Users/John/Niagara4.0/stations

- J300E_T38
- J645_N4
- J6E_East
- J6E_EastB
- J6E_West
- J700_N4
- N4_Super
- n4Demo
- n4TitanDemo
- Supvsr

/home/niagara/stations

- J6E_East

To perform the following station operations, do the following:

- Click on the left side for a copy from MultiSITE Supervisor User Home-to-daemon User Home.

Do this to install a station in a JACE.

- Click in right side for a copy from daemon User Home-to-MultiSITE Supervisor User Home.

Do this to make a local backup copy of a station, saved to your MultiSITE Supervisor computer.

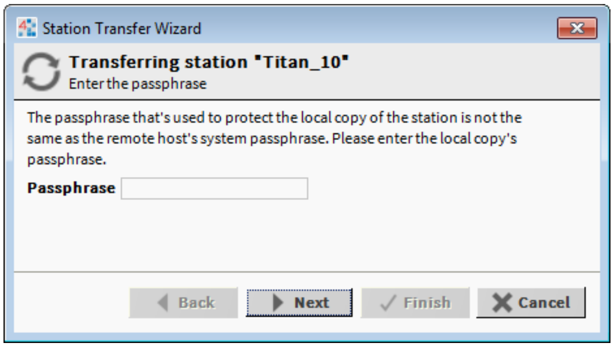
When you click Copy, the Station Transfer Wizard appears and guides you through the steps of the station transfer process.

Station Copier Passphrase check

When you click Copy, the Station Transfer Wizard attempts to validate the Bog file's passphrase with the target host's system passphrase. If they are the same, then it guides you through the rest of the station transfer process.

If the passphrase for the bog file is not the same as the passphrase for the target host platform then you are prompted to enter the bog file's passphrase, as shown below.

Figure 70: Station Transfer Wizard prompt for bog file passphrase



The passphrase that's used to protect the local copy of the station is not the same as the remote host's system passphrase. Please enter the local copy's passphrase.

Passphrase

The above dialog is prompting you to enter the bog file's passphrase.

If a BOG file is protected with an unknown passphrase, you can use the MultiSITE Supervisor toolbar icon to Unlock (force-remove) the passphrase, making the file unprotected, or "force-change" the passphrase to enter a new value. Choosing either of these options clears any sensitive data in the file.

Note:

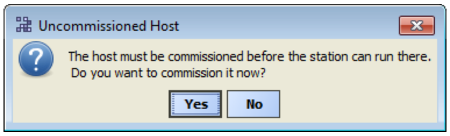
When you Unlock (force-remove) or Change (force-change) the passphrase on a Bog file, it results in the loss of the sensitive data in the file.

Station Copier dependencies check

The Station Copier checks, whenever installing a station, to determine if the target JACE platform does not already have all modules installed that are required by that station. Such dependencies may prevent the installation of a selected station. Changes are summarized as follows:

If any module needed by the station has a dependency that requires the JACE to be commissioned (upgrade core Niagara software or QNX OS), the station install immediately stops, upon station selection. Steps in the Station Transfer Wizard do not appear. A dialog explains that the JACE needs commissioning, and provides the option to start the Commissioning Wizard, as shown in the figure below.

Figure 71: Selected station cannot be installed without first commissioning the JACE.



The host must be commissioned before the station can run there.
Do you want to commission it now?

Click Yes to start the Commissioning Wizard, or No to simply return to the Station Copier.

This may occur if are trying to install a station in a new, uncommissioned JACE-8000, or in another JACE controller that has been converted from AX to N4, but still not yet commissioned.

If all modules needed by the station are found on your PC, the Station Transfer Wizard starts normally. However, upon reaching the "Modules step", in some cases you may see a caution. For further details see the "Modules step" section.

Station Transfer Wizard

This wizard assists with any station copy (installing or backing up) by presenting a number of steps. The exact steps vary by the direction of copy, as well your selections in wizard step dialogs. In each step, click Next to advance to the next step. As needed, click Back to return to a previous step and make changes, or click Cancel to exit from the wizard (no station copy performed).

Note:

Use Cancel if you need to make a different selection to copy; this reruns the wizard.

The wizard's Finish button is enabled only in the final step. When you click Finish, the related operations begin, and you see progress updates in the Transferring Station dialog. When complete, click Close in the dialog to exit the wizard.

Note:

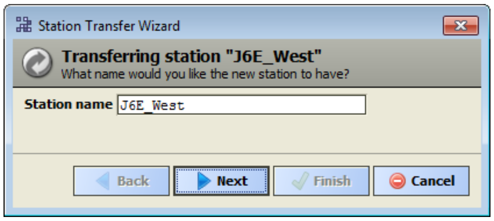
In the unlikely case where the source station config.bog file is currently in use ("locked"), the wizard opens in a state where you must Cancel to exit (no other steps are given).

- If installing a station, the source config.bog is locked if it contains unsaved changes (it is being edited elsewhere in MultiSITE Supervisor). After saving changes, you can try to copy again.
- If backing up a station, the source config.bog is locked if currently in process of being saved. You can retry the copy later.

Name step

The first step in the Station Transfer Wizard is to confirm the name (or type a new name) for the copied station directory.

Figure 72: Station Transfer Wizard dialog, name step



Station Transfer Wizard

Transferring station "J6E_West"

What name would you like the new station to have?

Station name J6E_West

Default name is the station directory being copied. If you rename the station, it will be identical to the source (copied) station in every way except name of its station directory.

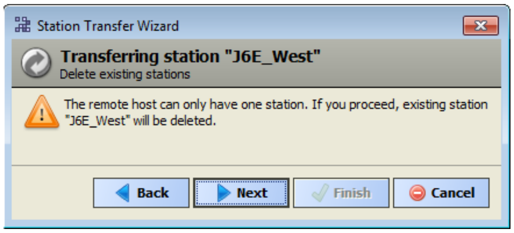
Delete step

This step is skipped for any station backup, or if a station install in either of these cases:

- No existing station exists on the target.
- The existing station is named the same as the one you are installing.

This step occurs because all JACE platforms have a support limit of one (1) installed station. The delete step simply cautions you that the existing station will be deleted. See the figure below.

Figure 73: Station Transfer Wizard dialog, delete step



Station Transfer Wizard

Transferring station "J6E_West"
Delete existing stations

The remote host can only have one station. If you proceed, existing station "J6E_West" will be deleted.

Note:

The entire remote station directory (all subdirectories and files) is deleted when the station install starts. If unsure, it may be best to Cancel, and then backup the remote JACE station first.

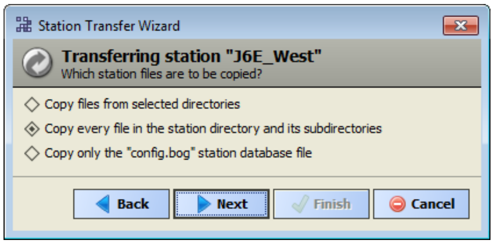
The next step is the “Content step”.

Content step

Note that this wizard step is skipped if the source station consists of only a config.bog file.

After the “name step” and possibly “delete step”, the wizard asks you to select what station files to copy, with the default selection being “all” files and folders under that station directory. See the figure below.

Figure 74: Station Transfer Wizard dialog, content step



Station Transfer Wizard

Transferring station "J6E_West"
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

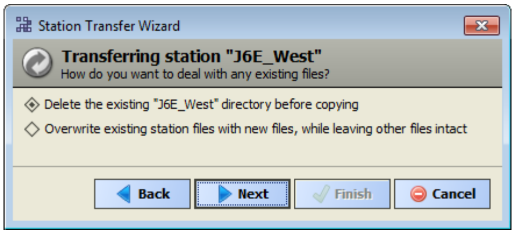
The three possible selections are:

- Copy files from selected directories (not shown if source station has no subdirectories). If you select this, a later “Details step” allows you to select the source subdirectories.
- Copy every file in the station directory and its subdirectories.
- Copy only the “config.bog” station database file. The next step is the “Disposition step”.

Disposition step

Note that this wizard step occurs only when an identically-named target station already exists. If the target station already exists, a disposition step asks what is to be done with it, as shown below.

Figure 75: Station Transfer Wizard dialog, disposition step



Station Transfer Wizard

Transferring station "J6E_West"
How do you want to deal with any existing files?

◆ Delete the existing "J6E_West" directory before copying
◇ Overwrite existing station files with new files, while leaving other files intact

The two possible selections are:

- Delete existing station directory before copying.
- Overwrite existing station files with new files, while leaving other files intact.

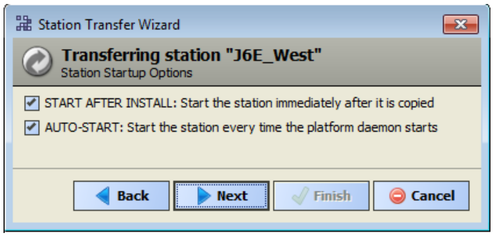
If you previously selected “copy everything” from the “Content step”, the default pre-selection is the first (delete existing station directory). Otherwise, the second selection (overwrite) is pre-selected.

The next step is the “Station settings step”.

Station settings step

Note that this wizard step is skipped for any station backup. This step specifies the station’s Auto-Start setting.

Figure 76: Station Transfer Wizard dialog, station settings



Station Transfer Wizard

Transferring station "J6E_West"
Station Startup Options

☑ START AFTER INSTALL: Start the station immediately after it is copied
☑ AUTO-START: Start the station every time the platform daemon starts

Two items are listed:

- START AFTER INSTALL: Start the station immediately after it is copied.
- AUTO-START: Start the station every time the platform daemon starts.

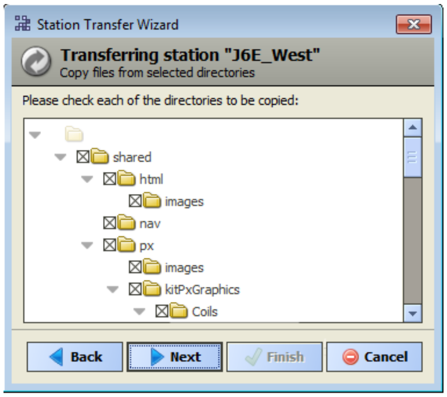
Auto-start is one of two station settings for any station, as specified in the Application Director view by using “start checkboxes”. See the section “Application and output controls”.

Typically, you enable both settings and go to the next step, either the “Details step” or the “Modules step”.

Details step

Note that this wizard step is skipped for any station backup, as well as for a station install, unless you selected “copy selected directories” in the “Content step”.

Figure 77: Station Transfer Wizard dialog, details step



Station Transfer Wizard

Transferring station "J6E_West"

Copy files from selected directories

Please check each of the directories to be copied:

-
  - ☒ shared
    - ☒ html
      - ☒ images
    - ☒ nav
    - ☒ px
      - ☒ images
      - ☒ kitPxGraphics
        - ☒ Coils

As shown above, this step provides a tree to select station subdirectories (folders) to include in the copy. By default, all selectable folders are both expanded and selected, while unselectable folders are not. Note that if present, a station’s alarm and history folders are not selectable. For any selectable folder, click to toggle it as either selected (with X) or unselected (no X).

Modules step

This wizard step is skipped if a station backup, or if all modules required by the station to be installed are already in the JACE controller. In this case, you see either the “Stop station step” or “Review step” instead.

This step occurs if the target platform is missing one or more of the modules required by the station being copied (installed). It lists the missing modules/versions that will be installed during the station copy operation. If included, this is the final step before the station copy process starts.

Note:

Dependencies of the missing modules are compared against the software that is already installed in the target platform. The Station Copier looks for versions of those missing modules in your User Home software database that can be installed without re-commissioning the target platform, by default.

There are two possible results when the wizard reaches this step:

- Station can be installed with most current modules
- Station can be installed with “out of date” modules

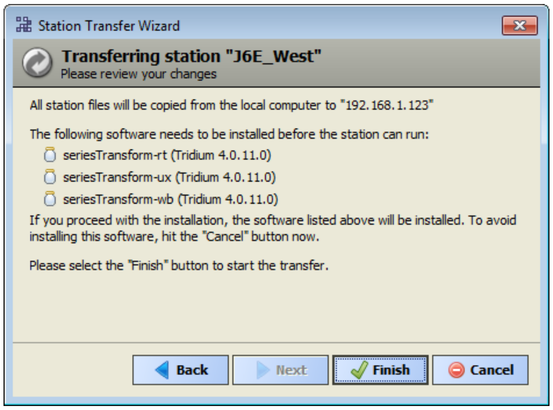
In either case, to continue, you click either of the following:

- Finish — Start the local-to-remote copy, including installation of the listed modules. Progress updates appear in a “Transferring station” dialog.
- Cancel — Exit from the Station Transfer Wizard, then either select another station to install, or if a JACE upgrade is possible (and you have purchased an upgrade license for it) run the Commissioning Wizard to upgrade the controller, including the installation of a station.

Station can be installed with most current modules

If all missing modules can be installed using the most current versions, they are listed without any warning, as shown below.

Figure 78: Station install example, all missing modules are most current versions



Transferring station "J6E_West"
Please review your changes

All station files will be copied from the local computer to "192.168.1.123"

The following software needs to be installed before the station can run:

- seriesTransform-rt (Tridium 4.0.11.0)
- seriesTransform-ux (Tridium 4.0.11.0)
- seriesTransform-wb (Tridium 4.0.11.0)

If you proceed with the installation, the software listed above will be installed. To avoid installing this software, hit the "Cancel" button now.

Please select the "Finish" button to start the transfer.

Station can be installed with “out of date” modules

If any module to be installed is not the most current version, you have the option to cancel the station install. A dialog explains that you can use the Commissioning Wizard to upgrade the JACE.

This may occur at a later time, after a “point release” such as N4.1, where you have previously imported the software database of an N4.0 installation.

For related details, see the following topics: “About your software database”, “Software Import”, and Upgrading a controller.

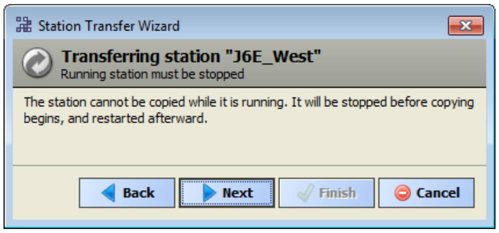
Stop station step

You can see this wizard step in any of these scenarios:

- You are copying the station running in a remote platform to your local computer, and you selected either “copy files from selected directories” or “copy only the config.bog station database file” in the previous “Content step”. Note that this step is skipped if you elect to “copy every file in the station directory and its subdirectories”. However, a station save occurs before the station copy transfer starts.
- If installing a “same-named” station.

This step reminds you that the station must be stopped while it is copied, as shown below.

Figure 79: Station Transfer Wizard dialog, stop station step



Transferring station "J6E_West"
Running station must be stopped

The station cannot be copied while it is running. It will be stopped before copying begins, and restarted afterward.

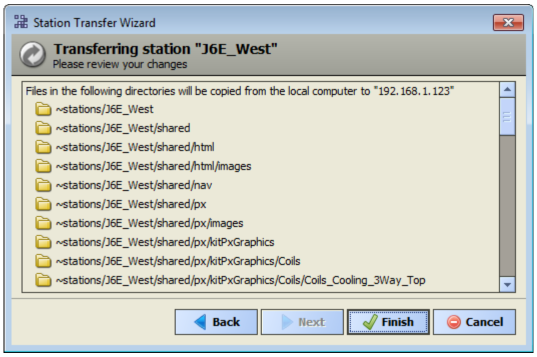
Click Next to go to the “Review step”.

Review step

Note that this wizard step is skipped when installing a station where additional modules are required. Instead, the “Modules step” provides the Finish button.

This step provides a summary of choices from previous steps, and a Finish button to begin the station copy process.

Figure 66 Station Transfer Wizard dialog, review step



Station Transfer Wizard

Transferring station "J6E_West"
Please review your changes

Files in the following directories will be copied from the local computer to "192.168.1.123"

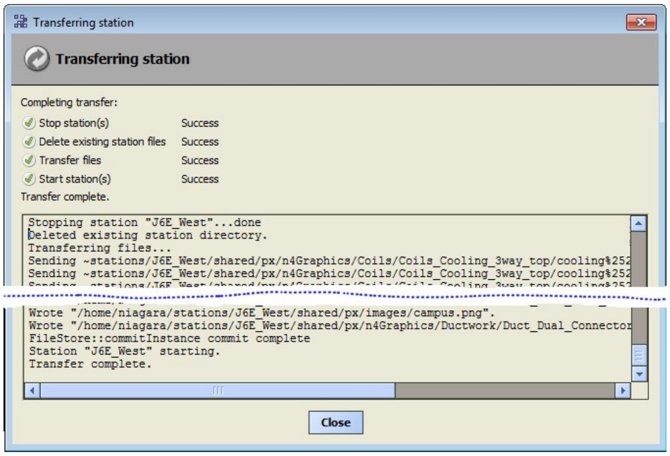
- ~stations/J6E_West
- ~stations/J6E_West/shared
- ~stations/J6E_West/shared/html
- ~stations/J6E_West/shared/html/images
- ~stations/J6E_West/shared/nav
- ~stations/J6E_West/shared/px
- ~stations/J6E_West/shared/px/images
- ~stations/J6E_West/shared/px/kitPxGraphics
- ~stations/J6E_West/shared/px/kitPxGraphics/Coils
- ~stations/J6E_West/shared/px/kitPxGraphics/Coils/Coils_Cooling_3Way_Top

As shown above, if you selected only specific station subdirectories to copy (from the “Details step”), they are listed. If needed, click Back to make changes, or click Finish to begin the copy process and observe progress in the “Transferring station” dialog.

Transferring station

After clicking Finish in the “Modules step” or “Review step” of the Station Transfer Wizard, the station copy process begins and updates appear in this dialog, as shown below.

Figure 80: Station Transfer Wizard, Transferring station (copy) process



Transferring station

Transferring station

Completing transfer:

✓ Stop station(s)	Success
✓ Delete existing station files	Success
✓ Transfer files	Success
✓ Start station(s)	Success

Transfer complete.

```
Stopping station "J6E_West"...done
Deleted existing station directory.
Transferring files...
Sending ~stations/J6E_West/shared/px/n4Graphics/Coils/Coils_Cooling_3way_top/cooling%252
Sending ~stations/J6E_West/shared/px/n4Graphics/Coils/Coils_Cooling_3way_top/cooling%252
Wrote "/home/niagara/stations/J6E_West/shared/px/images/campus.png".
Wrote "/home/niagara/stations/J6E_West/shared/px/n4Graphics/Ductwork/Duct_Dual_Connector
FileStore::commitInstance commit complete
Station "J6E_West" starting.
Transfer complete.
```

Depending on the type of copy, the following operations may be included in this process:

- If installing a station (copy from User Home-to-daemon User Home):
  - Stop all stations — whenever modules must be installed.
  - Stop one station — any JACE where same station is being reinstalled.
  - Delete station(s) — if you chose to delete station in the “Disposition step”, or if a station needs to be deleted to stay under maximum number of stations (only one for any JACE platform)
  - Transfer files — includes station and module files (actual copy portion).

  - Start station — if a station had to be stopped (module installation), or if you chose to start the station in the "Station settings step".
- If backing up a station (copy from daemon User Home-to-local User Home):
  - Save station — whenever remote station is currently running.
  - Transfer files — includes station files (actual copy portion).

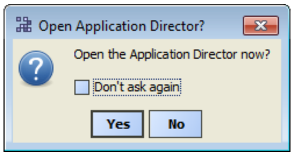
Note:

A popup explaining that the existing station must be saved (if a backup) or stopped (if installing) may appear for a few seconds. Following, and during execution of the various operations, a Cancel button is available. If you click Cancel before all operations complete, the installation (or backup) is not valid.

After all operations are finished, a Close button is available and the last update in the dialog is "Transfer complete." Click Close to exit the wizard.

By default, after installing a station, the wizard exits with a popup asking if you wish to switch to the Application Director platform view.

Figure 81: Switch to Application Director popup


Open Application Director?
Open the Application Director now?
□ Don't ask again
Yes
No

Note:

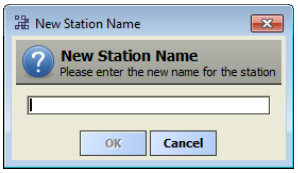
Since it is a good idea to observe a station's output upon first startup, it is recommended that you select Yes. To automatically switch to the Application Director after installing a station, click the checkbox "Don't ask again" before selecting Yes. Then, you will not see this popup again.

Renaming stations

The Station Copier lets you rename any station, either in your User Home (left side) or in the opened platform's daemon User Home (right side).

As shown below, a Rename dialog appears when you select a station and click Rename.

Figure 82: Rename station dialog

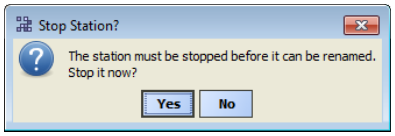


Note:

Be careful when renaming stations, as there is no undo. Furthermore, please note the following:

- Any running station that is renamed must first be stopped. A confirmation popup dialog informs you of this after you enter the new station name and click OK.

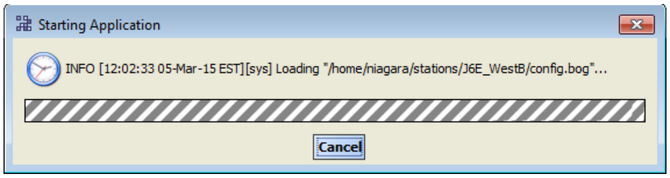
Figure 83: Rename station warning



The station must be stopped before it can be renamed. Stop it now?

After the station stops, it becomes renamed, and then it automatically restarts. A series of other dialogs appear, each showing a station startup message.

Figure 84: Rename station, starting application dialog



INFO [12:02:33 05-Mar-15 EST] [sys] Loading "/home/niagara/stations/J6E_WestB/config.bog"...

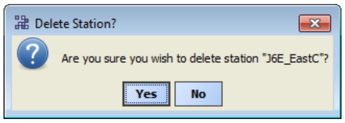
- If a renamed running station is already included in the NiagaraNetwork of other stations, its corresponding NiagaraStation component will remain "down" until renamed to match the new name. Therefore, all child components (Niagara proxy points and so on) will also be down until this is done. In addition, other unforeseen consequences may result from changing the name of a station that has already been integrated into other stations.

Therefore, station renames are best done on your User Home (left side) stations, or when initially configuring a job site network, such as when first installing (copying) a station.

Deleting stations

The Station Copier lets you delete any station, either in your User Home (left side) or in the opened platform's daemon User Home (right side).

Figure 85: Confirm delete station dialog



Are you sure you wish to delete station "J6E_EastC"?

As shown above, a confirmation dialog appears when you select a station and click Delete.

Note:

Be careful when deleting stations, as there is no undo. Furthermore, note the following:

- The entire selected station directory gets deleted, including all subdirectories and file contents.
- Special notification does not occur if you choose to delete a running station (you may briefly see a "stop station" popup, with opportunity to Abort).
- Also in general (as a precaution), before deleting a running station, it is generally recommended to make a backup copy first. If desired, when backing up, you can rename it using some "temp" convention to flag it for later housekeeping.

Station installation troubleshooting and FAQs

Following are some frequently asked questions and answers about the Station Copier that may help in troubleshooting.

Q: I started the Station Copier, selected the station and clicked Copy, and got a message prompting me to enter a file passphrase.

A: The bog file’s passphrase is not the same as the target host’s system passphrase. You must enter the correct file passphrase to proceed with the station copy. An alternative is to edit the bog file offline to either unlock the file, making it unprotected, or to change the passphrase value. However, either of these choices will clear any sensitive information in the file.

Q: I started the Station Copier, entered the station name and got a message indicating that the controller requires commissioning.

A: The controller may be new or you may be upgrading from NiagaraAX to Niagara 4.0 and you forgot to commission the platform first. Run the Commissioning Wizard and come back to the Station Copier later.

Q: I started the Station Copier, selected the station to copy and clicked Next, but the only option available is to Cancel and exit the wizard.

A: The station database (config.bog) is locked. This happens if:

- The config.bog has been edited elsewhere in MultiSITE Supervisor and contains unsaved changes. After saving changes, try the copy again.
- The system is in the process of saving the config.bog using the BackupService. Wait a while and try the copy again.

TCP/IP Configuration

TCP/IP Configuration is one of several platform views. Typically, you use it to initially configure a remote controller's TCP/IP settings.

Note:

If connected to any Windows-based platform, all settings in this view are read-only. You typically use the Windows Control Panel for making these changes on a PC.

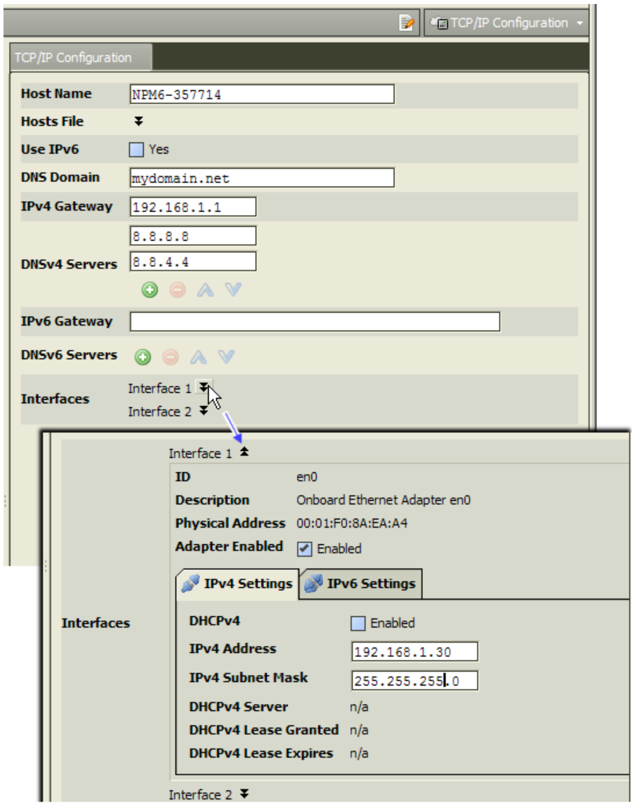
Configuring TCP/IP communication settings is a task for the systems integrator when initially setting up a controller.

Prerequisites:

Step 1 Open a secure connection to the platform.

Step 2 Expand the Platform container in the Nav tree and double-click the TCP/IP Configuration container.

Figure 86: TCP/IP Configuration container.



Host Name	NPM6-357714
Hosts File	
Use IPv6	□ Yes
DNS Domain	mydomain.net
IPv4 Gateway	192.168.1.1
DNSv4 Servers	8.8.8.8 8.8.4.4
IPv6 Gateway	
DNSv6 Servers	
Interfaces	Interface 1 Interface 2

Interface 1

ID	en0
Description	Onboard Ethernet Adapter en0
Physical Address	00:01:F0:8A:EA:A4
Adapter Enabled	☑ Enabled

DHCPv4	□ Enabled
IPv4 Address	192.168.1.30
IPv4 Subnet Mask	255.255.255.0
DHCPv4 Server	n/a
DHCPv4 Lease Granted	n/a
DHCPv4 Lease Expires	n/a

Interface 2

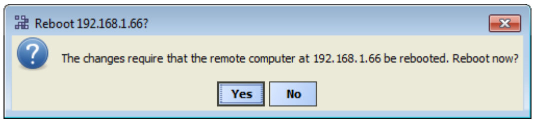
The system displays the main TCP/IP properties.

Step 3 Click the drop-down arrows to expand a group of properties. To save yourself time when making multiple changes, enter all changes before you continue.

Step 4 When you finish the configuration, click Save.

The system displays a Reboot dialog.

Figure 87: Reboot dialog



Reboot 192.168.1.66?

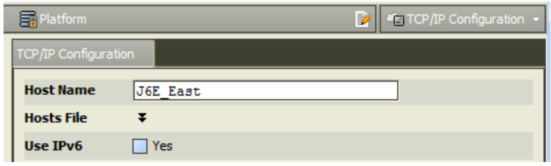
The changes require that the remote computer at 192.168.1.66 be rebooted. Reboot now?

Step 5 Reboot the controller for the changes to take effect.

TCP/IP Host fields

The top of the TCP/IP Configuration view provides the platform's TCP/IP host settings.

Figure 88: Hosts fields on platform TCP/IP Configuration view



Host Name J6E_East

Hosts File

Use IPv6 □ Yes

These available host fields are as follows:

- Host Name

Synonymous with "computer name," this is a string that can be processed by a DNS server to resolve to an IP address. On Windows-based systems, this hostname is the computer's identification in its workgroup or domain. If using hostnames, each Niagara platform should have a unique hostname.

- Hosts File

The hosts file is a standard TCP/IP hosts file, where each line associates a specific IP address with a known hostname. To review, click the expand control to see all entries.

For a JACE controller, you can edit its host file.

  - To add an entry, click at the end of the last line and press Enter. Then type the IP address, at least one space, then the known hostname.
  - To delete an entry, drag to highlight the entire line, and then press Backspace.

Click the expand control again to collapse the Hosts File editor.

- Use IPv6

Default is No (unchecked). If set to Yes (checked), Niagara (platform daemon and station) respond to IPv6 requests, that is, it creates IPv6 server sockets (daemon) and IPv6 fox multicast sockets.

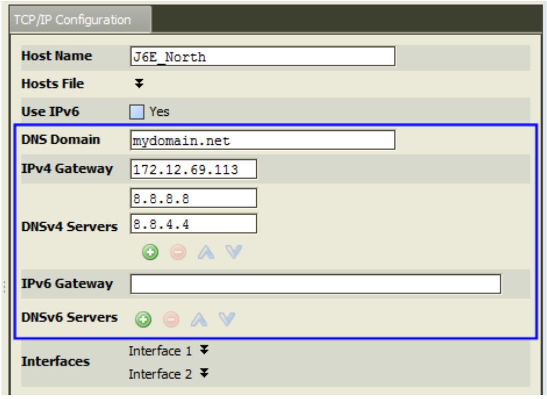
TCP/IP DNS fields

If connected to a JACE controller, the DNS and gateway settings are also "host-level" parameters in the TCP/IP Configuration view, as shown below.

Note:

For a Windows-based host, DNS and gateway settings are available under each Interface section.

Figure 89: Host-level fields for any JACE controller includes DNS and gateway



TCP/IP Configuration

Host Name	J6E_North
Hosts File	
Use IPv6	□ Yes
DNS Domain	mydomain.net
IPv4 Gateway	172.12.69.113
DNSv4 Servers	8.8.8.8 8.8.4.4
IPv6 Gateway	
DNSv6 Servers	
Interfaces	Interface 1 Interface 2

The available fields for JACE controllers are listed below:

- DNS Domain: The TCP/IP Domain Name System (DNS) domain this host belongs to, if used.
- IPv4 Gateway: The IP address of the router that forwards packets to other IPv4 networks or subnets. A valid gateway address is required in multi-station (JACE) jobs to allow point discoveries under NiagaraNetworks.
- DNSv4 Servers: The IP address of one or more DNS servers (if available), where each can automate associations between hostnames and IPv4 addresses. Included are icon-buttons to Add (to enter IP address of server), Delete, and move Up/Down (to set the DNS search order).
- IPv6 Gateway: The IPv6 address for the router that forwards packets to other IPv6 networks or subnets.
- DNSv6 Servers: The IPv6 address for one or more IPv6 DNS servers (if available), where each can automate associations between hostnames and IPv6 addresses. Included are icon-buttons to Add (to enter IP address of server), Delete, and move Up/Down (to set the DNS search order).

TCP/IP Interface fields

For each Ethernet port on the connected platform, the TCP/IP Configuration platform view provides an expandable Interface section.

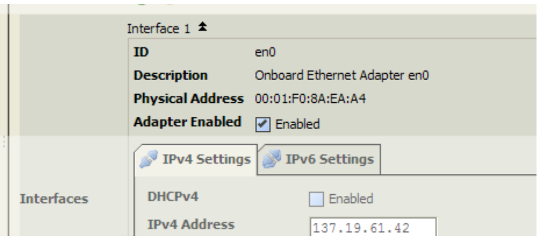
All compatible JACE controllers have two Ethernet ports: LAN1 and LAN2. In the TCP/IP Configuration view, they are listed as Interface 1 (en0) and Interface 2 (en1).

Note:

A JACE-8000 controller includes an onboard "WiFi" adapter. If enabled, it appears in the TCP/IP Configuration view with multiple Interface selections. Only one mode below can be enabled, according to the WiFi switch position on the controller.

- tiw_sap — (Titan wireless supplicant Access Point configuration)
- tiw_sta — (Titan wireless supplicant Client mode configuration)

Figure 90: TCP/IP Interface fields, top properties



Interface 1

ID en0

Description Onboard Ethernet Adapter en0

Physical Address 00:01:F0:8A:EA:A4

Adapter Enabled ☑ Enabled

DHCPv4 □ Enabled

IPv4 Address 137.19.61.42

As shown above, each Interface has the following properties at the top:

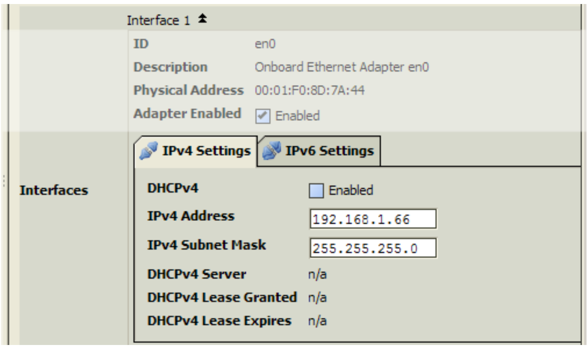
- ID: A read-only OS identifier for the hardware interface, such as "en0" if a JACE controller, or if a Windows platform, either a 128-bit GUID (globally unique identifier) or a Windows network connection name, such as "Local Area Connection 2".
- Description: A read-only text string such as "Onboard Ethernet Adapter en0" for a JACE controller, or "Intel(R) PRO/100 VE Network Connection" for a Win32-based host, describing a NIC model.
- Physical Address: The unique 48-bit MAC address of the Ethernet adapter, in six two-hexadecimal digits. For example, for the "en0" Interface 1 port of a JACE controller: 00:01:F0:80:13:E6
- Adapter Enabled: Checkbox to specify whether the Ethernet port is usable.

Below the properties above, each Interface has two separate tabs, as follows (each with properties):

- IPv4 Settings
- IPv6 Settings

IPv4 Settings

Figure 91: IPv4 tab for Interface of JACE controller, in platform TCP/IP Configuration view



Interface 1

ID: en0
Description: Onboard Ethernet Adapter en0
Physical Address: 00:01:F0:8D:7A:44
Adapter Enabled: ☑ Enabled

Interfaces

IPv4 Settings | IPv6 Settings

DHCPv4: □ Enabled
IPv4 Address: 192.168.1.66
IPv4 Subnet Mask: 255.255.255.0
DHCPv4 Server: n/a
DHCPv4 Lease Granted: n/a
DHCPv4 Lease Expires: n/a

The following properties are on the IPv4 Settings tab of the selected Interface:

- DHCPv4: A checkbox to specify DHCP (Dynamic Host Configuration Protocol) instead of static IP addressing. Successful use requires a DHCP server installed on your network. If enabled, other interface fields such as IP Address and Subnet Mask become read-only, as these are assigned by the DHCP server after the platform reboots.

Note that only ONE adapter of any JACE controller may have DHCP enabled.

In general (for stability), static IP addressing is recommended over DHCP. If configuring for DHCP, it is recommended that you reserve a specific, fixed IP address for this JACE host in the network's DHCP server/ router configuration, noting the MAC address of this adapter as shown above.

Note:

⊘ Do not enable DHCP unless sure that your network has one or more DHCP servers. Otherwise, the JACE may become unreachable over the network.

- DNS Domain: (Windows hosts only) The TCP/IP Domain Name System (DNS) domain the host belongs to, if used.
- IPv4 Address: The "static" IP address for this host, unique on your network.

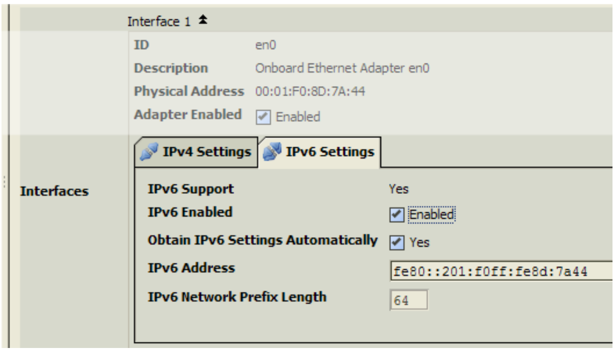
Be careful to understand the following:

- – If enabling multiple ports, note that IP address must be on different subnets, otherwise the ports will not function correctly. For example, with a typical "Class C" subnet mask of 255.255.255.0, setting Interface 1=192.168.1.99 and Interface 2=192.168.1.188 is an invalid configuration, as both addresses are on the same subnet.
- – A JACE controller does not provide IP routing or bridging operation between different Interfaces (LAN ports, GPRS, dialup, WiFi).

- IPv4 Gateway: (Windows hosts only) IP address for the device that forwards packets to other networks or subnets.
- IPv4 Subnet Mask: The "static" IP subnet mask used by this host.
- DHCPv4 Server: Applies only if DCHP is enabled. Shows read-only address of the DHCP server from which this host last obtained its IP address settings.
- DHCPv4 Lease Granted: Applies only if DCHP is enabled. Shows a read-only timestamp of when the DHCP lease started.
- DHCPv4 Lease Expires: Applies only if DCHP is enabled. Shows a read-only timestamp of when the DHCP lease will expire, and will need renewal.
- DNSv4 Servers (DNS Servers): (Windows hosts only) The IP address for one or more DNS servers, each of which can automate associations between hostnames and IP addresses. Included are icon-buttons to Add (to enter IP address of server), Delete, and move Up/Down (to set the DNS search order).

IPv6 Settings

Figure 92: IPv6 tab for Interface of JACE controller, in platform TCP/IP Configuration view



Interface 1

ID en0

Description Onboard Ethernet Adapter en0

Physical Address 00:01:F0:8D:7A:44

Adapter Enabled ☑ Enabled

Interfaces

IPv6 Support Yes

IPv6 Enabled ☑ Enabled

Obtain IPv6 Settings Automatically ☑ Yes

IPv6 Address fe80::201:f0ff:fe8d:7a44

IPv6 Network Prefix Length 64

The following properties are on the IPv6 Settings tab of the selected Interface:

- IPv6 Support: Yes or No, as read-only. Indicates if host platform's OS supports IPv6.
- IPv6 Enabled: Checkbox for Enabled, where default is cleared (disabled). If a Windows host, this indicates if it is configured with the IPv6 protocol.
- Obtain IPv6 Settings Automatically: Checkbox for Enabled (default). Provides for "auto-configuration" of IPv6 address, if acceptable. If enabled on a JACE controller, the next two properties are read-only. If cleared, the two properties below must be entered manually.
- IPv6 Address: The host's IP address in IPv6 format, to be unique on its network.
- IPv6 Network Prefix Length: The number of left-most contiguous bits of the IPv6 address (in decimal) that compose the subnet prefix.
- DNSv6 Servers: (Windows hosts only, providing host's OS has IPv6 enabled) Read-only IPv6 address for one or more DNS servers, each of which can automate associations between hostnames and IPv6 addresses.

Provisioning as a way to automate platform tasks

This document focuses on the platform user interface, that is, the different platform views and functions available when you (a MultiSITE Supervisor user) open a direct platform connection to a host.

However, be aware that a Supervisor station can perform provisioning, which can automate some platform tasks. Provisioning typically applies to subordinate controllers, which are represented in the Supervisor station as Stations (devices) under the NiagaraNetwork.

Note:

Some of the provisioning views provided by a Supervisor are nearly identical to platform views described in this document, including the Software Manager and Application Director, and work in the same fashion. However, if you are new to Niagara, become familiar with the direct platform views described in this document, before using provisioning in a Supervisor.

File locations

During the MultiSITE Supervisor installation and platform commissioning processes, the software differentiates between two types of files based upon the content of the files: configuration and runtime data. Files and folders that contain configuration data reside in separate locations from files and folders that contain runtime data. This separation enhances security by denying general access to the runtime files and allowing each user access to only their personal configuration files.

As a result of separating configuration and runtime data, the system supports multiple home directories on the Supervisor or engineering workstation. These homes may be identified as:

- The system home contains runtime files, such as core software modules, the JRE, and binary executables.
- MultiSITE Supervisor user home for each user contains configuration data, including option files, and registries.
- A platform daemon user home for the Supervisor or engineering workstation contains platform configuration data.
- Two station homes called protected station home and station home are part of each user home.

Homes on a Supervisor

The following table provides a summary of the Supervisor or engineering workstation homes with shortcut information.

Home in the Workbench Nav tree	Home in the Platform Administration view	Niagara 4 alias	Windows folder location and contents	File ORD shortcut
My Host→My File System→Sys	System Home	niagara_home	C:\niagara\niagara-4.x.xx Executables and software files	! (as in NiagaraAX)
My Host→My File System→User Home	N/A	niagara_user_home	C:\Users\userName\Niagara4.x\<brand> Workbench user home for each human user contains that user’s unique configuration files.	~ (unique to N4)
shared folder	N/A	station_home	C:\Users\userName\Niagara4.x\tridium\shared	^ (as in NiagaraAX)
stations folder	N/A	protected_station_home	C:\ProgramData\Niagara4.x\tridium\stations \<stationName>	^^ (unique to N4)
N/A	User Home	niagara_user_home	C:\ProgramData\Niagara4.x\<brand> Platform daemon user home (non-human user) holds platform daemon configuration files. Requires a local platform connection to view in the Platform Administration view.	~ (unique to N4)

Due to our policy of continuous product innovation, some specifications may change without notification

Homes on a controller

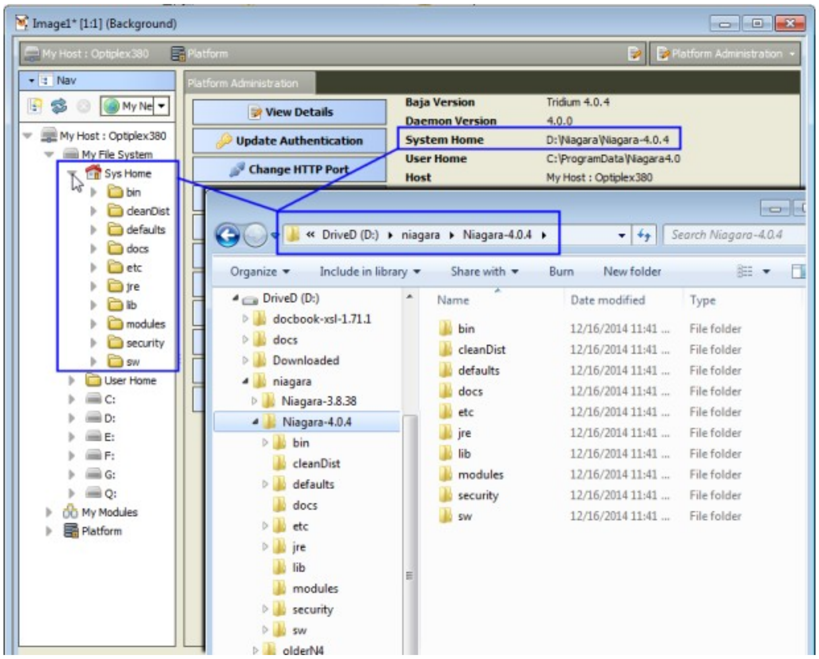
On a controller there are two homes.

Home in the Platform Administration view	Home in the Platform Administration view	Niagara 4 alias	OFD location and contents	File ORD shortcut
Platform→Remote File System→Sys Home (Read Only)	System Home	niagara_home	/opt/niagara Contains operating system data.	! (as in NiagaraAX)
Platform→Remote File System→User Home (Read Only)	User Home	niagara_user_home	/home/niagara Contains configuration data and the installed and running station.	~ (unique to N4)

System home

Sometimes identified by its alias, niagara_home, the system home is the sole location to which the Workbench installation wizard and platform commissioning wizard install Niagara runtime components, such as core software modules, the JRE, and binary executables. License files and license certificates reside in the MultiSITE Supervisor system home, under the security subfolder. A system home contains no configuration files that can be changed by a user. Except when it is time to upgrade, these runtime files are read-only.

Figure 93: Example Sys Home (niagara_home) on Supervisor platform



Baja Version	Tridium 4.0.4
Daemon Version	4.0.0
System Home	D:\Niagara\Niagara-4.0.4
User Home	C:\ProgramData\Niagara4.0
Host	My Host : Optiplex380

Name	Date modified	Type
bin	12/16/2014 11:41 ...	File folder
cleanDist	12/16/2014 11:41 ...	File folder
defaults	12/16/2014 11:41 ...	File folder
docs	12/16/2014 11:41 ...	File folder
etc	12/16/2014 11:41 ...	File folder
jre	12/16/2014 11:41 ...	File folder
lib	12/16/2014 11:41 ...	File folder
modules	12/16/2014 11:41 ...	File folder
security	12/16/2014 11:41 ...	File folder
sw	12/16/2014 11:41 ...	File folder

The example above shows the file system for Niagara 4 Supervisor running on a Windows PC. In the Nav tree, the system home folder is referred to as its Sys Home. In the Platform Administration view, the same system home is referred to as System Home.

In the example, the actual location of the system home folder on this PC is: C:\Niagara\Niagara\-4.0.15.

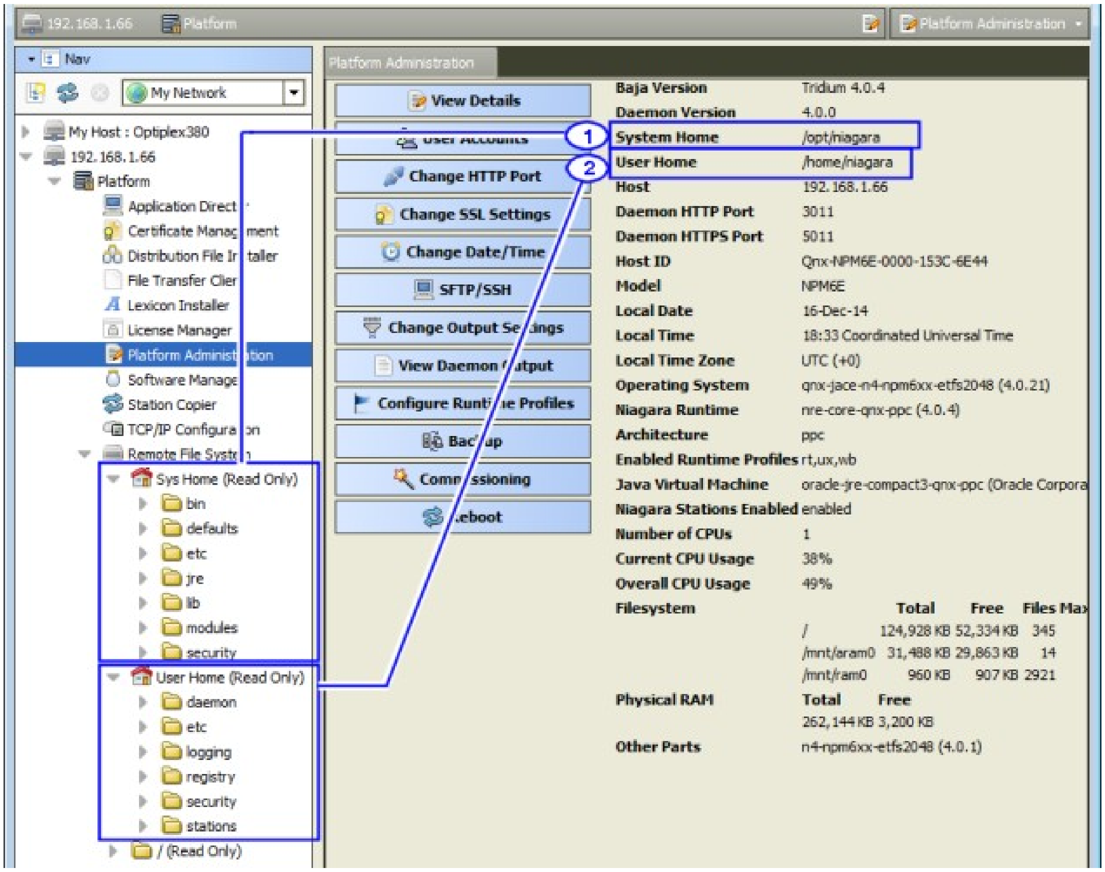
The system home on a controller appears as System Home in the Platform Administration view. The actual location of the system home folder for a controller is: /opt/niagara/opt/Niagara.

Controller user home

The user homes are the locations under which all configurable data reside. Included are stations, templates, registry, logs, and other data. Referred to by the alias niagara_user_home, the separation of these files from the runtime files stored in the system home folder is new in Niagara 4.

The JACE controller has one system home and one user home.

Figure 94: JACE Sys Home (niagara_home) and User Home (niagara_user_home) locations



Baja Version	Tridium 4.0.4
Daemon Version	4.0.0
System Home	/opt/niagara
User Home	/home/niagara
Host	192.168.1.66
Daemon HTTP Port	3011
Daemon HTTPS Port	5011
Host ID	Qnx-NPM6E-0000-153C-6E44
Model	NPM6E
Local Date	16-Dec-14
Local Time	18:33 Coordinated Universal Time
Local Time Zone	UTC (+0)
Operating System	qnx-jace-n4-npm6xx-etfs2048 (4.0.21)
Niagara Runtime	nre-core-qnx-ppc (4.0.4)
Architecture	ppc
Enabled Runtime Profiles	rt,ux,wb
Java Virtual Machine	oracle-jre-compact3-qnx-ppc (Oracle Corpora
Niagara Stations Enabled	enabled
Number of CPUs	1
Current CPU Usage	38%
Overall CPU Usage	49%

Filesystem		Total	Free	Files Max
	/	124,928 KB	52,334 KB	345
	/mnt/aram0	31,488 KB	29,863 KB	14
	/mnt/ram0	960 KB	907 KB	2921

Physical RAM	Total	Free
	262,144 KB	3,200 KB

Other Parts	n4-npm6xx-etfs2048 (4.0.1)

Callout 1 above identifies a controller's system home (alias: niagara_home) in both the Nav tree and the Platform Administration view. In the Nav tree, you can find the controller's system home by expanding Platform→Remote File System. The actual folder for the system home is /home/niagara.

Callout 2 identifies the controller's user home or daemon user home (alias: niagara_user_home) that contains the installed and running station and other configuration files. The actual folder for the daemon user home is: /home/niagara.

Due to our policy of continuous product innovation, some specifications may change without notification

Windows platform user homes

For security reasons, each person that is a user of a Windows platform has their own user home. This means that each Supervisor platform has at least two user home locations: MultiSITE Supervisor User Home (for people), and a platform daemon User Home (for the daemon server processes).

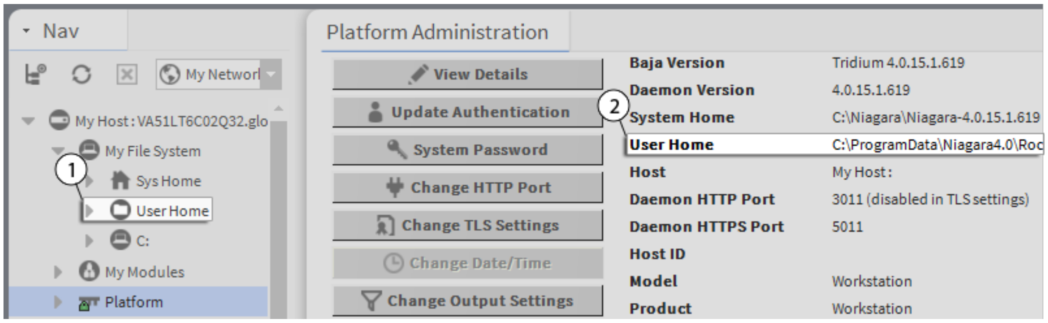
The Supervisor or engineering workstation that is licensed to run a station has a daemon user home. The daemon is a server process and represents a (non-human) user that manages the Supervisor's running station. The Supervisor's daemon user home contains daemon-specific configuration information. The actual location of the Supervisor's daemon user home is C:\ProgramData\Niagara4.0\distech. The platform daemon is installed to this location and started from this location as a Windows service.

In addition to this daemon user home, a Windows host has a separate MultiSITE Supervisor user home for each person (operator, administrator) who logs on with credentials to a Windows-based platform licensed for Workbench, meaning a Supervisor or engineering workstation. Any given PC or workstation has at least one, and may contain multiple Workbench user homes.

Each person's Workbench user home is available in the Nav tree as a node under My Host→My File System and contains unique configuration information that is not shared. This is where to find any new Workbench station, as well as any remote station backups, templates and other configuration files. The actual location of each person's user home is in the Niagara4.0 folder under your Windows User account.

If you open a local platform connection to your Supervisor PC, expand My File System in the Nav tree, and go to the Platform Administration view, you can see both types of user homes at the same time.

Figure 95: Local platform connection to a Supervisor station with MultiSITE Supervisor and daemon user homes

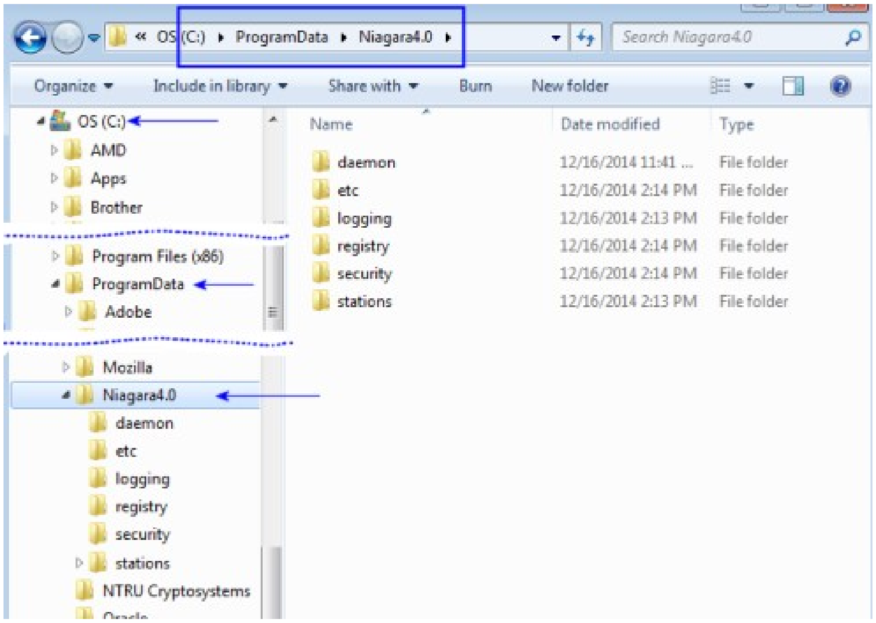


Baja Version	Tridium 4.0.15.1.619
Daemon Version	4.0.15.1.619
System Home	C:\Niagara\Niagara-4.0.15.1.619
User Home	C:\ProgramData\Niagara4.0\Roc
Host	My Host :
Daemon HTTP Port	3011 (disabled in TLS settings)
Daemon HTTPS Port	5011
Host ID	
Model	Workstation
Product	Workstation

- Callout 1 identifies Workbench User Home.
- Callout 2 identifies the daemon User Home.

When you first install Niagara 4 on your PC and start the daemon (by choosing the install option Install and Start Platform Daemon on installation), the installation program creates this daemon User Home (Niagara4.0 folder). Initially, it contains an empty stations sub-folder, until you copy a station to it.

Figure 96: Example of a daemon User Home location in Windows Explorer



Name	Date modified	Type
daemon	12/16/2014 11:41 ...	File folder
etc	12/16/2014 2:14 PM	File folder
logging	12/16/2014 2:13 PM	File folder
registry	12/16/2014 2:14 PM	File folder
security	12/16/2014 2:14 PM	File folder
stations	12/16/2014 2:13 PM	File folder

You can do this station copy in different ways. In Niagara 4, you can let the New Station wizard initiate this copy from its last Finish step. Or as needed, you can manually open a local platform connection and use the Station Copier.

The actual location of each user's home folder is under that user's personal Windows account. Some example Workbench user home locations are the following:

C:\Users\John\Niagara4.0\distech

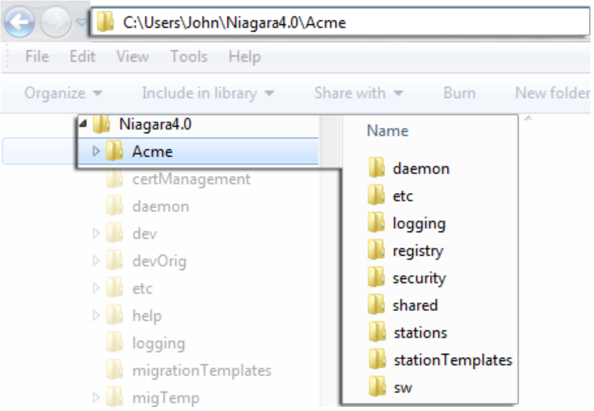
C:\Users\Mike\Niagara4.0\distech

where "John" and "Mike" are separate Windows user accounts. The first time a Windows user starts Workbench, the system automatically creates that user's unique user home folder.

- The person that installs Niagara 4 on a PC acquires the first such user home. If no other Windows users log on to that PC, this may be the only Workbench user home on the platform.
- However, if another person logs on to Windows on that computer and starts Workbench, that user also acquires their own Workbench user home.

The following figure shows an example Workbench user home location in Windows Explorer.

Figure 97: Example of an automatically-created Workbench User Home in Windows Explorer


C:\Users\John\Niagara4.0\Acme

Station homes

Niagara 4 uses the Java Security Manager to protect against malicious from accessing station or platform data and APIs. The Security Manager uses signed policy files that specify the permissions to be granted to code from various sources. Included are tighter controls about which applications have access to parts of the file system. Two folders under the Workbench User Home serve to protect sensitive data while allowing authorized access to data that can be shared.

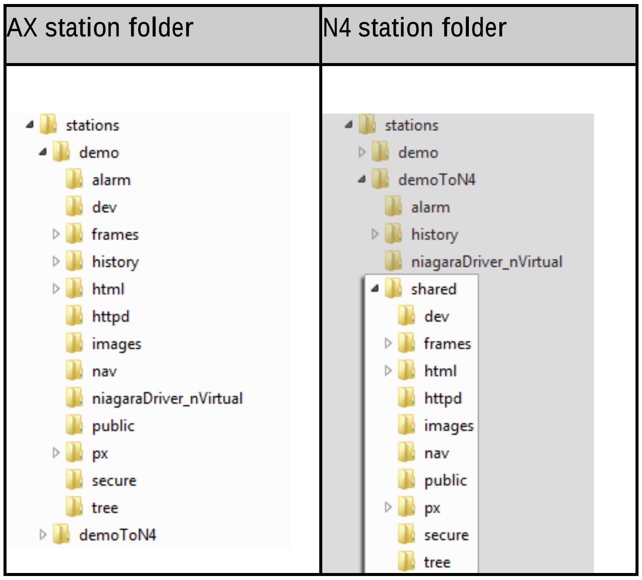
- The stations sub-folder, otherwise known as the protected station home (alias: protected_station_home) contains the running station's file system, and may be accessed only by core Niagara software modules. Station items that are always in protected station home, that is, items that are not under the shared sub-folder include the following folders, as applicable:

– alarm
– history
– niagaraDriver_nVirtual
– provisioningNiagara
– dataRecovery

All files in the stations folder root (config.bog, config.backup.timestamp.bog, etc.) are always in protected station home. For this reason, in Niagara 4 it is no longer necessary to blacklist or whitelist station files or folders.

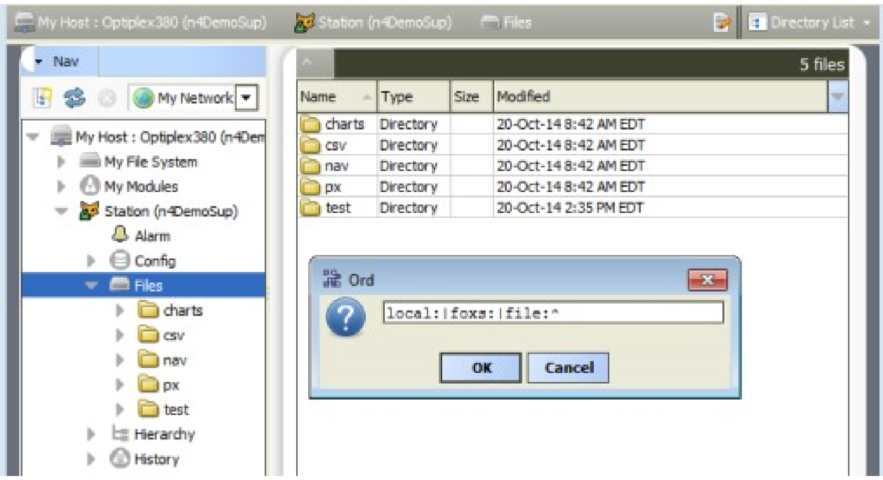
- The shared sub-folder, otherwise known as the station home (alias: station_home), allows all modules to have read, write, and delete permissions. The alias station_home retains the same file ORD shortcut (^) as used in NiagaraAX—only in Niagara 4 this points to the station's shared sub-folder.

Figure 98: Example NiagaraAX station file folders compared to Niagara 4 station file folders



As shown in the figure above, comparing an AX station file folder structure (left side) to the same station migrated to Niagara 4, a number of folders are now under this shared sub-folder. Included are folders and files used in graphical (Px) views or navigation, such as images, px, nav and so on. Modules that are prevented from writing to the station root by the Security Manager must also write to the shared sub-folder.

Figure 99: File ORD for the station home in Niagara 4 now points to the shared folder



Name	Type	Size	Modified
charts	Directory		20-Oct-14 8:42 AM EDT
csv	Directory		20-Oct-14 8:42 AM EDT
nav	Directory		20-Oct-14 8:42 AM EDT
px	Directory		20-Oct-14 8:42 AM EDT
test	Directory		20-Oct-14 2:35 PM EDT

```
local:|foxs:|file:^
```

As shown in a station running above, the station home (alias: station_home) file ORD (^) now points to the contents of the shared sub-folder. Other items in protected station home are no longer accessible or visible.

Copying a new station to the daemon user home

In Niagara 4, the New Station Wizard tool finishes with an option to copy the station from the station home (the location for each new station) under your Workbench User Home to the User Home of the local platform daemon.

Prerequisites: The new station exists in the station home (under User Home).

Step 1 When the New Station Wizard prompts you with the option to Copy station, select the option and click Finish.

Step 2 Make a local platform connection and log on.

The Station Copier transfers the station and prompts you with the options to start the station after copying and enabling auto-start.

Step 3 Select the option to start the station.

The Application Director opens with the new station present in the daemon User Home.

The new station now exists in two locations on your local host: the original location in your MultiSITE Supervisor User Home, and also in the platform daemon User Home.

Once the station is running in the daemon User Home, you can make a backup of the running station, where the backup .dist file goes in the backups folder of your Workbench User Home. Or, you can use the platform Station Copier to copy the station back to the stations folder of your Workbench User Home.

Note:

Using the Station Copier to copy the station back to your Workbench User Home is highly recommended if you made any changes to the station. This is essential if you are installing it (copying it) to any remote platform. Remember, the copy of the station in your Workbench User Home is immediately obsolete as soon as you make changes to the copy of the station running in the daemon User Home.

Running a station from Workbench User Home

Instead of running a station out of the daemon User Home, you can run a station directly from your Workbench User Home (outside of normal platform daemon control).

You do this using the Niagara 4 console command:

station stationName

This is not a recommended way to run a production station, but instead more of a developer utility that allows quick access to station debug messages in the console window. If you run the station this way, be mindful of possible port conflicts with any other station that the daemon user may be running locally (in daemon User Home), meaning Fox ports, Web ports, and so on.

Shared file strategy

A sharing strategy makes it possible for multiple users of a single Supervisor or engineering workstation to share station files including backups.

If multiple people log on (differently) to Windows on Niagara 4 host and use Workbench, each person has their own separate Workbench User Home.

Windows users require permissions to access other users' files; yet it's possible that different users of a system (Supervisor or engineering workstation) may need to share items such as station backups, station copies, saved template files, and so on. Such items may be in multiple Workbench User Home locations in Niagara 4 (unlike in NiagaraAX where a single !\backups or !\stations folder applies to all users).

Therefore, in some scenarios you may need to establish a sharing strategy, perhaps re-copying such items to a commonly-accessible folder location on the Niagara 4 Windows PC. For example, you might create a shared folder under the Niagara 4 Sys Home location (Workbench User Home is not shareable).

Upgrading a controller

You must use the Commissioning Wizard to upgrade the software in a MultiSITE VM3. This means either an “update” upgrade (say from build 4.0.101 to 4.0.106), or a full “minor” release upgrade, for example build 4.0.106 to build 4.1.88.

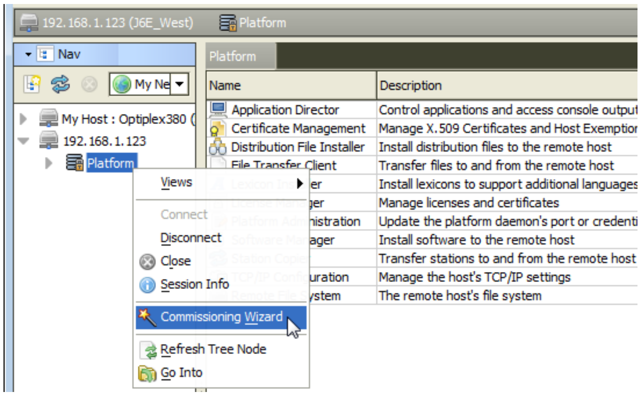
Note:

When updating a multi-station system for the first time to an update release, it is recommended to upgrade a Supervisor before its subordinate JACEs.

Any JACE to be upgraded from one minor version to another, say from 4.0.nn to 4.1.nn, requires a license upgrade, purchased before starting the upgrade. Otherwise, the Commissioning Wizard will not perform the upgrade. This prevents the scenario where an upgraded controller cannot start its station, due to a licensing error.

With a platform connection to any JACE, access the Commissioning Wizard by simply right-clicking on that platform and selecting it from the menu, as shown in the figure below.

Figure 100: Commissioning Wizard (right-click option in opened platform)

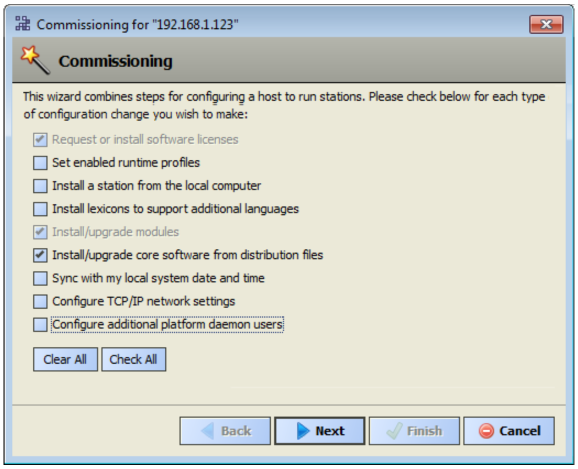


Platform

Name	Description
Application Director	Control applications and access console output
Certificate Management	Manage X.509 Certificates and Host Exemptior
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 credenti
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
Remote File System	The remote host's file system

If this is a controller upgrade, in the wizard’s opening selection of steps you typically deselect most items that were previously run at the controller’s initial commissioning time, for example to set enabled runtime profiles, set date and time, configure TCP/IP settings, and so on. See the figure below.

Figure 101: Typical upgrade selections for existing JACE (already running a station)



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 additional platform daemon users

To upgrade a JACE, you select either of the following:

- In the case where the upgrade requires an updated license installed: “Request or install software licenses” (this may already be pre-selected).
- In the case where a station install also requires commissioning the JACE (i.e. upgrade): “Install station from the local computer”
- And always: “Install/upgrade core software from distribution files”

When you proceed in this manner, the wizard automatically finds and selects all core distributions needed for the JACE. Then, in the pre-selected “Install/Upgrade modules” step, the wizard provides the option to also upgrade all out-of-date software modules (always do that).

A final summary step allows you to review the upgrade before the wizard executes and performs its operations.

CHAPTER 2 PLATFORM SERVICES

This chapter explains the platform access available in a running station, in other words, the station's perspective on its host platform. Unlike the various platform views, a platform connection is not needed to access platform services. Instead, you need only a standard station (Fox) connection.

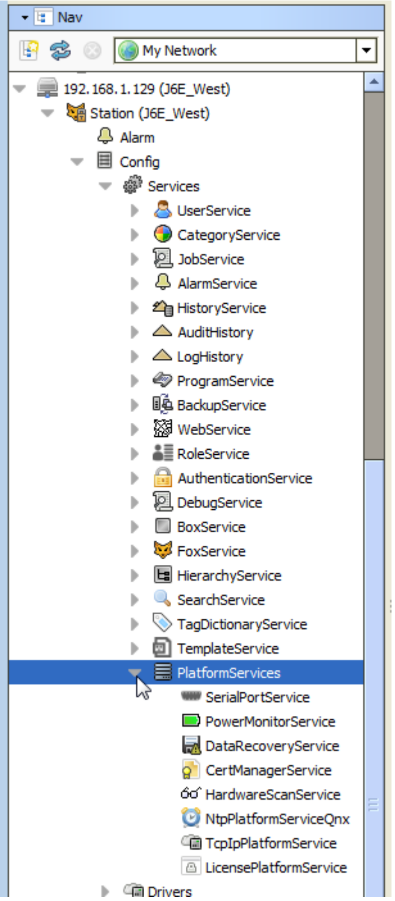
The following topics are covered in this chapter:

- About Platform Services
- PlatformServiceContainer parameters
- SystemService (under PlatformServices)
- Platform service types
- Using platform services in a station
- About the NtpPlatformService

About Platform Services

Under Config, Services, every running station has a PlatformServices container, which any station user, with admin-level permissions to this component, can access.

Figure 102: Example JACE station's PlatformServices



Platform services in a running station provide two main types of functionalities

- A subset of platform views available in a platform connection. Platform services does not provide the full set of functions available in a platform connection. For example, you cannot install or upgrade software, or transfer stations and files. However, a number of platform configuration views are available under a station's PlatformServices.
- Certain platform configuration settings accessible only through PlatformServices, that is, they are not available in a client platform connection.

Note:

When engineering station security, be careful about assigning user permissions to PlatformServices and its child service components. In general, you should regard this portion of the station as most critical, as it allows access to items such as host licenses and TCP/IP settings. Furthermore, right-click actions on the PlatformServices include "Restart Station".

Component differences for platform services

PlatformServices and all child components are unique from all other station components. PlatformServices is different from all other components in a station in the following ways:

- It acts as the station interface to specifics about the host platform (whether JACE or a PC).
- It is built dynamically at station runtime, you do not see PlatformServices in an offline station.
- Changes you make to PlatformServices and all child services are not stored in the station database. Instead, changes are stored in other files on that platform, such as its platform.bog file, or within the platform's operating system.

Note:

⃠ Do not attempt to edit platform.bog directly; always use PlatformServices' views.

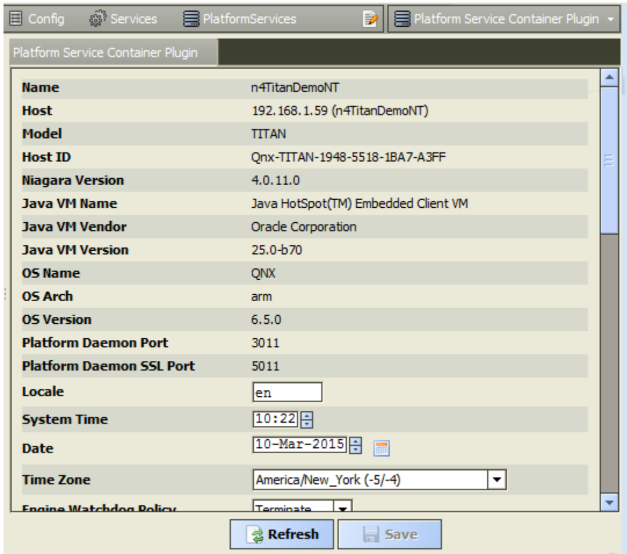
In summary, when you make changes under a station's PlatformServices, those changes are independent of the running station. If you install another station, platform services are dynamically recreated again when the new station starts, based upon the last settings.

In addition, understand that some changes in platform services views may require the host to be rebooted to become effective. Examples include TCP/IP changes, or some NTP-related changes in a controller. A "Reboot Now?" popup dialog appears upon saving such a change.

PlatformServiceContainer parameters

In addition to being a container, the default Platform Service Container Plugin view provides various status and configuration entries for the host platform. In the Nav tree, double-click PlatformServices to access this view, as shown below.

Figure 103: PlatformServicesContainerPlugin view (many entries not shown)


Config
Services
PlatformServices
Platform Service Container Plugin
Platform Service Container Plugin
Refresh
Save

Name	n4TitanDemoNT
Host	192.168.1.59 (n4TitanDemoNT)
Model	TITAN
Host ID	Qnx-TITAN-1948-5518-1BA7-A3FF
Niagara Version	4.0.11.0
Java VM Name	Java HotSpot(TM) Embedded Client VM
Java VM Vendor	Oracle Corporation
Java VM Version	25.0-b70
OS Name	QNX
OS Arch	arm
OS Version	6.5.0
Platform Daemon Port	3011
Platform Daemon SSL Port	5011
Locale	en
System Time	10:22
Date	10-Mar-2015
Time Zone	America/New_York (-5/-4)
Engine Watchdog Policy	Terminate

Included are many read-only status values as well as configuration parameters. Each is described in separate sections as follows:

- PlatformServiceContainer status values
- PlatformServiceContainer configuration parameters

By default, any PlatformServiceContainer also provides three right-click actions. See the section, “PlatformServiceContainer actions”.

PlatformServiceContainer status values

Status values in a station’s PlatformServices container include the following:

- Name: Name of running station.
- Host: IP address of host platform.
- Model: Model of host platform type, such as NPM6, JACE-8000, or Workstation. See the section, “Models of platforms” for further details.
- Host ID: Niagara host identifier, a string unique to this one machine.
- Niagara Version: Version and build number of the Niagara distribution running in the host platform.
- Java VM Name: Java virtual machine used, for example, “Java HotSpot(TM) Embedded Client VM” for any N4 controller, or “Java HotSpot(TM) 64-Bit ServerVM” for a Supervisor on a Windows host.
- Java VM Vendor: Vendor for Java VM: Oracle Corporation.
- Java VM Version: Version of Java VM, for example, “25.0-b 70” for the Java 8 compact3 VM on a controller, or “25.31-b07” for the Java 8 SE VM on a Windows host.
- OS Name: Operating System name, such as “QNX” or “Windows 7.”
- OS Arch.: Machine architecture for OS, such as “arm” or “ppc” (controller hosts) or “amd64” (Windows hosts).
- OS Version: Operating System version, such as “6.5.0” (QNX) or “6.1” (Windows 7).
- Platform Daemon Port: Port number on which the platform daemon that started the station is listening for its platform server (3011, or another port number). This can prove useful in case you changed the platform port, but then forgot what the new port is.

- Platform Daemon TLS Port: Port number on which the platform daemon is listening for its platform TLS server (5011, or another port number, provided that platform TLS enabled). If platform TLS is disabled, it reads Unknown. This can prove useful in case you changed the platform TLS port), but then forgot what the new port is.

Note that in the container plugin, most of the remaining entries are configuration parameters. However a few status values are also mixed in, and are described below.

- Number of CPUs: Number of CPUs used in the host platform (typically 1 if a controller, more if a Windows host).
- Current CPU Usage: Percentage of CPU utilization in the last second.
- Overall CPU Usage: Percentage of CPU utilization since the last reboot.
- Filesystem: File storage statistics for the host, including total file space, available (free) space, and file block size (minimum size for even the smallest file). For a JACE-8000 host, the statistics may look similar to the following:

	Total	Free	Files	Max Files
/	3,476,464 KB	3,039,088 KB	602	108640
/mnt/aram0	393,215 KB	381,019 KB	0	0
/mnt/ram0	8,192 KB	8,192 KB	0	0

- Physical RAM: Current total and free RAM statistics for the host. For a JACE-8000, the statistics may look similar to the following:

Total	Free
1,048,576 KB	113,424 KB

- Serial Number: (Appears only if a JACE host). The controller's unique serial number.
- Hardware Revision: (Appears only if a JACE host). Hardware revision of the controller.
- Hardware Jumper Preset: (Applies only if a JACE host, except for a JACE-8000) Either true or false, indicates whether or not the mode jumper is installed for "serial shell mode" access. Read at boot time only.

See the next section "PlatformServiceContainer configuration parameters".

PlatformServiceContainer configuration parameters

Configuration properties of a station's PlatformServices Container are listed below. If needed, you can change any in the container plugin view (property sheet). Click Save to write to the host platform.

Note:

It is recommended that you leave engine-related parameters and other advanced settings at default values, unless you have been directed otherwise.

Locale

Determines locale-specific behavior such as date and time formatting, and also which lexicons are used. A string entered must use the form: language [“_” country [“_” variant]]. For example, U.S. English is “en_US” and traditional Spanish would be “es_ES_Traditional”.

System Time

This is the current local time in host (read-only if a Windows host).

Date

This is the current local date in host (read-only if a Windows host).

Time Zone

This is the current local time zone for host (read-only if a Windows host).

Engine Watchdog Policy

The engine watchdog is a platform daemon process, to which the station periodically reports its updated engine cycle count. The watchdog purpose is to detect and deal with a “hung” or “stalled” station, and is automatically enabled when the station starts.

The Engine Watchdog Policy defines the response taken by the platform daemon if it detects a station engine watchdog timeout. Watchdog policy selections include:

- Log Only: Generates stack dump and logs an error message in the system log. (The station should ultimately be restarted if a watchdog timeout occurs with the “Log Only” setting).
- Terminate: (Default) Kills the VM process. If “restart on failure” is enabled for the station (typical), the station is restarted.
- Reboot: Automatically reboots the host JACE platform. If “auto-start” is enabled for the station, the station is restarted after the system reboots.

Engine Watchdog Timeout

Default is 1 minute, and range is from 0 minutes to infinity. If the station's engine cycle count stops changing and/or the station does not report a cycle count to the platform daemon within this defined period, the platform daemon causes the VM to generate a stack dump for diagnostic purposes, then takes the action defined by the Engine Watchdog Policy.

Enable Station Auto-Save

Either Enable (default) or Disable. This allows for “auto-save” of running station to “config_backup_<YYMMDD>_<HHMM>.bog” file at the frequency defined in next property. Auto-saved backup files are kept under that station's folder.

Station Auto-Save Frequency

Default is every 24 hours for any JACE platform, or every (1) hour if a Windows host. Range is from 1 to many hours.

Station Auto-Save Backups to Keep

Oldest of kept backups is replaced upon next manual save or auto-save backup, once the specified limit is reached. The default value for JACE platform is 0 (none), and should be kept low.

However, changing to 1 provides a benefit in the case where a catastrophic (yet inadvertent) station change is made, such that a station “kill” can be issued to revert back to the backup copy on the JACE.

In Windows hosts, the default is 3, and typically can be safely adjusted up, if desired.

Battery Present

This applies to configuration of a JACE's backup battery (Applies only if a JACE host other than a JACE-8000). This is used to specify whether the controller has an integral backup battery, typically an onboard NiMH battery. The default property value is true, which is recommended unless the controller is both SRAM-equipped and is without an attached backup battery. There is no way to detect the latter through software.

If set to false and saved, upon the next reboot the station's PowerMonitorService no longer monitors for a backup battery, with the underlying "power daemon" stopped. This prevents nuisance "battery bad" alarms. Station backup is dependent totally on SRAM and the station's DataRecoveryService. The JACE must have the platDataRecovery module installed, and be licensed for DataRecovery.

The configuration described above is only one of three possible backup options for an SRAM-equipped controller that can also have a backup battery installed (example. JACE-6E or JACE-3E, or else a JACE-6 or JACE-7 with an SRAM option card). The two other options are to use both backup battery and SRAM for backup, or to use backup battery only (and not SRAM). These other two options require that this Battery Present property is set to true.

Failure Reboot Limit

(JACE platforms only) This limits the number of station restarts that can be triggered by station failures, within the Failure Reboot Limit Period (see below). Default value is 3.

Failure Reboot Limit Period

(JACE platforms only) This specifies the repeating frequency of the Failure Reboot Limit period, with a default value at 10 minutes.

These two "Failure Reboot" settings are also adjustable (in any version of QNX-based host) within that JACE's !daemon/daemon.properties file, for the following two properties:

– failureRebootLimit=x (where x is integer, default is 3)
– failureRebootLimitPeriod=y (where y is long in milliseconds, default is 3600000)

RAM Disk Size

This has one configurable field and one read-only field:

– Min Free: Minimum allowable free size in %. If status is not Ok, a "Low RAM disk space" warning is overlaid in all Workbench views of the station.
– Size: Read-only in MB, where default is 32 for a JACE-3E or JACE-6 or JACE-6E series, or 48 for a JACE-7 series, or 394 for a JACE-8000 series. Specifies the size of RAM disk used to store history and alarm files.

Java Heap

This has one configurable "Min Free" field, in MB. Specifies the minimum free Java heap size, in MB, against which the station compares (tests) for low memory conditions, that is excessive Java heap. The default varies according to JACE model. This test automatically runs once a minute. If the heap free byte count is less than the defined minimum free heap size, a "low memory warning" appears in all Workbench views of the station. The warning is a yellow message box overlaid on any new view accessed, or on any current view that is refreshed. This warning is removed when the heap free byte count rises above the defined minimum size—such as might occur if enough components are deleted from the station.

All memory statistics, including those for heap, are accessible on a station opened in Workbench, via the Resource Manager view of the Station component.

Open File Descriptors

This has one configurable "Min Free" field, related to number of files (and/or open sockets). It specifies the maximum amount of file descriptors that can be used. That is, the read-only "Max Open" number minus the "Min Free" amount. File descriptors are used for histories, modules, and Fox connections. If exceeded, a "Station has too many open files or sockets" warning is overlaid in all Workbench views of the station.

Free RAM

This has one configurable “Min Free” field, in KB. It specifies the minimum RAM that can be left free during station operation. If status is not Ok, a “Low free RAM” warning is overlaid in all Workbench views of the station.

Disk Space

This has one configurable “Min Free” field, in %. It specifies the minimum percentage of disk storage that can be left free during station operation. Below this amount, a “Platform running low on disk space” warning is overlaid in all Workbench views of the station.

Files

This has one configurable “Min Free” field, to specify the minimum number of free files available during station operation. Below this amount, a related platform warning appears. Note that the PlatformServiceContainer status property “Filesystem” includes both the current number of files and the maximum number of files for each partition on a JACE controller.

See the next section, “Model-specific PlatformServiceContainer properties”.

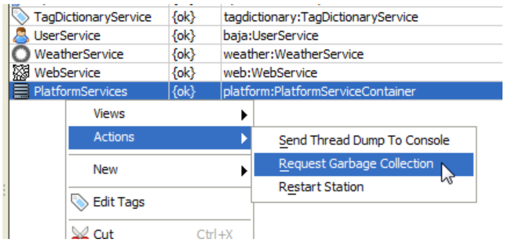
Model-specific PlatformServiceContainer properties

Some JACE controller models may have yet more PlatformServices properties, specific to special hardware features. This is in addition to the standard and additional properties described above. Typically, these are configured at JACE commissioning time.

PlatformServiceContainer actions

The PlatformServices Container also provides three right-click actions, as shown below.

Figure 104: PlatformServicesContainer actions.



TagDictionaryService	{ok}	tagdictionary:TagDictionaryService
UserService	{ok}	baja:UserService
WeatherService	{ok}	weather:WeatherService
WebService	{ok}	web:WebService
PlatformServices	{ok}	platform:PlatformServiceContainer

These actions are described as follows:

- Send Thread Dump to Console: This causes that host’s platform daemon to have the station send a VM thread dump to its standard output (console), equivalent to the “Dump Threads” command in the platform Application Director view. This is typically used only during troubleshooting.

Note:

Apart from Application Director (platform access) to view station output, you can also view a “snapshot” of station output in a browser. Do this via the “stdout” link in the spy utility, at the URL http://<hostIP>/ord?spy:/stdout.

- Request Garbage Collection: This causes the JVM running the station to perform garbage collection. This results in a “best effort” towards releasing unused objects and making more memory available on the “heap”. Note that current heap and memory statistics for any running station are available on the ResourceManager view of the station component.
- Restart Station: This produces a popup confirmation dialog. This applies directly to any station, whether running on a JACE controller or a Windows platform. It is equivalent to issuing a “Restart” command from the platform Application Director view. The station is saved on its host, and then restarted. Note that unlike in NiagaraAX, this does not result in a reboot of a JACE controller.

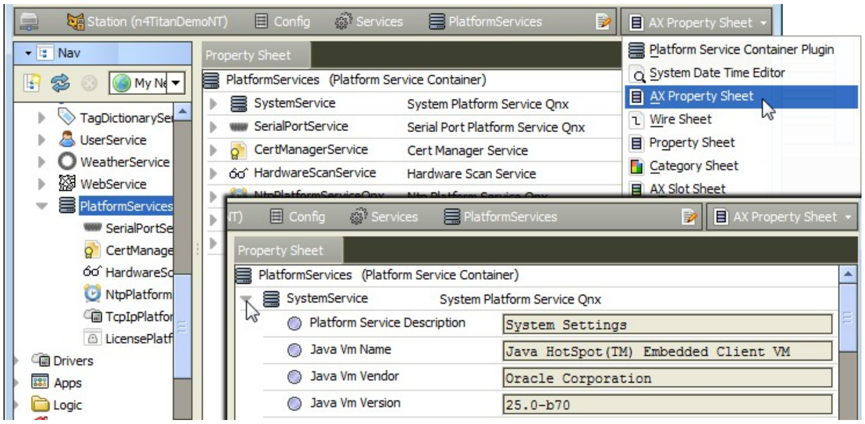
Note:

Also, most child services under the PlatformServices Container have an available “Poll” action, which refreshes their property values. See the section “Platform service types”, for a listing of possible child services.

SystemService (under PlatformServices)

PlatformServices also contains a child “SystemService” container, accessible from its property sheet as shown below. Unlike other child services, SystemService does not appear in the Nav tree.

Figure 105: SystemService from property sheet of PlatformServices.



PlatformServices (Platform Service Container)

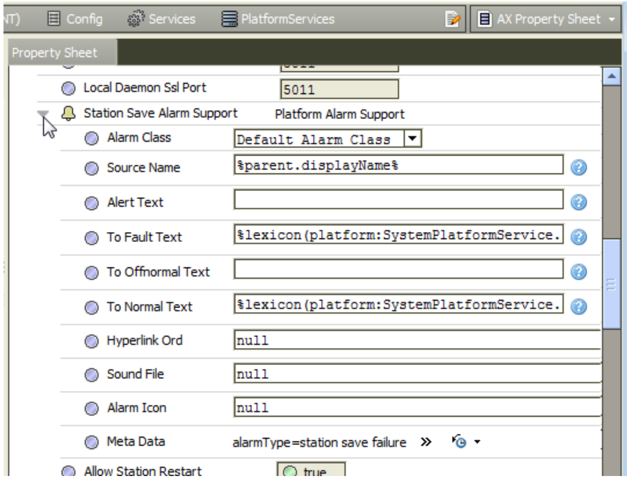
SystemService	System Platform Service Qnx
SerialPortService	Serial Port Platform Service Qnx
CertManagerService	Cert Manager Service
HardwareScanService	Hardware Scan Service

PlatformServices (Platform Service Container)

SystemService	System Platform Service Qnx
Platform Service Description	System Settings
Java Vm Name	Java HotSpot(TM) Embedded Client VM
Java Vm Vendor	Oracle Corporation
Java Vm Version	25.0-b70

When you expand SystemService, you see most of the same properties available in the default Platform Service Container Plugin view (see “PlatformServiceContainer parameters”). In addition, as shown below, there is a container slot “Station Save Alarm Support”.

Figure 106: Station Save Alarm Support expanded in property sheet of SystemService.



Local Daemon Ssl Port	5011
Station Save Alarm Support	Platform Alarm Support
Alarm Class	Default Alarm Class
Source Name	%parent.displayName%
Alert Text	
To Fault Text	%lexicon(platform:SystemPlatformService.
To Offnormal Text	
To Normal Text	%lexicon(platform:SystemPlatformService.
Hyperlink Ord	null
Sound File	null
Alarm Icon	null
Meta Data	alarmType=station save failure
Allow Station Restart	true

Properties under “Station Save Alarm Support” allow you to configure the alarm class and other parameters to use for “station save” alarms. Such an alarm may occur, for example, if there is insufficient disk space to complete the save.

Properties work the same as those in an alarm extension for a control point.

Note:

Other platform warnings from defined limits, such as for low memory, low disk space, and so on are not really alarms, they simply generate a yellow overlay in the lower right corner when viewing the station in Workbench. If you need actual alarms, you can link from an appropriate boolean slot of the SystemService component (for example, “LowHeap”) into other persisted station logic in another area of the station.

If linking to PlatformServices, be aware that you should change the link type from “handle” to “slot path”. For related details, see the section “PlatformServices binding and link caveats”.

Platform service types

In addition to the SystemService found under its property sheet, the PlatformServices Container has various child services, of which different types are listed below.

Note:

Some platform services are intended to support installations where all configuration must be done using only a browser connection (and not an Workbench platform connection to an JACE’s platform daemon). Examples include types TcpIpService and LicenseService.

The list of visible platform service types includes the following:

CertManagerService

For management of PKI certificate stores and/or allowed host exceptions, used in certificate-based TLS connections between the station/platform and other hosts.

TcpIpPlatformService

This provides access to the same configuration using the platform’s TCP/IP Configuration view. See “TCP/IP Configuration”.

LicensePlatformService

This provides access to the same configuration using the platform’s License Manager view. See “License Manager”.

SerialPortService

This allows review of available serial ports on the host platform (JACE platforms only).

PowerMonitorService

This provides configuration and status of the controller’s battery monitoring and AC power-fail shutdown routines (All platforms except for JACE-8000 series). See the section “Power monitoring” for details.

NtpPlatformService

This provides the Niagara 4 interface to the NTP (Network Time Protocol) service or daemon of the platform’s OS (QNX or Windows), including several configuration parameters and a list specifying one or more NTP time servers. For details, see the section “About the NtpPlatformService”.

DataRecoveryService

(JACE platforms only) This allows monitoring the service that automatically creates and manages static RAM buffers in the controller, allowing “battery-less” operation (if so configured), or usage of the SRAM along with an installed backup battery (if applicable).

HardwareScanService

(JACE platforms only) Optional platform service that provides a graphical diagram of communication ports and other features on the hosting platform, including callouts to a table that explain the location, description (such as COM2), port type, and status/usage of each item. This requires installation of the modules platHwScan, and a corresponding platHwScanType.

Using platform services in a station

Apart from configuration usage, some platform services under the Container provide status values that you can further incorporate. Typically, each value also provides built-in alarm features. Usage is typically for power monitoring.

Power monitoring

By default, through the PowerMonitorService, any JACE provides status monitoring of the following items, via “Boolean” type slots:

- AC power: (“Primary Power Present” slot): True whenever AC power is currently supplied to the JACE.
- Battery level: (“Battery Good” slot): True if last JACE test of NiMH backup-battery was good. Also included is a “Time of Last Test” slot that provides a timestamp for the last battery test.

If needed, you can make Px bindings or links to these slots. However, see the section “PlatformServices binding and link caveats”.

In addition to these read-only status slots, the PowerMonitorService provides related configuration slots, which you typically review at commissioning time.

Battery monitoring disabled

This does not apply to a JACE-8000 series controller. An SRAM-equipped JACE can be configured for “batteryless” operation. The platDataRecovery module must be installed, and JACE licensed with the “dataRecovery” feature. The PowerMonitorService will continue to monitor for an (optional) backup battery, and upon loss of AC power, allows continuous operation on battery power until the Shutdown Delay time is reached, unless you set the “Battery Present” property (of its PlatformServiceContainer) from true (the default) to false. This disables backup battery support and prevents ongoing “battery bad” nuisance alarms, when there is no backup battery. For related details see the section “PlatformServiceContainer configuration parameters”.

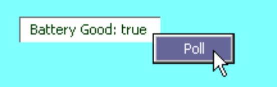
PlatformServices binding and link caveats

Because any station’s PlatformServices are dynamically built upon startup, if binding it’s slots to Px widgets (or linking to other station components), be aware of the following limitations or guidelines:

- Subscription behavior is unique to a station’s PlatformServices slots, in that property values initially load, but do not automatically update. To explicitly refresh such properties, you must invoke the “poll” action of the container for those properties.

For example, if on a Px page you bind a BoundLabel to the PowerMonitorService’s “Battery Good” slot, it will display text as “true” or “false.” However, this value does not update until the user right-clicks for the “Poll” action, which forces a fresh read.

Figure 107: Poll action on bound PlatformServices property

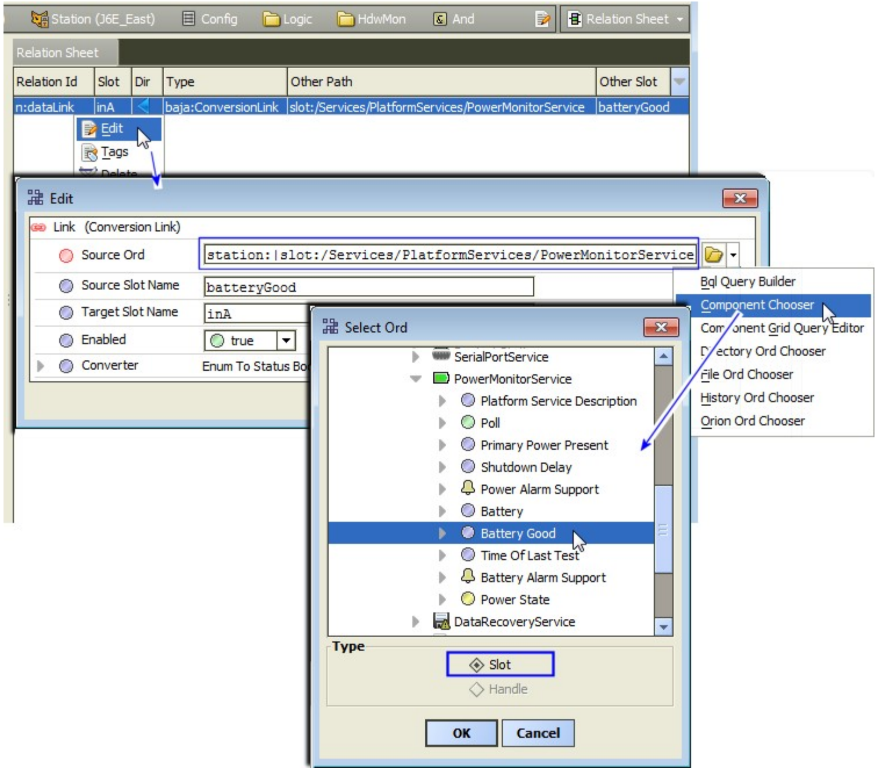

Battery Good: true

- Links from PlatformServices (and child slots) to other station components must use a source ord “slot path”, versus “handle”. Otherwise, after a station restart or host reboot, handle-sourced links may be lost. An example link being edited to use slot path is shown in the figure above.

Note:

Consider the “update limitation” before linking PlatformServices slots into other components that provide control logic. Linked slot values may well be outdated shortly after station startup, yet still “subscribed” and not marked as “stale.”

Figure 108: From RelationSheet of target component, editing link to use slot path for source ord.



Relation Id	Slot	Dir	Type	Other Path	Other Slot
n:dataLink	inA		baja:ConversionLink	slot:/Services/PlatformServices/PowerMonitorService	batteryGood

Link (Conversion Link)

Source Ord: station:|slot:/Services/PlatformServices/PowerMonitorService

Source Slot Name: batteryGood

Target Slot Name: inA

Enabled: true

Converter: Enum To Status Bo

However, note that the station’s plugins (views) for the PlatformServices do provide updated property values, as they work in concert with the special polling used for platform-resident data.

About the NtpPlatformService

PlatformServices in any station contains a child NtpPlatformServicesOS, which provides an interface to the RFC 1305-compliant NTP (Network Time Protocol) service or daemon running on that host platform. NTP is the currently recommended time synchronization protocol to use between inter-networked devices, offering more accuracy than the older RFC 868 Time Protocol.

By default, this platform service is disabled.

- If left disabled, this platform service does nothing.
- If enabled, this platform uses NTP as a client to sync its clock with time values retrieved from one or more NTP time servers, according to other configuration properties.

Note:

An enabled NtpPlatformService will not allow client synchronization with time servers using RFC 868, even if the station also has a TimeSyncService under its Config, Services folder. See the section “Interaction with station’s TimeSyncService” for related details.

See the following sections for more details:

- About the Ntp Platform Service Editor
- NTP port/firewall considerations

About the Ntp Platform Service Editor

For either platform OS type (Windows or QNX), the default view for any NtpPlatformService is an Ntp PlatformService Editor OS view, your typical interface. Double-click any NtpPlatformService to see this editor.

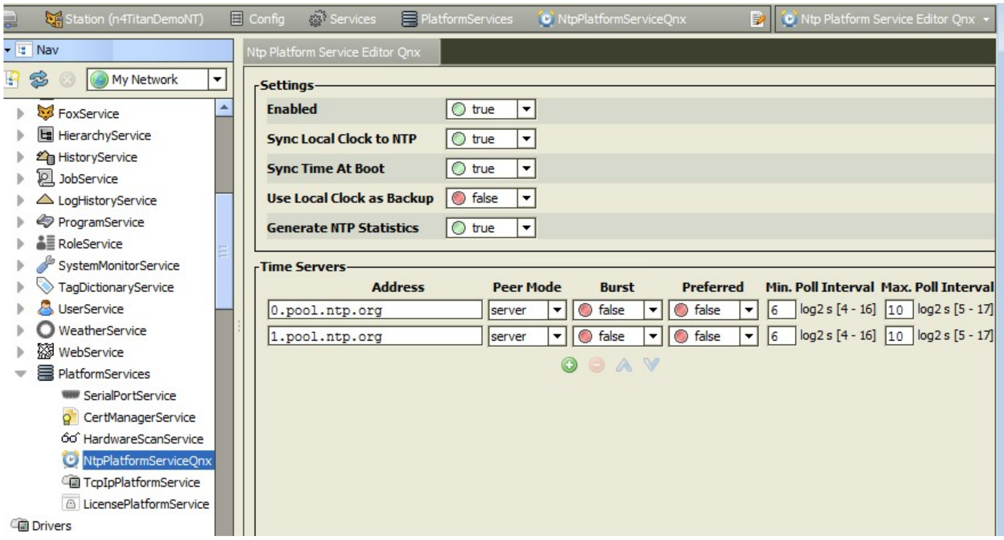
In the NtpPlatformService Editor on any Windows platform is disabled and read-only.

- Ntp Platform Service Editor QNX
- Ntp Platform Service Editor Win32

About the Ntp Platform Service Editor Qnx

An example Ntp Platform Service Editor for a JACE controller is shown below. This is the default view for the NtpPlatformServiceQnx.

Figure 109: Ntp Platform Service Editor Qnx



Settings

Enabled	true
Sync Local Clock to NTP	true
Sync Time At Boot	true
Use Local Clock as Backup	false
Generate NTP Statistics	true

Time Servers

Address	Peer Mode	Burst	Preferred	Min. Poll Interval	Max. Poll Interval
0.pool.ntp.org	server	false	false	6 log2 s [4 - 16]	10 log2 s [5 - 17]
1.pool.ntp.org	server	false	false	6 log2 s [4 - 16]	10 log2 s [5 - 17]

This dialog provides access to some of the key settings of the NTP daemon (ntpd) of the QNX OS running on the host JACE platform.

There are two main areas: Settings at top, Time Servers at bottom. The NtpPlatformServiceQnx also has an available “Sync Now” action. For more details, see the section “Sync Now action”.

Ntp Platform Service Editor Qnx settings

Settings in the Ntp Platform Service Editor Qnx include the following properties:

- Enabled

If true, the host will use NTP to sync its clock with time values retrieved from other servers.

- Sync Local Clock to NTP

If true, this enables the host to adjust its local clock by means of NTP. If disabled (false), the local clock free-runs at its intrinsic time and frequency offset. This flag is useful in case the local clock is controlled by some other device or protocol and NTP is used only to provide synchronization (as server) to other clients. In this case, the local clock driver can be used to provide this function and also certain time variables for error estimates and leap-indicators.

- Sync Time At Boot

Default is false. If true, when the JACE boots, before the stations starts or the ntpd starts, it executes the ntpdate command. This updates the system local time.

- Use Local Clock as Backup

If true, should the specified NTP server(s) become unavailable at the time of a poll, the time used is provided by the system clock. This prevents the timing of the polling algorithm in the ntpd (which is executed at specified/changing intervals) from being reset.

A true value does not result in any change to the NTP daemon’s polling interval (frequency). In fact, by using the local system clock the NTP-calculated polling time would remain the same, and therefore not result in more polling.

- Generate NTP Statistics

If true, the NtpPlatformService reports whatever information it can about its operation. To access these statistics with the station opened in Workbench, right-click the NtpPlatformServiceQnx and select Views→ SpyRemote. Keep in mind that the ntpd is a QNX process; thus Niagara has no control over what it reports.

Ntp Platform Service Editor Qnx time servers

Each entry in the time servers list in the Ntp Platform Service Editor Qnx specifies a server to which the host’s clock will be synced when the service is Enabled (true), and “Sync Local Clock to NTP” is also true. These servers are not used if either of these properties is false.

Controls below the list allow you to add ⊕ and delete ⊖ servers, as well as reorder up ▲ or down ▼ (to establish priority order, highest at top). Fields for each time server includes the following:

- Address

Fully qualified domain name, IP address, or host files alias for the NTP time server.

- Peer Mode

Peer mode to use with the server, as either server or peer (symmetricActive).

- Burst

This is False by default. If true, when server is reachable, upon each poll, a burst of eight packets are sent, instead of the usual one packet. Spacing between the first and second packets is about 16 seconds to allow a modem call to complete, while spacing between remaining packets is about 2 seconds.

- Preferred

If true, designates a server as preferred over others for synchronization. Note also that priority order (top highest, bottom lowest) is also evaluated if multiple servers are entered.

- Min. Poll

Minimum poll interval for NTP messages, from 4 to 16. Note units are in “log-base-two seconds,” or 2 to the power of n seconds (NTP convention), meaning from 2 to the 4th (16 seconds) to 2 to the 16th (65,536 seconds).

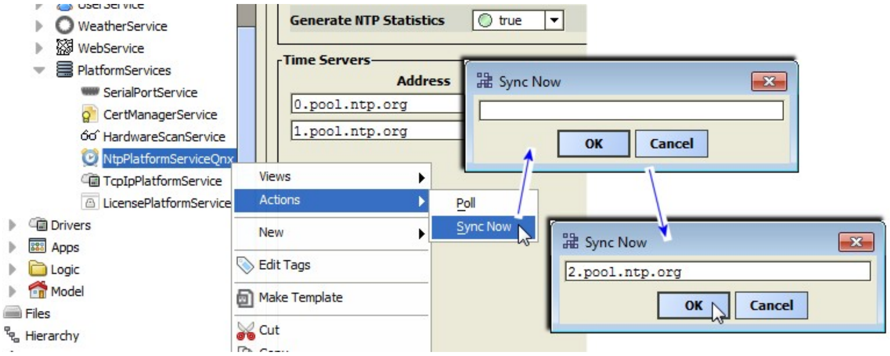
- Max. Poll

Maximum poll interval for NTP messages, from 10 to 17. Note units are in “log-base-two seconds,” or 2 to the power of n seconds (NTP convention), meaning from 2 to the 10th (1,024 seconds) to 2 to the 17th (131,072 seconds).

Sync Now action

In addition to the “Poll” action present on any NtpPlatformService, the NtpPlatformServiceQnx component has an additional “Sync Now” action.

Figure 93 Sync Now action on NtpPlatformServiceQnx



Generate NTP Statistics: true

Time Servers — Address: 0.pool.ntp.org, 1.pool.ntp.org

Sync Now: 2.pool.ntp.org

As shown here, this action produces a popup Sync Now dialog, which is blank.

To use, type in the fully qualified domain name of a public NTP server (as shown above), or the IP address of any accessible NTP server, and then click OK.

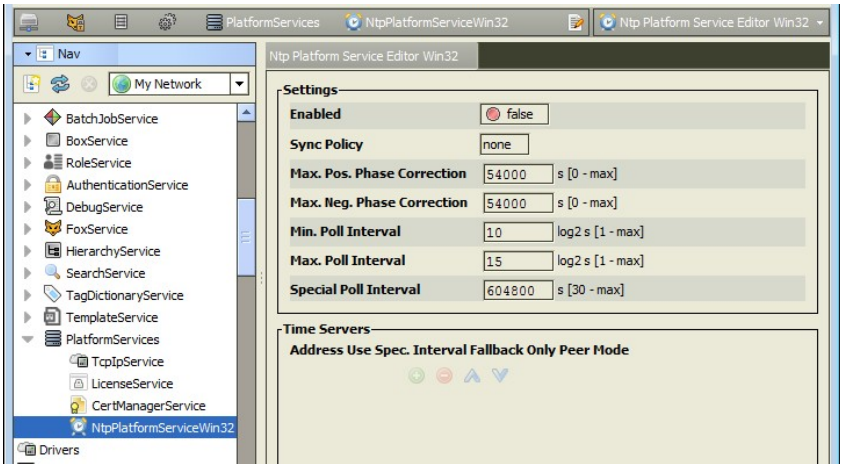
To verify, look for a related entry in the station’s spy “platform diagnostics” log. Do this in Workbench by right-clicking the station, then selecting Spy→ platform diagnostics→ log or from the File menu, File→Open ord (Ctrl + L) and enter:

ip:EC-BOS_IP_address|fox:|spy:/platform diagnostics/log

About the Ntp Platform Service Editor Win32

An example Ntp Platform Service Editor Win 32 is shown below. This is the default view for the NtpPlatformService on a Windows-based (Win32 or Win64) host.

Figure 110: Ntp Platform Service Editor Win32



Settings

Enabled	false	
Sync Policy	none	
Max. Pos. Phase Correction	54000	s [0 - max]
Max. Neg. Phase Correction	54000	s [0 - max]
Min. Poll Interval	10	log2 s [1 - max]
Max. Poll Interval	15	log2 s [1 - max]
Special Poll Interval	604800	s [30 - max]

Time Servers

Address	Use Spec. Interval	Fallback Only	Peer Mode

This dialog provides access to some of the key settings of the Windows Time service (W32Time) on the host platform. As in all Ntp Platform Service Editors, there, there are two main areas: Settings at top, Time Servers at bottom.

Note:

Settings are only a small subset of those possible to configure. For more fine-grained tuning of the time service, Windows registry settings can be set according to Microsoft’s latest instructions. Visit the Microsoft tech support site for more information on a particular Windows OS.

NTP port/firewall considerations

On any host, NTP requires the use of UDP port 123, this port is not configurable. On a JACE platform this is not an issue.

However, on a Windows host platform, in addition to configuring NTP using Windows native tools, typically you need to make the necessary firewall exception or “iptable” entry to allow UDP port 123 traffic. Otherwise, NTP time synchronization can fail because of firewall-blocked messages.

CHAPTER 3 PLATFORM COMPONENT GUIDES

The following topics are covered in this chapter:

- platCrypto-CertManagerService
- platform-DaemonSecureSession
- platDataRecovery-DataRecoveryService
- Components in platform module
- Components in platHwScan
- Components in platPower module
- Components in platSerialQnx module

platCrypto-CertManagerService

The component is a platCrypto platform service of any Niagara 4 station. It has few visible properties, but provides a default Certificate Management view, that is equivalent to that same-named platform view.

The Certificate Management view provides the means to import and export signed certificates (for TLS secure connections) into the platform’s key and trust stores, and to perform other related functions.

platform-DaemonSecureSession

This platCrypto component represents a secure platform connection to a host made in Workbench in the Nav tree view.

The platform session icon (🔒) is labeled Platform , shows a small padlock, and is directly under the host for the platform session is in progress. To support such connections, the host must have its Platform TLS Settings enabled (accessed in its Platform Administration view).

As in a regular (un-encrypted) platform connection, the default view is the Nav Container View, which provides a table of all the various platform views.

platDataRecovery-DataRecoveryService

This component (💾) in the platDataRecovery module automatically creates and manages buffers in a controller’s available SRAM (Static Random Access Memory), allowing a controller to function without a battery.

The controllers with integral SRAM include: JACE-8000, JACE-3E, JACE-6E, JACE-603, JACE-645) as well as a JACE-6 and JACE-7 with an installed SRAM option card.

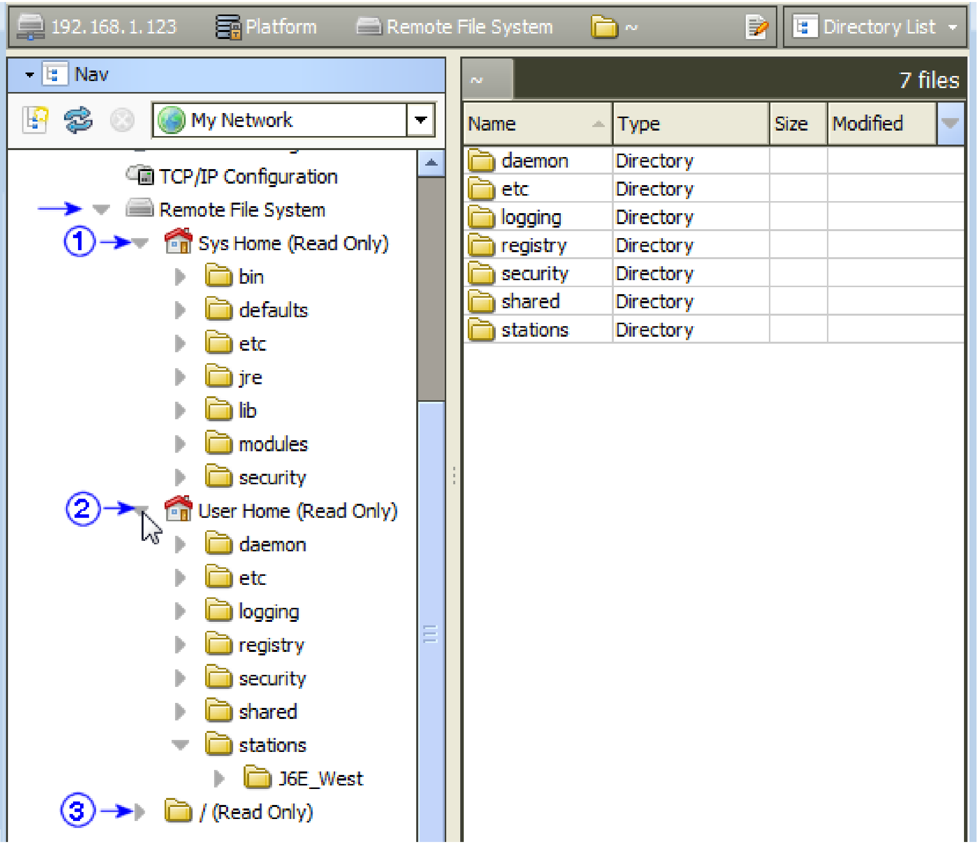
Some SRAM-equipped controllers support a backup battery with the addition of an optional NiMH onboard battery pack, or an external 12V sealed lead-acid battery. For these controllers, both the DataRecoveryService and PowerMonitorService run in the station’s PlatformServices container, operating independently or in unison, as configured.

Components in platform module

platform-DefaultDaemonFileSpace

This component (▭) is in the program module. The Remote File System view is one of several platform views. It provides a read-only view of the remote platform’s file system.

Figure 111: Remote File System for JACE controller platform



Name	Type	Size	Modified
daemon	Directory		
etc	Directory		
logging	Directory		
registry	Directory		
security	Directory		
shared	Directory		
stations	Directory		

The Remote File System (DefaultDaemonFileSpace) represents the files accessible for read-only access when platform-connected to a remote host. As needed, you can expand folders and examine and/or copy files to your local computer. Included in the Nav tree under the Remote File System are main nodes for the following:

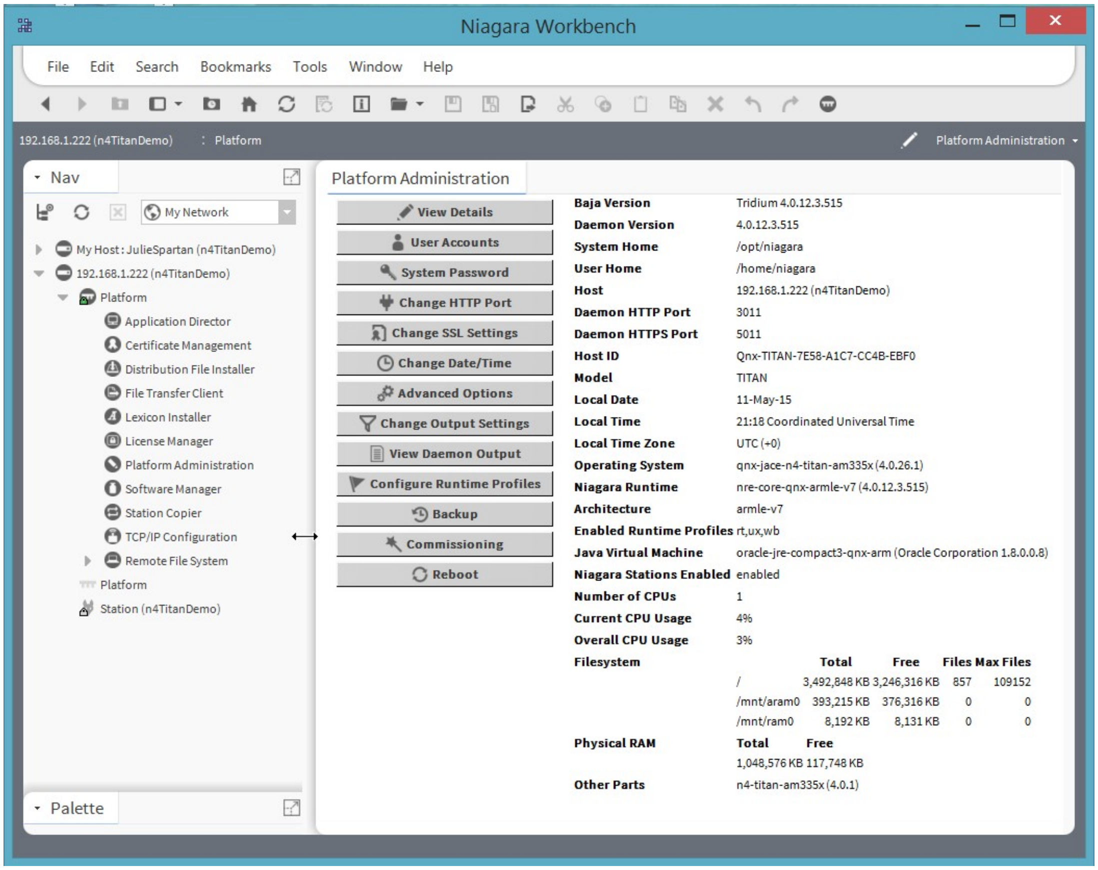
- The system home (Sys Home) root folder, under which all installation/runtime files are installed.
- The user home (User Home) root folder for the platform daemon, under which all configuration files are stored.
- (JACE controllers only) The root folder for the entire file system, with browse capability.

To edit or write files on the remote Niagara platform, you must use the platform File Transfer Client view.

platform-DaemonSession

This component represents a platform connection to a host made in Workbench. To access this component, expand My Host→Platform and double-click Platform Administration.

Figure 112: Platform Administration



Baja Version	Tridium 4.0.12.3.515
Daemon Version	4.0.12.3.515
System Home	/opt/niagara
User Home	/home/niagara
Host	192.168.1.222 (n4TitanDemo)
Daemon HTTP Port	3011
Daemon HTTPS Port	5011
Host ID	Qnx-TITAN-7E58-A1C7-CC4B-EBF0
Model	TITAN
Local Date	11-May-15
Local Time	21:18 Coordinated Universal Time
Local Time Zone	UTC (+0)
Operating System	qnx-jace-n4-titan-am335x (4.0.26.1)
Niagara Runtime	nre-core-qnx-armle-v7 (4.0.12.3.515)
Architecture	armle-v7
Enabled Runtime Profiles	rt,ux,wb
Java Virtual Machine	oracle-jre-compact3-qnx-arm (Oracle Corporation 1.8.0.0.8)
Niagara Stations Enabled	enabled
Number of CPUs	1
Current CPU Usage	4%
Overall CPU Usage	3%

Filesystem		**Total**	**Free**	**Files**	**Max Files**
	/	3,492,848 KB	3,246,316 KB	857	109152
	/mnt/aram0	393,215 KB	376,316 KB	0	0
	/mnt/ram0	8,192 KB	8,131 KB	0	0

Physical RAM	**Total**	**Free**
	1,048,576 KB	117,748 KB

Other Parts	n4-titan-am335x (4.0.1)

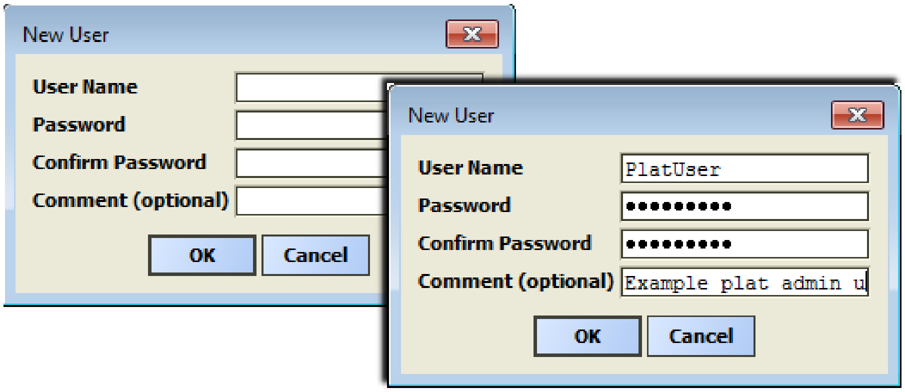
In the Nav tree view, the DaemonSession icon (▤) is labeled Platform, and is directly under the host for which the platform session is in progress.

The default view is the Nav Container View, which provides a list of all the platform views.

New User window

Clicking New User opens the New User window.

Figure 97 Example of New User window after typing user name, password, and comment



User Name	PlatUser
Password	•••••••••
Confirm Password	•••••••••
Comment (optional)	Example plat admin u

Follow these basic guidelines to create strong passwords:

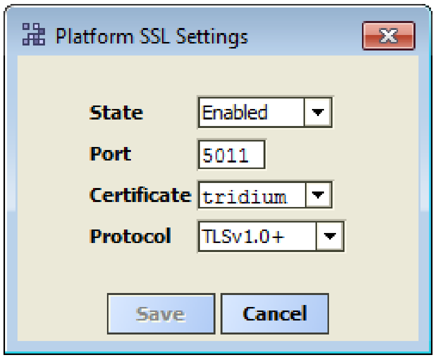
- Use both upper and lower case.
- Include numeric digits.
- Include special characters.
- 🛇 Do not use dictionary words.
- 🛇 Do not use your company name.
- 🛇 Do not make your password the same as your user name.
- 🛇 Do not use common numbers like telephone numbers, addresses, your birthday, and so on.

Property	Value	Description
User Name	text	A maximum of 14 alphanumeric characters (a - z, A - Z, 0 - 9), where the first character must be alphabetic, and the following characters either alphanumeric or underscore (_).
Password	A minimum of 10 characters using: at least one UPPER CASE letter, at least one lower case letter, and at least one digit (numeral)	Two fields allow you to create and verify a strong password. The password must match in both password fields. The characters you enter display as asterisks (*). An error popup reminds you if you attempt to enter a password that does not meet minimum rules.
Comment	Optional text: maximum of 64 alphanumeric characters, with these also allowed: - = + ( ) @. _	As of now, comment text cannot be re-edited after adding it to a user account.

Change TLS Settings window

This window provides access to the primary TLS settings.

Figure 113: Platform TLS Settings with default values (enabled)



State: Enabled

Port: 5011

Certificate: tridium

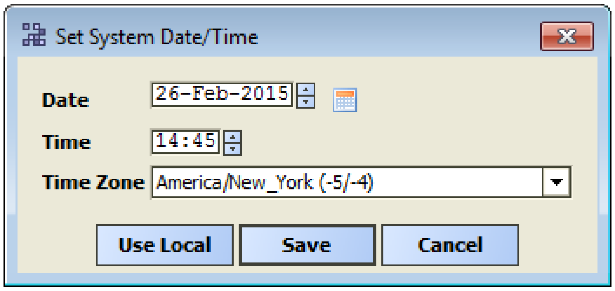
Protocol: TLSv1.0+

Properties	Value	Description
State	Disabled, Enabled, or Tls Only	Specifies how Workbench clients connect to this host's platform daemon. • Disabled: Secure platform connections not possible (only regular platform connections). • Enabled: Secure platform connections permitted, as well as regular platform connections. • Tls Only: Only secure platform connections are allowed. Any attempt to connect without security goes unresolved (errors out). This state is reflected among the properties listed on the main Platform Administration view, as "Platform TLS Support" state. ***Note:*** The Tls Only option provides the best security. In Niagara 4, all platforms support secure (TLS) platform connections, even if a freshly "clean disted" controller.
Port	four-digit number (default is 5011)	Identifies the software port monitored by the platform daemon for a secure platform connection. This is different than the default HTTP port (3011) for a regular platform connection that is not secure. ***Note:*** • If there is a firewall on the host (or its network), before changing this port, make sure that the firewall will allow traffic to the new port.
Certificate	text (default is the tridium self-signed certificate)	The alias for the server certificate in the platform's key store to use for any platform TLS connection. The default is automatically created when Niagara is first loaded. If another certificate has been imported in the platform's key store, use the drop-down control to select it instead. Certificates on the platform are managed via the platform Certificate Management view.
Protocol	TLSv1.0+ — (default) Includes TLS versions 1.0, 1.1, and 1.2, providing the most flexibility; TLSv1.1+ — Only TLS versions 1.1 or 1.2 are accepted; TLSv1.2 — Only TLS version 1.2 is accepted.	Defines the minimum TLS (Transport Layer Security) protocol version that the platform daemon's secure server accepts to negotiate with a client for a secure platform connection. During the handshake, the server and client agree on which protocol to use.

Set System Date/Time window

This window configures the remote platform’s date and time.

Figure 114: Set System Date/Time window



Date 26-Feb-2015

Time 14:45

Time Zone America/New_York (-5/-4)

Field	Description
Date	Defines a day-month-year.
Time	Always displays in 24-hour format.
Time Zone	Each time zone provides a text description, and in parenthesis the hour offset from UTC (and if daylight savings time is used) the offset plus daylight savings. For example: America/New_ York (-5,-4).

platform-LicenseDatabaseTool

The LicenseDatabaseTool (Local License Database) represents your Workbench PC’s “local license database.” The default view is the Workbench License Manager, which allows you to manage locally-stored licenses.

platform-LicensePlatformService

The LicensePlatformService provides station access to the host platform’s license(s) and certificate(s). This service is found under the running station’s PlatformServices container. From the default plugin (view), you can perform the same operations as from the License Manager view using a platform connection.

platform-NtpPlatformServiceQnx

The NtpPlatformServiceQNX is the Niagara interface to the NTP (Network Time Protocol) daemon of the QNX OS running on a controller. If enabled, it provides client and server support for NTP. The default view of this platform service is the Ntp Platform Service Editor Qnx plugin, in which you can adjust a few settings, as well as specify time servers.

platform-NtpPlatformServiceWin32

The NtpPlatformServiceWin32 is the Niagara 4 interface to the Windows Time service (W32Time) on a Win32-based platform’s Windows OS. This Windows service uses the SNTP (Simple Network Time Protocol) to synchronize to one or more designated time servers. The default view of this platform service is the Ntp Platform Service Editor Win32 plugin, in which you can adjust a few settings of the Windows Time service, including identifying NTP time servers. For more details, see the section, “About the NtpPlatformService”.

platform-PlatformAlarmSupport

PlatformAlarmSupport is a container slot that appears for each alarm value under a Platform Service, such as the PowerMonitorService for many JACE controllers.

For a JACE platform, examples of PlatformAlarmSupport components include:

- Battery Alarm Support: To configure how “low battery level” alarms are handled in the station.
- Power Alarm Support: To configure how “AC power loss” alarms are handled in the station.

Properties under each PlatformAlarmSupport container are used to designate the station’s Alarm Class to be used, and also to populate the alarm record when the specific alarm occurs. These properties work in the same fashion as those in an alarm extension for any control point.

platform-PlatformServiceContainer

PlatformServiceContainer (PlatformServices) provides a container for a station's PlatformService instances. The Platform Service Container Plugin is its primary view. The PlatformServiceContainer is available when online with any running station, under its Config, Services folder.

platform-SystemPlatformServiceQnxJavelina

SystemPlatformServiceQnxJavelina (SystemService) is the QNX implementation of SystemPlatformService in a station running on a JVLN-based (JACE-700) controller.

platform-SystemPlatformServiceQnxNpm6xx

SystemPlatformServiceQnx (SystemService) is the QNX implementation of SystemPlatformService in a station running on a JACE controller.

platform-SystemPlatformServiceWin32

SystemPlatformServiceWin32 (SystemService) is the Win32 implementation of SystemPlatformService.

platform-TcpIpPlatformService

TcpIpPlatformService provides station access to the host platform’s TCP/IP settings. This service is found under the running station’s PlatformServiceContainer. From the default plugin (view), you can perform the same operation as from the TCP/IP Configuration view using a platform connection. For more details see the section, “TCP/IP Configuration”. If a Win32 host and the platform authentication setting labeled “Stations allow stations to have admin access to platform daemon” is disabled, TCP/IP properties in this view are read-only.

Components in platHwScan

platHwScan-HardwareScanService

The Hardware Scan Service is an available platform service on a JACE station, providing that the JACE platform has the platHwScan module installed.

To function correctly, the appropriate platHwScanType module also needs to be installed on the JACE. Otherwise, the default Hardware Scan Service View will simply display:

Note:

Jar file platHwScanType is required to support this platform. The following table lists the appropriate platHwScanType modules:

Controller Series	platHwScanType module
JACE-6E, JACE-6, JACE-3E	platHwScanNpm
JACE-7 (700)	platHwScanJvln
JACE-603 (JACE-403 with retrofit board)	platHwScanJ603
JACE-645 (JACE-545 with retrofit board)	platHwScanJ645
JACE-602 Express (J-602-XPR or M2M)	platHwScanXpr
JACE-8000	platHwScanTitan

This default Hardware Scan Service View provides a diagram of the controller that shows its communication ports and other features (including, if applicable, installed communication options such as modules or cards). The diagram has callouts to a table that explains each item’s location, description (such as COM2), port type, usage, and status.

Components in platPower module

platPower-ExternalSlaBattery

ExternalSlaBattery is one of two “Battery” slots in the JavelinaBatteryPlatformService in a JACE-700 (JACE-7 series) controller station’s PlatformServices container. This slot indicates the host JACE platform can use an optional, sealed-lead acid (SLA) battery, in addition to the onboard NiMH backup battery.

platPower-JavelinaBatteryPlatformService

JavelinaBatteryPlatformService (PowerMonitorService) applies to a station running in a JACE-700 (JACE-7 series) controller. It can monitor primary power status and backup battery levels in both the onboard 12V NiMH battery and an optional 12V sealed-lead acid (SLA) battery. In addition, it can monitor alarm contacts of an external, customer-supplied UPS, if enabled and wired to the two corresponding onboard contact inputs (CIs) of the controller. Note the JACE-7 controller has three onboard CIs, with the intended use for UPS AC power lost, UPS low battery, and (door) tamper switch.

Note:

The tamper switch CI on the JACE-7 controller is enabled/monitored by two properties in the PowerMonitorService's parent PlatformServices Container).

Configuration properties in this PowerMonitorService allow changing the shutdown delay time, and also specifying whether external equipment is connected (12V SLA battery, UPS). Separate alarm source configuration properties are available for all five types of alarms (low NiMH battery level, low SLA battery level, primary power lost, UPS AC power lost, UPS low battery).

Typically, support is enabled and configured at JACE commissioning time.

platPower-NimhBattery

NimhBattery is a "Battery" container slot under the PowerMonitorService in a JACE-700 (JACE-7 series) station's PlatformServices container. This slot indicates the host JACE platform uses a nickel-metal hydride (NiMH) battery. Included are two status properties that show the current "State" (Idle, Charging, Discharging, Unknown) and "Charge Time Left" (in hours and minutes, if state is charging).

platPower-Npm2NimhBattery

This slot indicates the host JACE platform uses a nickel-metal hydride (NiMH) battery. Included are two status properties that show the current "State" (Idle, Charging, Discharging, Unknown) and "Charge Time Left" (in hours and minutes, if state is charging). This slot is located under the PowerMonitorService or PlatformServices container depending on controller type.

This slot also appears in the NpmDualBatteryPlatformService ("dual battery" PowerMonitorService) of a JACE that is capable and enabled for dual battery support.

platPower-NpmDualBatteryPlatformService

NpmDualBatteryPlatformService (PowerMonitorService) applies to a station running in a JACE platform that is capable and enabled for "dual battery" support. It is used to monitor primary power status and backup battery levels in both the onboard NiMH battery as well as the optional sealed-lead acid (SLA) battery. A few configuration parameters allow changing the shutdown delay time, as well as alarm source configuration for all three types of alarms (low NiMH battery level, low SLA battery level, primary power lost).

Typically, support is enabled and configured at JACE commissioning time.

platPower-NpmExternalSlaBattery

NpmExternalSlaBattery is one of two "Battery" slots under the NpmDualBatteryPlatformService in a "dual battery enabled" JACE's station's PlatformServices container. This slot simply indicates the host JACE platform can use an optional, sealed-lead acid (SLA) battery, in addition to the onboard NiMH backup battery.

platPower-PowerMonitorPlatformServiceQnx

PowerMonitorPlatformServiceQnx (PowerMonitorService) is used to monitor the primary power status and backup battery level in many JACE controllers. A few configuration parameters allow changing the shut-down delay time, as well as alarm source configuration for both types of alarms (low battery level, primary power lost).

This PowerMonitorService is found under the PlatformServices container in a station running on many JACE controllers except for those models that are capable and/or enabled for "dual battery" support.

Typically, support is enabled and configured at JACE commissioning time.

Components in platSerialQnx module

- SerialPortPlatformServiceQnx
- SerialPortQnx

platSerialQnx-SerialPortPlatformServiceQnx

SerialPortPlatformServiceQnx is the station’s interface to the platform’s serial port configuration, such as used by a JACE-3,-6,-7 series host. This service is found under the running station’s PlatformServices container as the SerialPortService.

platSerialQnx-SerialPortQnx

SerialPortQnx contains properties that describe how a serial port (RS-232 or RS-485) on a JACE controller is being used in software as COMn. Each one is a child of that JACE’s SerialPortService (SerialPortPlatformServiceQnx). Properties are the following:

- Owner: The driver network or function currently associated with that COM port, for example, “NrioNetwork”, “dialup”, “none”, “ModbusAsyncNetwork”, or “dbgjmpr” (latter indicated for COM1 when “serial shell” jumper is installed on JACE).
- Os Port Name: How the port is known to the QNX OS and associated low-level drivers.
- Port Index: Unique serial port index number, starting with 1 for COM1.

CHAPTER 4 PLATFORM PLUGIN GUIDES

The following topics are covered in this chapter:

- Plugin Reference Summary
- Plugins in platCrypto
- Plugins in platDaemon module
- Plugin in platDataRecovery
- Plugins in platform module
- Plugins in platHwScan
- Plugins in platPower

There are many ways to view plugins (views). One way is directly in the tree. In addition, you can right-click on an item and select one of its views. Plugins provide views of components.

Access the following summary descriptions on any plugin by selecting Help→ On View (F1) from the menu, or by pressing F1 while the view is open.

Plugin Reference Summary

Summary information is provided on views in the following modules:

- platCrypto
- platDaemon
- platDataRecovery
- platform
- platHwScan
- platPower

Plugins in platCrypto

platCrypto-CertManagerView

This view is a platform view on any Niagara host. It is also the default view of the CertManagerService under a station's PlatformServices. The Certificate Management view allows you to create digital certificates and Certificate Signing Requests (CSRs). You use this view to import and export keys and certificates to and from the Workbench, platform and station stores. You access this view, via Tools→ Certificate Management. Also included is a related Tools Certificate Signer Tool view.

You use this view to manage PKI (Public Key Infrastructure) and self-signed digital certificates to secure communication within Niagara network. Certificates secure TLS connections to this host.

Certificate Management

The Certificate Management view has four tabs:

- User Key Store
- System Trust Store
- User Trust Store
- Allowed Hosts

User Key Store tab

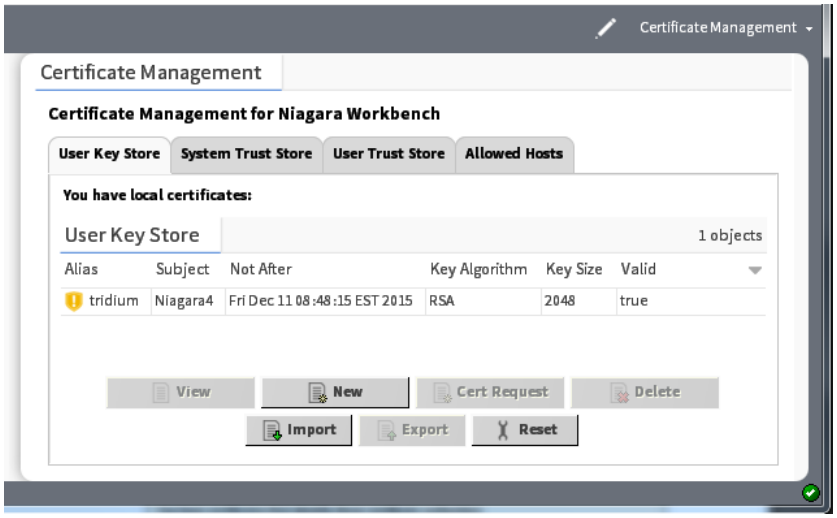
The User Key Stores contain server certificates and self-signed certificates with their matching keys. Each certificate has a pair of unique private and public encryption keys for each platform. A User Key Store supports the server side of the relationship by sending one of its signed server certificates in response to a client (Workbench, platform or station) request to connect.

If there are no certificates in a User Key Store when the server starts, such as when booting a new platform or station, the platform or station creates a default, self-signed certificate. This certificate must be approved as an allowed host. This is why you often see the certificate popup when opening a platform or station.

Default self-signed certificates have the same name in each User Key Store (tridium); however, each certificate is unique for each instance.

Clicking the New and Import buttons also adds certificates to the User Key Store.

Figure 115: Example of a Key Store



Certificate Management for Niagara Workbench

You have local certificates:

Alias	Subject	Not After	Key Algorithm	Key Size	Valid
tridium	Niagara4	Fri Dec 11 08:48:15 EST 2015	RSA	2048	true

Name	Value	Description
Alias	text	A short name used to distinguish certificates from one another in the Key Store. This property is required. It may identify the type of certificate (root, intermediate, server) location or function. This name does not have to match when comparing the server certificate with the CA certificate in the client's Trust Store.
Issued By	text	Identifies the entity that signed the certificate.
Subject	text	Specifies the Distinguished Name, the name of the company that owns the certificate.
Not Before	date	Specifies the date before which the certificate is not valid. This date on a server certificate should not exceed the Not Before date on the root CA certificate used to sign it.
Not After	date	Specifies the expiration date for the certificate. This date on a server certificate should not exceed the Not After date on the root CA certificate used to sign it.
Key Algorithm	text	Refers to the cryptographic formula used to calculate the certificate keys.
Key Size	number	Specifies the size of the keys in bits. Four key sizes are allowed: 1024 bits, 2048 bits (this is the default), 3072 bits, and 4096 bits. Larger keys take longer to generate but offer greater security.
Signature Algorithm	formula text	Specifies the cryptographic formula used to sign the certificate.
Signature Size	KB	Specifies the size of the signature.
Valid		Specifies certificate dates.
Self Signed	text	Read-only. Indicates that the certificate was signed with its own private key.

User Key Store buttons

Button Name	Description
View	Displays details for the selected item
New	Opens the window used to create the entity you are working on.
Cert Request	Opens a Certificate Request window, which is used to create a Certificate Signing Request (CSR).
Delete	Removes the selected record from the database.
Import	Adds an imported item to the database.
Export	Saves a copy of the selected record to the hard disk. For certificates, the file extension is .pem.
Reset	Deletes all certificates in the User Key Store and creates a new default certificate. It does not matter which certificate is selected when you click Reset. ***Note:*** • 🛇 Do not reset without considering the consequences. The Reset button facilitates creating a new key pair (private and public keys) for the entity, but may disable connections if valid certificates are already in use. Export all certificates before you reset.

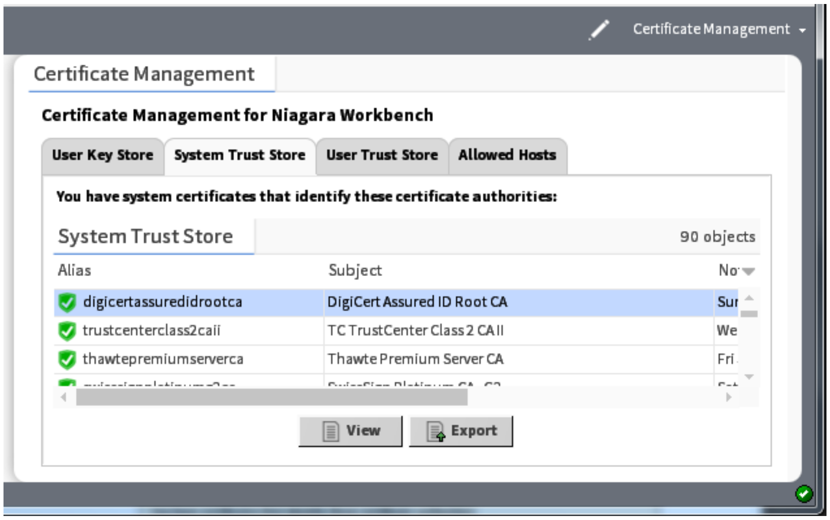
Trust Store tabs

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

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

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

Figure 116: Example of a Trust Store



Certificate Management

Certificate Management for Niagara Workbench

You have system certificates that identify these certificate authorities:

System Trust Store — 90 objects

Alias	Subject	No
digicertassuredidrootca	DigiCert Assured ID Root CA	Sur
trustcenterclass2caii	TC TrustCenter Class 2 CA II	We
thawtepremiumserverca	Thawte Premium Server CA	Fri

Trust Store columns

Name	Description
Alias	A short name used to distinguish certificates from one another in the Key Store. This property is required. It may identify the type of certificate (root, intermediate, server), location or function. This name does not have to match when comparing the server certificate with the CA certificate in the client's Trust Store.
Issued By	Identifies the entity that signed the certificate.
Subject	Specifies the Distinguished Name, the name of the company that owns the certificate.
Not Before	Specifies the date before which the certificate is not valid. This date on a server certificate should not exceed the Not Before date on the root CA certificate used to sign it.
Not After	Specifies the expiration date for the certificate. This date on a server certificate should not exceed the Not After date on the root CA certificate used to sign it.
Key Algorithm	Refers to the cryptographic formula used to calculate the certificate keys.
Key Size	Specifies the size of the keys in bits. Four key sizes are allowed: 1024 bits, 2048 bits (this is the default), 3072 bits, and 4096 bits. Larger keys take longer to generate but offer greater security.

Name	Description
Signature Algorithm	Specifies the cryptographic formula used to sign the certificate.
Signature Size	Specifies the size of the signature.
Valid	Specifies certificate dates.
Self Signed	Read-only. Indicates that the certificate was signed with its own private key.

Trust Store buttons

Button Name	Description
View	Displays details for the selected item
Delete	Removes the selected record from the database.
Import	Adds an imported item to the database.
Export	Saves a copy of the selected record to the hard disk. For certificates, the file extension is .pem.

Allowed Hosts tab

The Allowed Hosts tab contains security exemptions for the currently open platform. These are the certificates (signed or self-signed) received by a client from a server (host) that could not be validated against a root CA certificate in a client Trust Store. Whether you approve or reject the certificate, the system lists it in the Allowed Hosts list.

To be authentic, a root CA certificate in the client’s System or User Trust Store must be able to validate the server certificate’s signature, and the Subject of the root CA certificate must be the same as the Issuer of the server certificate.

Allowing exemptions makes it possible for a human operator to override the lack of trust between a server and client when the human user knows the server can be trusted.

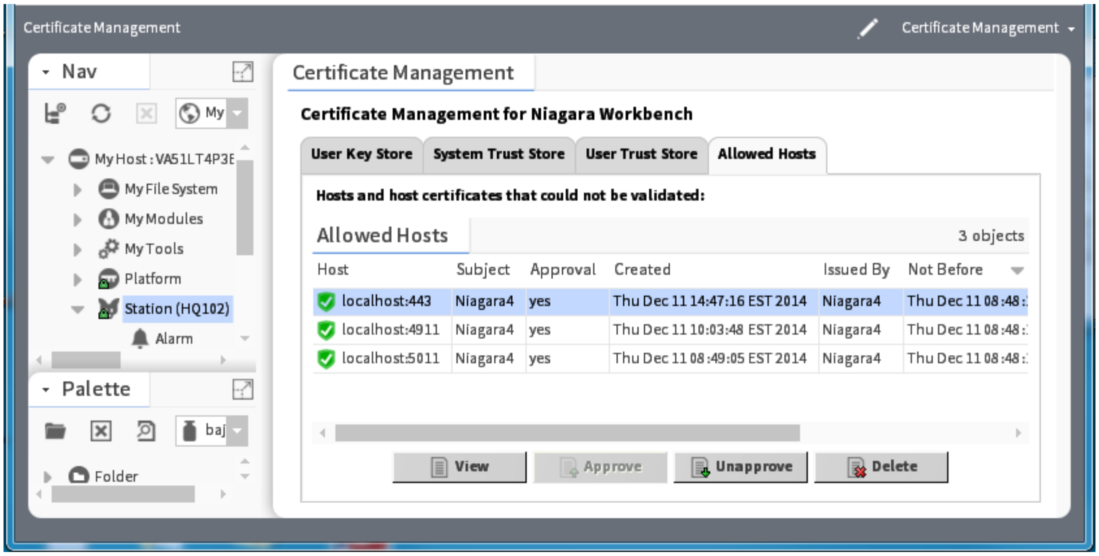
If this is Workbench to station connection, the system prompts you to approve the host exemption. Workbench challenges server identity at connection for unapproved hosts and, unless specific permission is granted, prohibits communication. Once permission is granted, future communication occurs automatically (you still have to log in). Both approved and unapproved hosts remain in this list until deleted.

If this is a station to station connection, and there is a problem with the certificates, the connection fails silently. There is no prompt to approve the host exemption. However, the last failure cause in the station (expand the station ClientConnection under NiagaraNetwork) reports the problem.

The approved host exemption in the Allowed Hosts list is only valid when a client connects to the server using the IP address or domain name that was used when the system originally created the exemption. If you use a different IP address or domain name to connect to the server, you will need to approve an updated exemption. The same is true if a new self-signed certificate is generated on the host.

Allowed Hosts columns

Figure 117: Example of an Allowed Hosts list



Certificate Management for Niagara Workbench

Hosts and host certificates that could not be validated:

Allowed Hosts 3 objects

Host	Subject	Approval	Created	Issued By	Not Before
localhost:443	Niagara4	yes	Thu Dec 11 14:47:16 EST 2014	Niagara4	Thu Dec 11 08:48:
localhost:4911	Niagara4	yes	Thu Dec 11 10:03:48 EST 2014	Niagara4	Thu Dec 11 08:48:
localhost:5011	Niagara4	yes	Thu Dec 11 08:49:05 EST 2014	Niagara4	Thu Dec 11 08:48:

Name	Value	Description
Host	text	Specifies the server, usually an IP address.
Subject	text	Specifies the Distinguished Name, the name of the company that owns the certificate.
Approval	Yes or No	Value: This specifies the servers within the network to which a client may connect. If approval is set to no, the system does not allow the client to connect.
Created	date	Identifies the date the record was created.
Issued By	text	Identifies the entity that signed the certificate.
Not Before	date	Specifies the date before which the certificate is not valid. This date on a server certificate should not exceed the Not Before date on the root CA certificate used to sign it.
Not After	date	Specifies the expiration date for the certificate. This date on a server certificate should not exceed the Not After date on the root CA certificate used to sign it.
Key Algorithm	text	Refers to the cryptographic formula used to calculate the certificate keys.
Key Size	number	Specifies the size of the keys in bits. Four key sizes are allowed: 1024 bits, 2048 bits (this is the default), 3072 bits, and 4096 bits. Larger keys take longer to generate but offer greater security.
Signature Algorithm	formula text	Specifies the cryptographic formula used to sign the certificate.
Signature Size	number	Specifies the size of the signature.
Valid	date	Specifies certificate dates.

Allowed Hosts buttons

Name	Value	Description
View	button	Displays details for the selected item
Approve	Yes or No	Designates the server as an allowed host.
Unapprove	Yes or No	Does not allow connection to this server host. The system terminates any attempted communication.

Plugins in platDaemon module

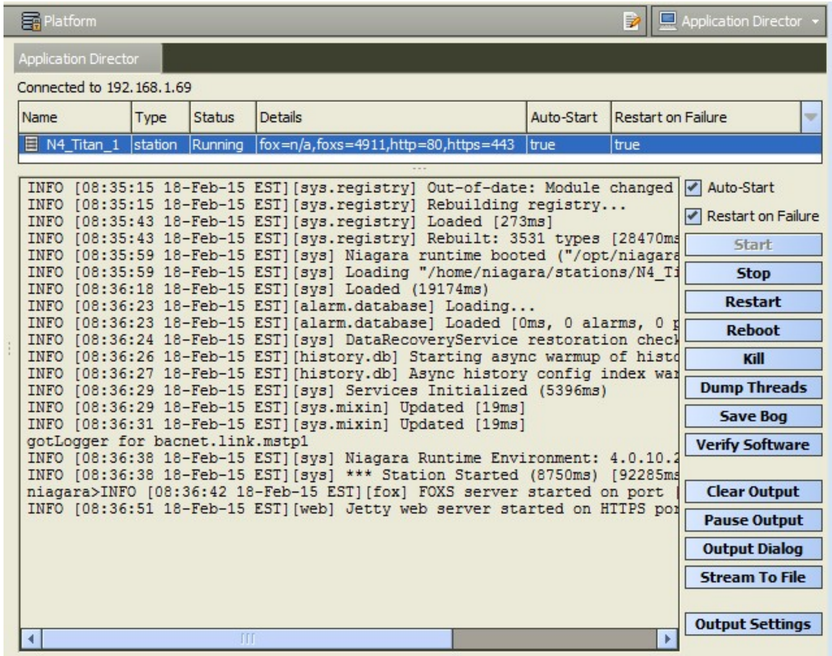
This section covers the following topics:

- Application Director
- Certificate Management
- Distribution File Installer
- Distribution View
- File Tranfer Client
- Lexicon Installer
- License Manager
- Software Manager
- Software View
- Platform Administration
- Station Copier
- TCP/IP Configuration

platDaemon-ApplicationDirector

The Application Director view interfaces to each station whether it is running or not.

Figure 118: Application Director view, looking at Niagara station



Connected to 192.168.1.69

Name	Type	Status	Details	Auto-Start	Restart on Failure
N4_Titan_1	station	Running	fox=n/a,foxs=4911,http=80,https=443	true	true

```
INFO [08:35:15 18-Feb-15 EST][sys.registry] Out-of-date: Module changed
INFO [08:35:15 18-Feb-15 EST][sys.registry] Rebuilding registry...
INFO [08:35:43 18-Feb-15 EST][sys.registry] Loaded [273ms]
INFO [08:35:43 18-Feb-15 EST][sys.registry] Rebuilt: 3531 types [28470ms
INFO [08:35:59 18-Feb-15 EST][sys] Niagara runtime booted ("/opt/niagara
INFO [08:35:59 18-Feb-15 EST][sys] Loading "/home/niagara/stations/N4_Ti
INFO [08:36:18 18-Feb-15 EST][sys] Loaded (19174ms)
INFO [08:36:23 18-Feb-15 EST][alarm.database] Loading...
INFO [08:36:23 18-Feb-15 EST][alarm.database] Loaded [0ms, 0 alarms, 0 p
INFO [08:36:24 18-Feb-15 EST][sys] DataRecoveryService restoration check
INFO [08:36:26 18-Feb-15 EST][history.db] Starting async warmup of histo
INFO [08:36:27 18-Feb-15 EST][history.db] Async history config index war
INFO [08:36:29 18-Feb-15 EST][sys] Services Initialized (5396ms)
INFO [08:36:29 18-Feb-15 EST][sys.mixin] Updated [19ms]
INFO [08:36:31 18-Feb-15 EST][sys.mixin] Updated [19ms]
gotLogger for bacnet.link.mstp1
INFO [08:36:38 18-Feb-15 EST][sys] Niagara Runtime Environment: 4.0.10.2
INFO [08:36:38 18-Feb-15 EST][sys] *** Station Started (8750ms) [92285ms
niagara>INFO [08:36:42 18-Feb-15 EST][fox] FOXS server started on port
INFO [08:36:51 18-Feb-15 EST][web] Jetty web server started on HTTPS por
```

☑ Auto-Start
☑ Restart on Failure

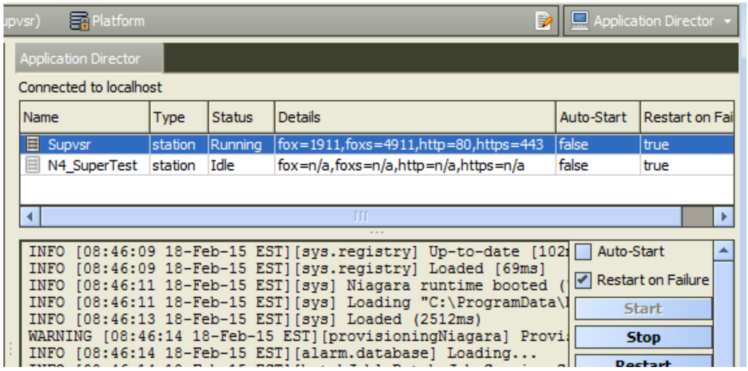
The Application Director is split into three main areas:

- Installed applications— on top
- Application output— main area. Related are log levels defined for the station.
- Application and output controls— right-side checkboxes and buttons

Note:

In the Application Director for any JACE, the installed applications area should show (at most) only one station, as shown above. However, the Application Director for a Windows platform (Supervisor, or engineering workstation) may show more than one station, as shown below.

Figure 119: Application Director for Supervisor host showing multiple stations



Connected to localhost

Name	Type	Status	Details	Auto-Start	Restart on Fai
Supvsr	station	Running	fox=1911,foxs=4911,http=80,https=443	false	true
N4_SuperTest	station	Idle	fox=n/a,foxs=n/a,http=n/a,https=n/a	false	true

```
INFO [08:46:09 18-Feb-15 EST][sys.registry] Up-to-date [102
INFO [08:46:09 18-Feb-15 EST][sys.registry] Loaded [69ms]
INFO [08:46:11 18-Feb-15 EST][sys] Niagara runtime booted (
INFO [08:46:11 18-Feb-15 EST][sys] Loading "C:\ProgramData\
INFO [08:46:13 18-Feb-15 EST][sys] Loaded (2512ms)
WARNING [08:46:14 18-Feb-15 EST][provisioningNiagara] Provi
INFO [08:46:14 18-Feb-15 EST][alarm.database] Loading...
```

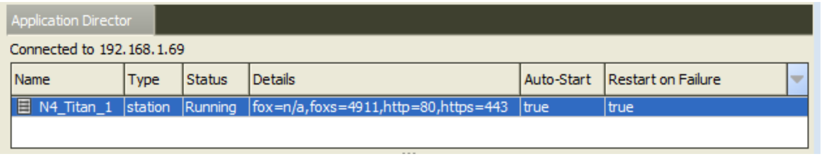
□ Auto-Start
☑ Restart on Failure

Even if a Windows platform is licensed for more than one station, running multiple stations at the same time requires you to use non-default ports for all but one of them to avoid port binding issues. For example, use a Fox and Foxs port other than 1911 or 3011 respectively, or Http and Https port other than 80 or 443 respectively.

Installed applications (stations) columns

The top area of the Application Director shows a table of installed applications (stations).

Figure 120: Application Director installed applications



Connected to 192.168.1.69

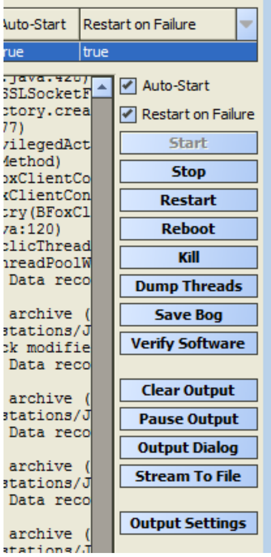
Name	Type	Status	Details	Auto-Start	Restart on Failure
N4_Titan_1	station	Running	fox=n/a,foxs=4911,http=80,https=443	true	true

Column	Value	Description
Name	text	The name of the station directory.
Type	always station	This identifies the entity as a Niagara station
Status	text	Read-only field. Indicates the condition of the station at last polling. • Idle — Station is not running, but can be started without a reboot. • Running — Station is running. • Starting — Platform daemon has started the station, but the station has not reported back its status back to the daemon. • Stopping — Daemon has ordered the station to stop, but its process has not yet terminated. • Halted — Station is not currently running, and cannot be restarted without a reboot. • Failed — Station terminated with a failure exit code.
Details	text	• fox= TCP/IP port monitored for regular (unencrypted) Fox connections to Workbench and other stations. Shows n/a if station is not running, or if Fox Enabled is set to false. • foxs= TCP/IP port monitored for secure Fox connections to Workbench and other stations, if so configured. Shows n/a if the host does not support (or is enabled) for a secure connection, or if the station is not running, or if Foxs Enabled is set to false. • http= HTTP port that the station's WebService monitors for regular (unencrypted) browser connections to the station. Shows "n/a" if station is not running, or if it does not have a running WebService, or if Http Enabled is set to false. • https= HTTP port that the station's WebService monitors for secure browser connections to the station, if so configured. Shows "n/a" if host does not support (or is enabled) for a secure connection, or if the station is not running, or if Https Enabled is set to false, or if the station does not have a running WebService.
Auto-Start	true or false	If true, the station starts whenever the platform daemon starts as configured in the check box to the right side of the window.
Restart on Failure	true or false	If true, the daemon automatically restarts the station after it terminates with a failure exit code as configured in the check box to the right side of the window.

Start-up options

Unlike in most Workbench views, where changes are entered first and then applied with a Save button, in the Application Director when you click check boxes and buttons, changes are applied immediately to the selected station.

Figure 121: Application Director start-up options and buttons



uto-Start	Restart on Failure
rue	true

```
:java:420)
SSLSocketF
ctory.crea
77)
vilegedAct
Method)
oxClientCo
xClientCon
cry(BFoxCl
va:120)
clicThread
hreadPoolW
 Data reco

 archive (
stations/J
ck modifie
 Data reco

 archive (
stations/J
 Data reco

 archive (
stations/J
 Data reco

 archive (
```

☑ Auto-Start

☑ Restart on Failure

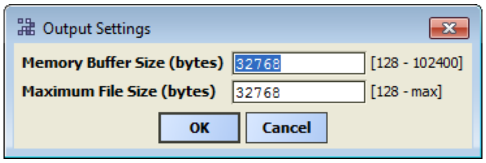
Option or button	Value	Description
Auto-start	check box	Specifies whether the station starts following platform daemon startup. A station restart occurs in the following cases: • Following a host reboot, such as after a power cycle • As the result of a Reboot command • Following the installation of any dist file(s) • Following any TCP/IP-related changes • When changing any existing module (upgrading or downgrading) A station restart may or may not follow the installation of new modules using the Software Manager, say, for a new driver. If a station restart is required for a module to become effective, a reboot is prompted.
Restart on Failure	check box	Specifies whether the platform daemon restarts the station if its process exits with a non-zero return code (for example, the engine watchdog had killed the station because of a deadlock condition). In Niagara 4, controllers can have a station restart without a reboot. Therefore, if this option is enabled, and the station fails (terminates with error), the station is restarted. If a controller has three automatic restarts within 10 minutes (or however many specified in the station's PlatformService Failure Reboot Limit property, the station remains in a failed state, regardless of the setting above.

Option or button	Value	Description
Start	Button enabled if the selected station has an Idle or Failed status in the installed applications area.	When pressed, the host’s platform daemon immediately starts the station, clears the text in the station output, and displays messages for the new station.
Stop	Button enabled if the selected station has a Running status in the installed applications area.	When pressed, opens a popup confirmation window. If you confirm, the host’s platform daemon shuts the station down gracefully (saving configuration to its config.bog file, and potentially saving history data).
Restart	Button enabled if the selected station has a Running status in the installed applications area.	When pressed, opens a popup confirmation window. If you confirm, the host’s platform daemon shuts the station down gracefully, then restarts it.
Reboot	Button always enabled.	When pressed, opens a popup confirmation window. If you confirm, reboots the selected host. This is considered a drastic action.
Kill	Button enabled only if the selected station has a status of Starting, Stopping, or Running the installed applications area.	When pressed, opens a popup confirmation window. If you confirm, the host’s platform daemon terminates the station process immediately. Always use Stop instead of Kill, unless unavailable (stuck for a long time as either Starting or Stopping). Unlike a station stop, a station kill does not cause the station to save its database (config.bog), histories or alarms, nor does it update the station output area.
Dump Threads	Button enabled only if the station has a Running status in the installed applications area.	When pressed, the host’s platform daemon has the station send a VM thread dump to its station output.
Save Bog	Button enabled only if the station has a Running status in the installed application area.	When pressed, the host’s platform daemon has the station locally save its configuration to config.bog.
Verify Software	Button enabled regardless of station status.	When pressed, Workbench parses the station’s config.bog and the host’s platform.bog files, looking for module references. It then checks to see if those modules (and any other software upon which they depend) are installed. If available in your Workbench installation, any missing software is listed in a pop-up window, the window offers to install the missing software into the remote host. Only modules (or versions of modules) needed by the station are installed that do not require commissioning. If the station needs modules that require commissioning, meaning an upgrade of core software, those modules are not copied.

Option or button	Value	Description
Clear Output	Button enabled only if the station has a Running status in the installed application area.	When pressed, the button toggles to Load Output, and the next press toggles back to Pause Output (and so on). • During a paused output, text remains frozen in the standard output area. This is useful when the station is rapidly writing output. • • When you press Load Output, text in the station output area is reloaded with the station's buffered output, and output remains updating in real time.
Output Dialog	Button enabled regardless of station status.	When pressed, it produces a separate non-modal output window displaying the same output text as in the Application Director's standard output area. Included are buttons to Dump Threads, Pause Output, Clear Output, and Close the window. ***Note:*** You may find this compact version of a station's standard output easier to work with than in the main area of the Application Director. Also, if needed you can open multiple output dialogs for comparison purposes.
Stream To File	Button	Opens a window for assigning a file name. Once open, the system saves all application output to this file.
Output Settings	additional properties	Opens a window for specifying how the platform daemon buffers the output from the station.

Output Settings window

Figure 122: Output Settings dialog



Memory Buffer Size (bytes) 32768 [128 - 102400]

Maximum File Size (bytes) 32768 [128 - max]

Note:

Changes to either output setting may clear the output buffer's contents.

Property	Value	Description
Memory Buffer Size	number	Defines the size of the memory buffer for the station output. If the station creates more output than the size of the memory buffer, the oldest output is lost.
Maximum File Size	number	When a station stops, its output buffer is written to a console. txt file. This setting defines the maximum size of that file.

platDaemon-DistInstaller

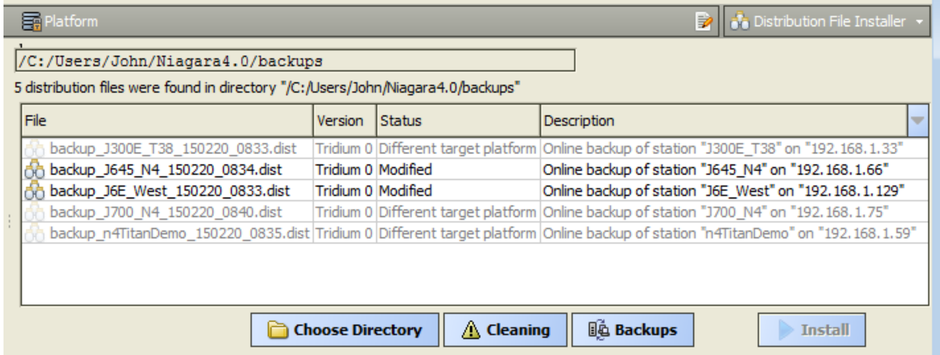
This view () allows you to install distribution (dist) files from your Workbench PC to the remote host platform.

Typical use is for restoring backups, or for installing a clean distribution file to essentially erase the file system of a controller and start again with the near-factory defaults.

Dist file selection

By default, the first time you use the Installer, the system searches the backups folder under your Workbench User Home (~\backups). If that folder does not exist yet (no backups have been made), the it searches the cleanDist folder under your Niagara Sys Home (!\cleanDist) instead.

Figure 123: Available dist files in Distribution File Installer



/C:/Users/John/Niagara4.0/backups

5 distribution files were found in directory "/C:/Users/John/Niagara4.0/backups"

File	Version	Status	Description
backup_J300E_T38_150220_0833.dist	Tridium 0	Different target platform	Online backup of station "J300E_T38" on "192.168.1.33"
backup_J645_N4_150220_0834.dist	Tridium 0	Modified	Online backup of station "J645_N4" on "192.168.1.66"
backup_J6E_West_150220_0833.dist	Tridium 0	Modified	Online backup of station "J6E_West" on "192.168.1.129"
backup_J700_N4_150220_0840.dist	Tridium 0	Different target platform	Online backup of station "J700_N4" on "192.168.1.75"
backup_n4TitanDemo_150220_0835.dist	Tridium 0	Different target platform	Online backup of station "n4TitanDemo" on "192.168.1.59"

At the bottom of the view, the ⚠ Cleaning and Backups buttons provide shortcuts to these two folder areas. If needed, you can also click the Choose Directory button to open a Change Directory window, and point the Installer to that location.

platDaemon-DistributionView

Distribution View is the dialog that appears when you double-click a distribution file listed in the platform's Distribution File Installer view. A number of details are provided about the selected distribution file, including all contents and any dependencies.

platDaemon-FileTransferClient

The File Transfer Client is the platform view that allows you to copy files and/or folders between your Workbench PC and the remote platform, as needed.

platDaemon-LexiconInstaller

Lexicon Installer allows you to install text-based lexicon file sets (for localization) on a remote host.

Note:

Standard lexicons are distributed as modules, for example: niagaraLexiconFr as the French lexicon, or niagaraLexiconDe for German. Workbench lexicon tools include a lexicon module maker, to make new or updated lexicon modules from lexicon files.

You can still install lexicon files using the Lexicon Installer, but to install lexicon modules you must use the platform Software Manager view.

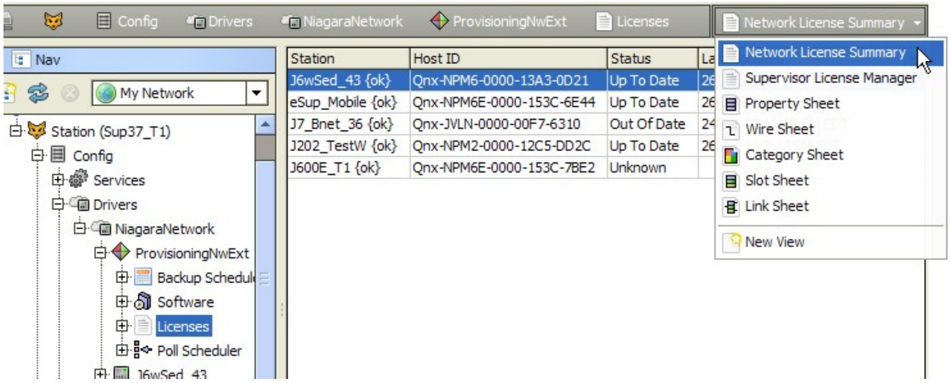
platDaemon-LicenseManager

The License Manager allows you to view and install files required for Niagara licensing.

provisioningNiagara-NetworkLicenseSummary

This view provides a summary table listing the currently known license information for each station (NiagaraStation) in the network. It is the default view for the SupervisorLicenses slot on the ProvisioningNwExt under the Supervisor's NiagaraNetwork.

Figure 124: Network Licenses Summary



Station	Host ID	Status	La
J6wSed_43 {ok}	Qnx-NPM6-0000-13A3-0D21	Up To Date	26
eSup_Mobile {ok}	Qnx-NPM6E-0000-153C-6E44	Up To Date	26
J7_Bnet_36 {ok}	Qnx-JVLN-0000-00F7-6310	Out Of Date	24
J202_TestW {ok}	Qnx-NPM2-0000-12C5-DD2C	Up To Date	26
J600E_T1 {ok}	Qnx-NPM6E-0000-153C-7BE2	Unknown	

Each row contains the license information for a host running a station. The SupervisorLicenses device extension of each child station populates the table. If you double-click on a row, the view changes to the SupervisorLicenses extension property sheet for that particular NiagaraStation.

Column	Value	Description
Station	text	Identifies the name of the station.
Host ID	text	A 20–character identifier that provides unique identification for each host.
Status	Up-To-Date	A status of Up To Date means that the license on the remote host agrees with the license that the Supervisor has for it in its (own) local license database. It may be possible that a more recent license is available for it on the licensing server.
Last Updated	date and time	The timestamp when the station's license was last updated.

platDaemon-SoftwareManager

The Software Manager is the platform view you use to install, upgrade, or remove modules in the connected Niagara platform.

platDaemon-SoftwareView

Software View is the dialog that appears when you double-click an item (for example, module) listed in the platform's Software Manager view. A number of details are provided about the selected item.

platDaemon-PlatformAdministration

The Platform Administration view provides access to various platform daemon (and host) settings and summary information. Included are buttons to perform various platform operations.

platDaemon-StationCopier

The Station Copier is the platform view used to install a station in either a remote or local Niagara platform, as well as make a local Workbench copy of a remote JACE station or a locally running station. You can also delete and rename stations using this view.

platDaemon-StationTextSummaryEditor

StationTextSummaryEditor is the dialog that appears when you click the export tool button when using the Application Director view. Setup in this dialog allows you to include/exclude the platform summary data, platform daemon console output, station console output, as well as limit both the daemon and station output.

platDaemon-TcpIpConfiguration

TCP/IP Configuration is the platform view you use configure a remote JACE host's TCP/IP settings. Typically, you make initial settings when you first commission a JACE for NiagaraAX, where this view is one step in the platform's Commissioning Wizard. For more details, see the section "TCP/IP Configuration".

Plugin in platDataRecovery

platDataRecovery-DataRecoveryServiceEditor

The Data Recovery Service Editor is the default view on the DataRecoveryService, as found in the PlatformServices of JACE controllers with onboard static RAM (SRAM or FRAM), or an installed SRAM option card.

This view allows monitoring of the "battery-less" support provided by this service. In a few cases, an SRAM-equipped JACE can additionally (and optionally) use a backup battery, such as an NiMH onboard battery pack, and (if applicable) and external 12V sealed lead-acid battery. In this case, both the DataRecoveryService and PowerMonitorService can exist in the station's PlatformServices container, operating independently or in unison, as configured.

Plugins in platform module

platform-LicensePlatformServicePlugin

License Platform Service Plugin allows you to manage the host's licenses and certificates under a station’s PlatformServices container. It provides the same interface as the License Manager view in a platform connection.

platform-NtpPlatformServiceEditorQnx

Ntp Platform Service Editor Qnx is the default view of the station’s NtpPlatformServiceQnx, which provides the platform interface to the NTP daemon (process) running on a JACE controller. This view provides access to a few related settings, plus allows specifying one or more remote time servers.

platform-NtpPlatformServiceEditorWin32

Ntp Platform Service Editor Win32 is the default view of a Windows platform station’s NtpPlatformServiceWin32, which provides the platform interface to the Windows Time service (W32Time) on the host platform’s Windows OS. In Niagara 4, this platform service remains disabled and read-only.

platform-PlatformServiceContainerPlugin

The Platform Service Container Plugin allows you to view and edit platform parameters on the host running the opened station. It is the default view for a station’s PlatformServices container.

platform-PlatformServiceProperties

PlatformServiceProperties allows you to view and edit platform parameters on the host running the opened station, using a property sheet.

platform-SystemDateTimeEditor

As an available view on a station’s PlatformServices container, the System Date Time Editor allows you to set the date, time, and time zone for the JACE platform running the station. If the station is running on a Windows platform, this view is read-only.

platform-SystemPlatformServicePlugin

System Platform Service Plugin allows you to view and edit platform parameters on a Windows based host running the station, and is the default view on the station’s SystemService (SystemPlatformServiceWin32).

platform-SystemPlatformServiceQnxPlugin

System Platform Service Qnx Plugin allows you to view and edit platform parameters on a JACE platform running the station, and is the default view on the station’s SystemService (SystemPlatformServiceQnx).

platform-TcpIpPlatformServicePlugin

Tcp Ip Platform Service Plugin allows you to manage the host's TCP/IP settings under a station’s PlatformServices container. It provides the same interface as the TCP/IP Configuration view in a platform connection. If the station is running on a Windows platform, this view is read-only.

platform-WorkbenchLicenseManager

Workbench License Manager allows you to browse and manage the contents of your Workbench PC’s “local license database.”

Plugins in platHwScan

platHwScan-HardwareScanServiceView

The Hardware Scan Service View is the default view on the platform service HardwareScanService in a station, providing that the JACE platform has the platHwScan module installed, along with the appropriate platHwScanType module. This view provides a graphical diagram of communication ports and other features on the hosting JACE platform, including callouts to a table that explain the location, description (such as COM2), port type, and status.

Plugins in platPower

platPower-JavelinaBatteryPlatformServicePlugin

The Javelina Battery Platform Service Plugin is the default view on the platform service PowerMonitorService in a JACE-7 (700) series controller. This view provides parameters for changing the shutdown delay time, as well as alarm source configuration settings.

Typically, support is enabled and configured at JACE commissioning time.

platPower-PowerMonitorPlatformServicePlugin

The Power Monitor Platform Service Plugin is the default view on the platform service PowerMonitorService in most JACE controller models. This view provides parameters for changing the shutdown delay time, as well as alarm source configuration settings.

Typically, support is enabled and configured at JACE commissioning time.

CHAPTER 5 LICENSE TOOLS AND FILES

The following topics are covered in this chapter:

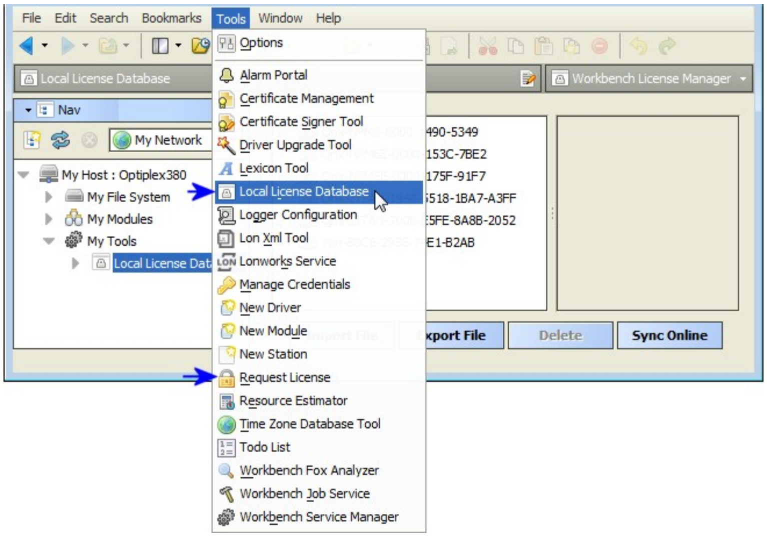
- Workbench License Manager
- Request License
- About the local license database
- About license archive (.lar) files
- About license files
- Global capacity licensing

This chapter provides details about the Workbench tools related to Niagara license files, including license management. Also included are details on the contents of license files.

License-related tools

Unlike platform views (which require a platform connection), or equivalent PlatformServices plugin views (requiring a station connection), the tools are available whenever running full Workbench. Find tools on the Workbench Tools menu, as shown below.

Figure 125: Tools menu in Niagara 4 Workbench includes licensed-related tools



License-related tools include the following:

- Workbench License Manager tool (see the section “Workbench License Manager”)
- Request License tool (see the section “Request License”)

The following License management topics are covered in this chapter, in addition to Workbench License tools:

- “About the local license database”
- “About license archive (.lar) files”

The section “About Niagara license files” includes the following topics:

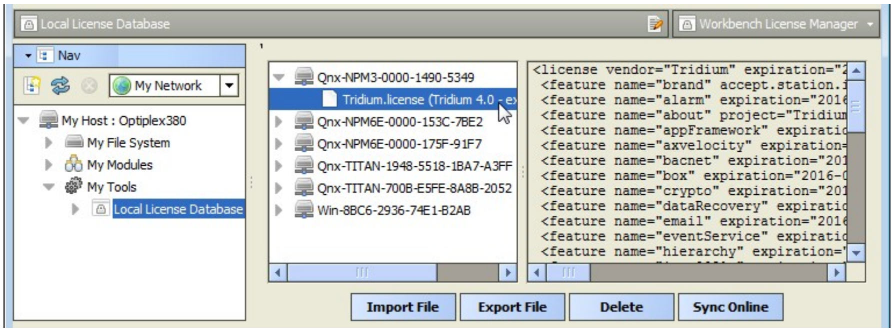
- “Items common to all license files”
- Controller hardware features
- “Driver attributes”
- “Driver types”
- “Applications”
- “Global capacity licensing”

- “Capacity licensing operation and recount”
- “Checking capacity licensing status”
- “Capacity licensing fault notifications”
- “Capacity licensing notes about histories”

Workbench License Manager

The Workbench License Manager view is available via Tools→Local License Database.

Figure 126: Workbench License Manager



```
<license vendor="Tridium" expiration="2
 <feature name="brand" accept.station.i
 <feature name="alarm" expiration="2016
 <feature name="about" project="Tridium
 <feature name="appFramework" expiratio
 <feature name="axvelocity" expiration=
 <feature name="bacnet" expiration="201
 <feature name="box" expiration="2016-0
 <feature name="crypto" expiration="201
 <feature name="dataRecovery" expiratio
 <feature name="email" expiration="2016
 <feature name="eventService" expiratio
 <feature name="hierarchy" expiration="
```

As shown above, this view lets you browse and manage the contents of your “local license database.”

Note:

For details about the license database structure, see “About the local license database”.

This view provides a two-pane window into all the license files and parent “host ID” folders, where

- Left pane provides tree navigation, where you can expand folders and click (to select) license files.
- Right pane shows the text contents of any selected license file.

Buttons at the bottom of this view provide a way to manage the contents of your local license database, and are described below:

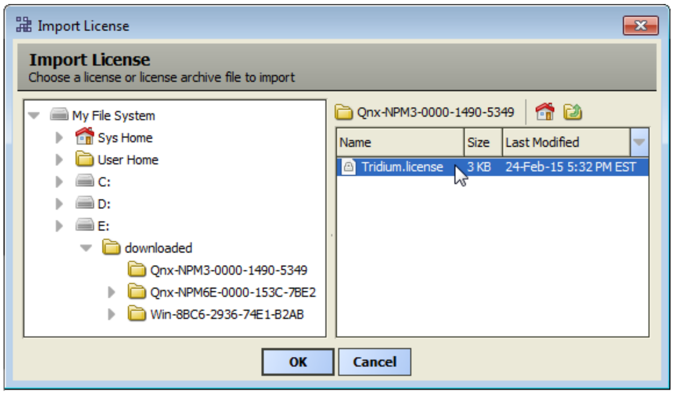
- Import File: Always available, this allows you to add license file(s) from a local license file or license archive (.lar) file.
- Export File: Always available, this allows you to save all licenses (or any selected licenses) locally, as a license archive file.
- Delete: This allows you to delete licenses from your Workbench local license database.
- Sync Online: Typically available if you have Internet connectivity. This lets you update all licenses (or any selected licenses) in your local license database with the most current versions, via the online licensing server.

Import File using Workbench License Manager

The Import File button in the Workbench License Manager is always enabled, and opens the Import License window for you to navigate to a source file (.license or .lar).

Only two types of files appear for selection.

Figure 127: Import License dialog to find local license file or license archive file

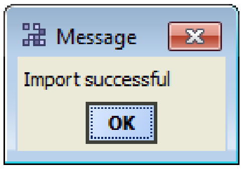


Import License
Choose a license or license archive file to import

Name	Size	Last Modified
Tridium.license	3 KB	24-Feb-15 5:32 PM EST

To add to (or update in) your local license database, select a license file and click OK . A popup window confirms success, and the license(s) are added or updated in your database.

Figure 128: Import success



Import successful

If any of the license(s) you select to import are older than the ones currently in your local database, meaning that the generated attribute timestamp is earlier, newer license(s) in your local license database are not overwritten. However, the same Import successful message popup appears for such file import operations.

Export File

The Export File button in the Workbench License Manager allows you to save any number (or all) licenses in your local license database locally on your Workbench PC, as a license archive (.lar) file.

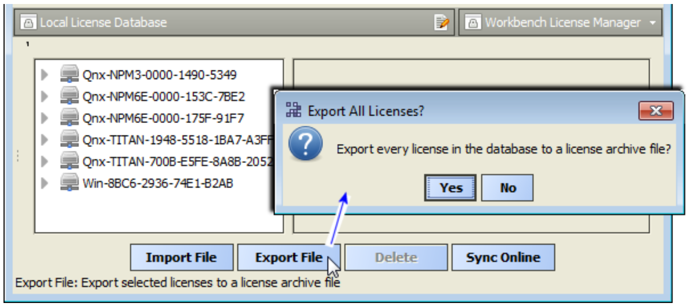
Note:

The license archive format allows you to easily share saved .lar files (however named) among multiple PCs without overwriting a license file for a different host platform. You can use the “Import File” command in the Workbench License Manager to add/update licenses in a license archive, or the equivalent “Import” command from the platform License Manager (or similar License Platform Service Plugin).

For more details, see “About license archive (.lar) files”.

If you click Export File without first selecting any licenses (and/or) host IDs, every license in your local license database will be included in the archive, as noted in a confirmation dialog. See below.

Figure 129: Export All Licenses confirmation dialog



Qnx-NPM3-0000-1490-5349
Qnx-NPM6E-0000-153C-7BE2
Qnx-NPM6E-0000-175F-91F7
Qnx-TITAN-1948-5518-1BA7-A3FF
Qnx-TITAN-700B-E5FE-8A8B-2052
Win-8BC6-2936-74E1-B2AB

Export All Licenses?

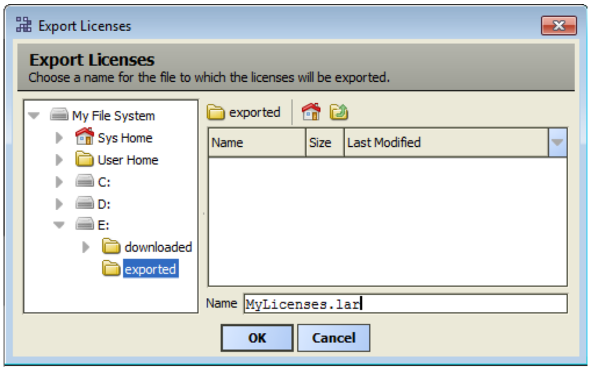
Export every license in the database to a license archive file?

Export File: Export selected licenses to a license archive file

Or, you can select one or more entries in the left pane (host IDs or license files) to include only those selected (highlighted) licenses to be in the exported archive file.

When you click Yes (if all) or Export File for selected licenses, an Export Licenses dialog lets you navigate to the spot to save the .lar file, as shown below.

Figure 130: Export Licenses dialog



Export Licenses

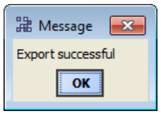
Choose a name for the file to which the licenses will be exported.

Name: MyLicenses.lar

Use the dialog’s navigation controls to specify another target folder or drive, as needed. Before saving, you can also rename the license archive file, to make it more identifiable. For example, instead of: licenses.lar, you could rename it MyECBOS6s.lar.

Upon export of license(s) to a license archive file, a popup dialog appears, as shown below.

Figure 131: Export file success



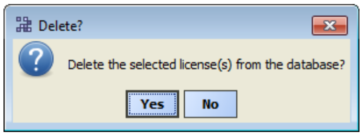
Message

Export successful

Delete

The Delete button in the Workbench License Manager is enabled when you have one or more host IDs and/or license files selected in the left pane, and produces a confirmation dialog to delete licenses from your local license database, as shown below.

Figure 132: Delete licenses confirmation



Delete?

Delete the selected license(s) from the database?

Click Yes to delete the license(s), or No to leave the local license database unchanged.

Note:

Following a delete, you may need to click the Refresh button in order to update the left pane contents. Note that if the selected "host ID" folder contained only a .license file, the entire folder is removed with a delete. However, if the folder contained other files (or subfolders), only the .license file is actually deleted, but it will no longer appear in the left pane.

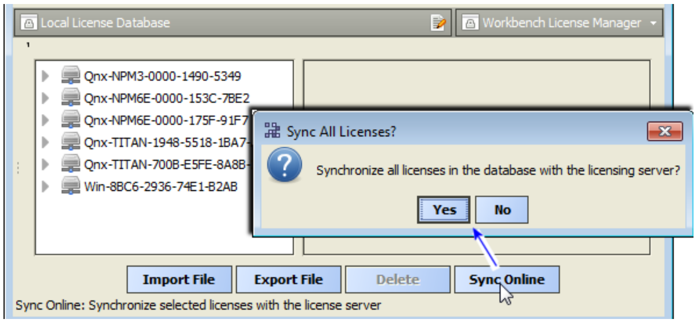
Sync Online

The Sync Online feature in the Workbench License Manager allows you to update any number (or all) licenses in your local license database with the most current license, available online from the licensing server. This feature requires Internet connectivity from your Workbench PC.

For related details, see "About the licensing server".

If you click Sync Online without first selecting any licenses (and/or) host IDs, every license in your license database will be included in the sync request, as noted in a confirmation dialog. See below.

Figure 133: Sync All Licenses confirmation dialog



Local License Database | Workbench License Manager

- Qnx-NPM3-0000-1490-5349
- Qnx-NPM6E-0000-153C-7BE2
- Qnx-NPM6E-0000-175F-91F7
- Qnx-TITAN-1948-5518-1BA7
- Qnx-TITAN-700B-E5FE-8A8B
- Win-8BC6-2936-74E1-B2AB

Sync All Licenses?

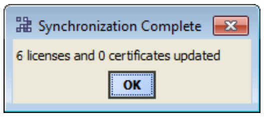
Synchronize all licenses in the database with the licensing server?

Sync Online: Synchronize selected licenses with the license server

Or, you can select one or more entries in the left pane (host IDs or license files) to include only those selected (highlighted) licenses to be included in the sync request.

When you click Yes (if all) or Sync Online for selected licenses, an immediate request is sent to the licensing server. Intermediate popup dialogs may briefly appear while the sync request is handled. The operation concludes with a Synchronization Complete dialog, which summarizes the number of licenses and certificate files that were updated in your local license database. See below.

Figure 134: Synchronization Complete dialog



Synchronization Complete

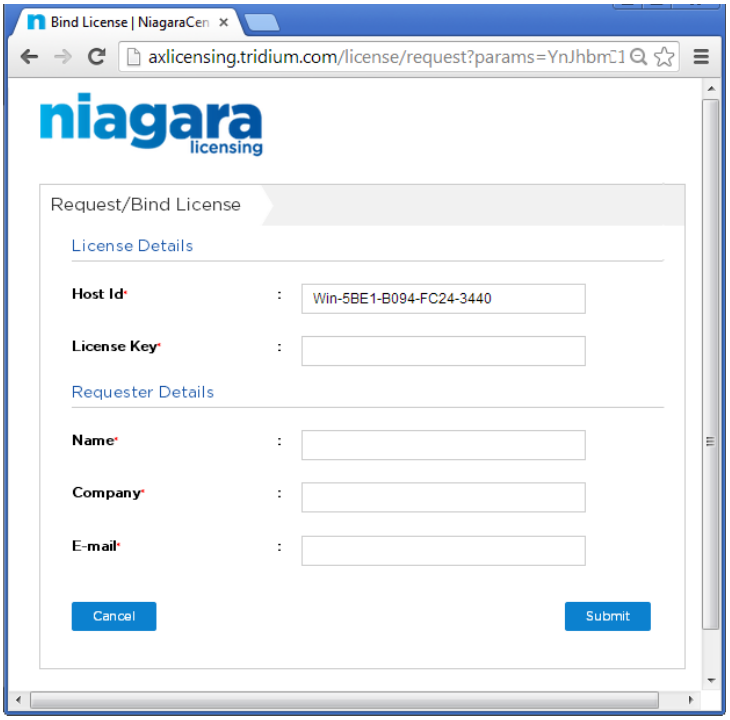
6 licenses and 0 certificates updated

If all licenses (and certificates) were already up-to-date, this dialog will say "0 licenses and 0 certificates updated".

Request License

In Workbench, selecting Tools→Request License opens a Request/Bind License form in your default browser. By default, the only pre-filled field in this form is the host ID of your PC. See below.

Figure 135: License request form opens in browser


Bind License | NiagaraCen
axlicensing.tridium.com/license/request?params=YnJhbm1
niagara
licensing

Request/Bind License

License Details

Host Id*	:	Win-5BE1-B094-FC24-3440
License Key*	:	

Requester Details

Name*	:	
Company*	:	
E-mail*	:	

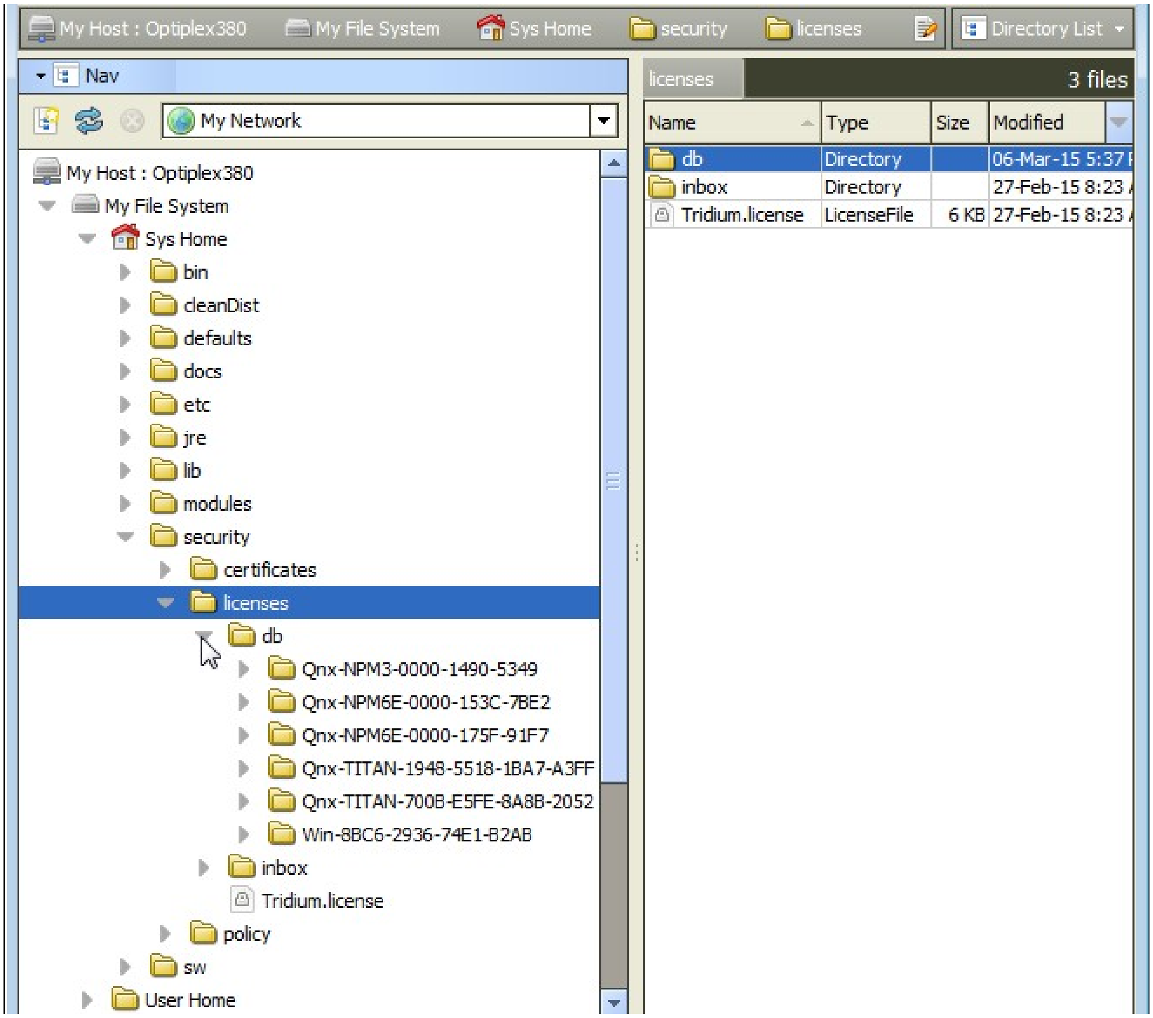
Typically, your Workbench PC is already licensed. Otherwise, you would not be able to successfully start Workbench to request a license.

However, you could use this as quick method to request a license for another PC on which you have installed Niagara. In that case, in this form you must enter the host ID for that other PC, along with the other pertinent information.

About the local license database

Any Workbench PC (including a Supervisor) has a "local license database", a structured collection of subfolders and files under its Niagara release (Sys Home) !/security/licenses/db directory. Each subdirectory has a unique Niagara "host ID" name, matching that for some remote host platform. The figure below shows an example license database structure, as viewed in the Nav tree.

Figure 136: Local license database (everything under !/licenses/db)



Name	Type	Size	Modified
db	Directory		06-Mar-15 5:37
inbox	Directory		27-Feb-15 8:23
Tridium.license	LicenseFile	6 KB	27-Feb-15 8:23

Your local license database is created and managed automatically by Workbench, and updated whenever you perform license operations from platform connections, PlatformServices plugins, or when using Workbench tools such as the Workbench License Manager. Note that you can see the same directory/file structure when looking at this location on your Workbench PC using Windows Explorer.

Note:

The license required for your (local) Workbench PC operation is in the root of the licenses folder, named simply by your brand, for example Distech.license.

Local license database rationale

The local license database design makes it easier for Workbench to store licenses for multiple host platforms, without inadvertently overwriting one license file with another. This saves you from having to make special license folders (subdirectories), and/or rename license files uniquely. The related “license archive” storage file format (.lar) also facilitates the exchange of licenses among different PCs, and is used in updating/synchronizing licenses to the online licensing server, as well as with provisioning features for Niagara Networks.

See “About license archive (.lar) files”.

Local license inbox

In addition to the !security/licenses/db folder, there is also a !security/licenses/inbox folder. The inbox allows “drag and drop” importing into your license database of both individual license files and “license archive” (.lar) files, which may have been “saved” or “exported” from other PCs, or perhaps sent to you from the licensing server.

After copying license files and/or .lar files into your inbox subfolder, you need to close and restart Workbench. Then, the appropriate “host ID” named subfolders are automatically created in your local license database, each with the appropriate license file(s). Contents of the inbox folder are then deleted.

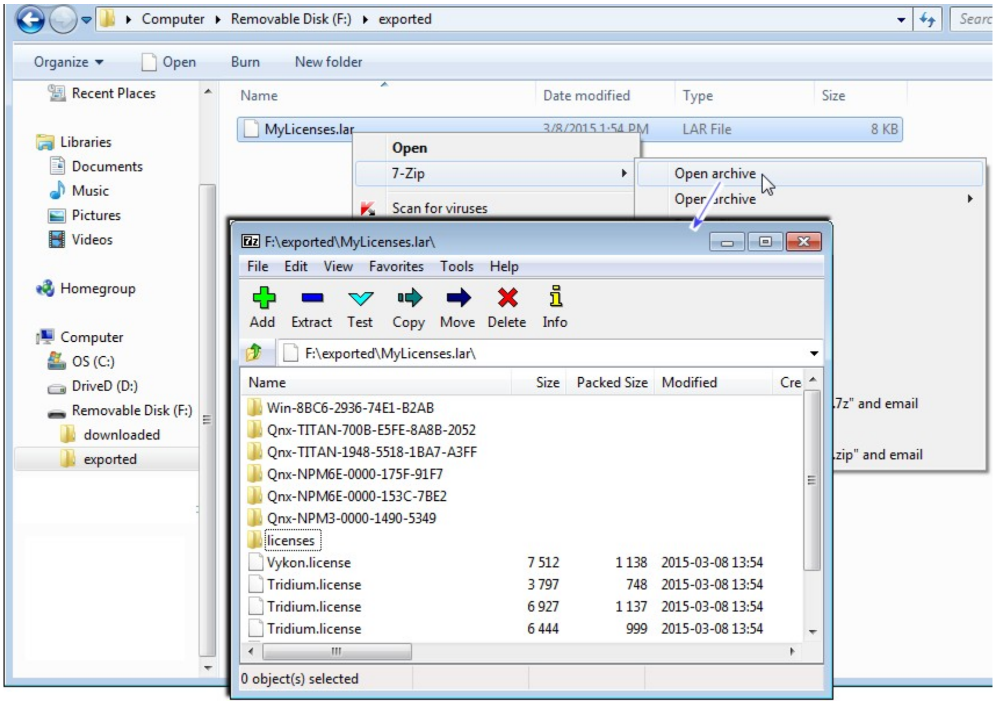
Note:

After you restart Workbench, your local license database will be correctly structured. In addition, now you can use the “Sync Online” feature of the Workbench License Manager to ensure you have the latest version of all your licenses. See the section “Sync Online”.

About license archive (.lar) files

When you use the platform License Manager view or the Workbench License Manager view (under Workbench Tools) to export one or more license files, they are saved in a compressed (Zip compatible) format known as a license archive, that is a file with a ".lar" file extension. Any .lar file is simply a zip of the exported license file(s) that includes the complete "licenses/hostID" folder (subdirectory) structure for any included licenses.

Figure 137: License archive (.lar) is license file(s) in zip format, including folder paths relative to sys home.



F:\exported\MyLicenses.lar\

Name	Size	Packed Size	Modified	Cre
Win-8BC6-2936-74E1-B2AB				
Qnx-TITAN-700B-E5FE-8A8B-2052				
Qnx-TITAN-1948-5518-1BA7-A3FF				
Qnx-NPM6E-0000-175F-91F7				
Qnx-NPM6E-0000-153C-7BE2				
Qnx-NPM3-0000-1490-5349				
licenses				
Vykon.license	7 512	1 138	2015-03-08 13:54	
Tridium.license	3 797	748	2015-03-08 13:54	
Tridium.license	6 927	1 137	2015-03-08 13:54	
Tridium.license	6 444	999	2015-03-08 13:54	

The figure above shows a .lar file in Windows Explorer, opened using 7-Zip, and its subsequent contents. In this case where the archive contains multiple licenses, it was created by an export performed using the Workbench License Manager tool. However, if you export a license in the License Manager when platform-connected to a remote host, the license archive file contains just the license(s) for that host.

About Niagara license files

A Niagara license file is a structured XML file that has a .license file extension. It enables a set of vendor specific features. Each license file is valid for one specific host platform (JACE, PC), matched by that host's unique host ID. License files are "digitally signed" by the vendor to prevent tampering.

The following sections provide more details on the contents of a Niagara 4 license file that validates against the Distech certificate:

- Items common to all license files (license, about, brand, signature)
- Controller hardware features (e.g. dataRecovery, mstp, ndio, serial, others)
- Driver attributes (name, expiration, device.limit, history.limit, point.limit, schedule.limit, parts)
- Driver types (many types, including bacnet, lonworks, modbusTcp, obixDriver, niagaraDriver)
- Applications (email, provisioning, station, web, Workbench, others)

Items common to all license files

license

All license files require an opening <license> line, where the last line in the license file is the closing </license> tag, and all contents (lines) in between are <feature> elements, plus one signature element.

In the first <license> line, there are a number of common attributes, as described below.

<license vendor="Tridium" expiration="never" version="3.8" hostId="Qnx-NPM6E-0000-153C-6E44" serialNumber="4856" generated="2015-01-27">

vendor

vendor="Tridium": This is always Tridium.

expiration

expiration="never": The expiration date of the license file. After the expiration date the Workbench software fails to start due to a license expired error. Typically, engineering copies of Workbench have expiration dates which expire on an annual basis. License files for actual projects are issued with non-expiring licenses, where this attribute value is "never".

version

version="3.8": The highest release version of software which can be installed in the JACE. If a newer version of software is installed, the JACE will fail on startup with a license version error.

hostId

hostId="Qnx-NPM6E-0000-153C-6E44": Alphanumeric code unique to the specific host. On a Windows-based platform, host ID is generated upon installation of the Niagara software, and typically begins with "Win-", for example "Win-5BE1-B094-FC24-3440".

JACE controllers are assigned a host ID at the factory. The first two segments are "Qnx-Model-" such as "Qnx-NPM6-" for a JACE-6 or "Qnx-TITAN-" for a JACE-8000 controller. The hostId in the license file must match the hostId of the JACE controller, otherwise the JACE cannot run a station.

serialNumber

serialNumber="329696": Applies to a license for a JACE controller only. Designates its unique serial number assigned from the factory. The serial number in the license file must match the serial number of the JACE.

generated

generated="2015-01-27": The date upon which the license file was generated.

brand

For any license with vendor="Tridium", the NiCS (Niagara Compatibility Structure) provides a structure (or schema) that OEMs can use to define the various levels and types of Niagara interoperability that their products will support.

NiCS definitions are contained in this feature item, which is checked by a station or tool when it starts up. There are five attributes to the NiCS: BrandID, Station Compatibility In, Station Compatibility Out, Tool Compatibility In, and Tool Compatibility Out. These elements can be combined in a variety of ways to achieve unlimited flexibility, and are described below.

<feature name=accept.station.in="*" accept.station.out="*" accept.wb.out="*" "brand" brandId="Distech" accept.wb.in="*"/>

accept.station.in

accept.station.in="*": A list of brands that this local station will allow Niagara data to come in from. Simply stated from a JACE perspective, "this is the list of brands that I can accept data from". The "*" is a wildcard designation to allow all brands.

accept.station.out

accept.station.out="*": A list of brands that this local station will allow Niagara data to be shared with. Simply stated, "This is the list of brands that I can share data with".

accept.wb.out

accept.wb.out="*": A list of brands that this tool is allowed to connect to and engineer. Simply stated, "This is the list of brands that I can engineer".

brandId

brandId="Distech": Every licensed station and tool has a Brand Identifier (BrandID). This field holds a text descriptor acts as the identifier for the product line. Each station or tool can have only one BrandID entry.

accept.wb.in

accept.wb.in="*": A list of brands that this station will allow to be connected to it for engineering of its application. Simply stated, "This is the list of brands that can engineer me".

about

The "about" feature is used to designate optional information, and does not affect station operation in any way. This information can be useful for filtering records when searching the license database. Two attributes in this feature are typically designated when ordering product:

<feature name="about" project="Testing" owner="Tech Pubs"/>

project

project="Tech Pubs": Optional attribute to designate a project. This grouping should typically be assigned to all JACE controllers used for a particular project.

owner

owner="Tech Pubs": Optional attribute to designate the name of a person or group responsible for the project, or possibly an end user.

signature

This ending element contains a digital signature which is created when the license file is generated. It prevents tampering with the license file. Attempts to edit the license file to enable additional features will render the license file useless.

Typically, the signature element is the last element contained in the license, so it is followed by the closing license tag as the last line in the license file.

<signature>MCwCFFOdq4wJcYgvhTVtrf0oSyuCDCwjAhRj+ H9pNxQGStBnhEkIqK8rONB10g==</signature> </license>

Controller hardware features

Some license features are specific to JACE controller hardware capabilities. Alphabetically, these include features dataRecovery, jre8qnx, mstp, ndio, nrio, and serial.

dataRecovery

This feature licenses a station's DataRecoveryService, sourced from its platDataRecovery module. This is required to support installed SRAM (Static RAM), whether integral "onboard SRAM" (such as for more recent controllers) or another JACE controller with an installed SRAM option card.

<feature name="dataRecovery" expiration="never" parts="NPB-SRAM">

jre8qnx

This feature licenses the (Oracle) Sun Hotspot Java 8 virtual machine (VM) to be able to run on the Niagara 4 JACE controller. There are no attributes.

<feature name="jre8qnx" expiration="never">

mstp

This feature determines how many of the available serial ports may be used for BACnet MS/TP communications. Note that features bacnet and serial must also exist in the license file.

<feature name="mstp" expiration="never" port.limit="5"

parts="DR-MSTP-AX"/>

port.limit

port.limit="5": This specifies the number of serial ports which may be used for MSTP communications. Typically this number matches the number of physical ports. Some JACE controller models have option card modules or slots with serial ports. If additional ports are added then the port limit may be less than the number of physical ports (if the port activation has not been ordered as well).

ndio

This feature enables the NDIO (Niagara Direct Input Output) driver, required to configure and use a JACE controller's Ndio-type I/O modules. Not all JACE controllers support such I/O modules (which attach/chain directly to the controller, using 20-pin connectors); refer to specific JACE controller data sheets to confirm whether this is an available option. Note that in the ndio features line (below), a “device” equates to an “Ndio Board”, and that history and schedule limits have no practical application.

<feature name="ndio" expiration="never" device.limit="none" history.limit="none" point.limit="none" schedule.limit="none"

parts="DR-NDIO"/>

nrio

This feature enables the NRIO (Niagara Remote Input Output) driver, required to configure and use a JACE controller's Nrio-type I/O modules and/or any onboard I/O of a controller. All N4 JACE controllers support NRIO modules (which communicate via RS-485). Note that in the nrio features line (below), a “device” equates to an “Nrio16Module”, and that history and schedule limits have no practical application.

<feature name="nrio" expiration="never" device.limit="16" history.limit="none" point.limit="none" schedule.limit="none" parts="DR-NRIO"/>

serial

This feature enables the use of JACE serial ports for various drivers, for example aapup or modbusAsync. Note that the JACE license needs this serial feature in addition to any specific driver feature. Only one serial feature line is needed, regardless of number of serial-based drivers. Note that in the case of a JACE used for BACnet MS/TP, it would require this serial feature and driver features bacnet and mstp.

<feature name="serial" expiration="never"/>

Driver attributes

Each driver is enabled by a feature line (element) in the license file. Most of the drivers utilize the same attributes within that feature. The most common driver attributes are shown below.

<feature name="driverName" expiration="expirationDate" device.limit="none" history.limit="none" point.limit="none" schedule.limit="none">

The various "limit type" attribute values can be either "none" or a numerical (limit) value, for example device.limit=32. Note that a limit value of none means unlimited, whereas a limit value of 0 means none allowed.

For many drivers, only the point.limit and device.limit attributes are applicable; yet most drivers include all .limit attributes. For example, none of the Modbus-related drivers have any history or schedule import/export capability, due to the simplicity of the Modbus protocol. Thus, "history.limit" and "schedule.limit" values have no significance in the feature for a Modbus driver.

Note:

In Niagara 4 (and depending on license), limit attributes in individual drivers may be superseded by “global capacity” limits, using a licensing model that sets limits that span across multiple drivers. This allows more flexibility to allocate the number of devices, points, and so on—without requiring ongoing license changes. For more details, see the section “Global capacity licensing”.

name

Feature name of the driver, often the same as the actual module (.jar file) name, for example bacnet, lonworks, etc.

expiration

Each driver has an expiration date which is typically the same as the expiration property of the license feature. In some cases such as beta testing agreements, individual drivers may be set to expire where the main license file is non-expiring.

device.limit

This attribute designates a license limit on the number of devices which may be added to this specific driver network in the station database. Above this limit, any added device component (and all its child components) will be in fault.

This limit has no impact on the actual physical limitation of a field bus. For example just because the lonworks feature is set to device.limit="none", this does not mean that you can exceed the normal limit of 64 devices per segment.

history.limit

This attribute limits the number of Niagara histories that can be imported from remote histories (logs or trends) into the station's history space, and/or exported from station histories to appear as histories in remote devices. Above this limit, any added history import descriptor (or history export descriptor) will be in fault, and the associated import/export will not be successful.

point.limit

This attribute designates the maximum number of proxy points that may be added to the station database for a particular driver. Above this limit, any added proxy point will be in fault.

schedule.limit

This attribute limits the maximum number of Niagara schedules that can be imported from remote schedules into the station's database, and/or exported from station schedules to appear as schedules in remote devices. Above this limit, any added schedule import descriptor (or schedule export descriptor) will be in fault, and the associated import/export will not be successful.

parts

This is an alphanumeric part code which is automatically assigned when generating the license file and is for internal use.

Driver types

Each driver type is enabled by a separate feature element (or line, starting with name attribute), and has common attributes.

Note:

New Niagara drivers are continually developed and offered as products. This section includes some, but not all drivers available. It is included in this section to illustrate how driver features appear in licenses.

Alphabetically, driver types listed here include aaphp, aapup, bacnet, bacnetAws, bacnetOws, fileDriver, lonworks, modbusAsync, modbusCore, modbusSlave, modbusTcp, modbusTcpSlave, obixDriver, opc, niagaraDriver, rdbOracle, rdbSqlServer, snmp, videoDriver and zwave.

aaphp

This enables the American Auto-Matrix Public Host Protocol (PHP) driver. The serial feature is also required.

aapup

This enables the American Auto-Matrix Public Unitary Host (PUP) driver. The serial feature is also required.

bacnet

This enables functionality of the BACnet driver for BACnet/Ethernet and BACnet/IP. If a JACE controller, other features can be added to enable BACnet MS/TP communications over serial ports: mstp and serial.

<feature name="bacnet" expiration="never" device.limit="none" export="true" history.limit="none" point.limit="none" schedule.limit="none"/>

export

export="true": When set to "true" this field enables BACnet server operation. When the field is set to "false" only BACnet client operation is permitted.

Note:

When BACnet export is enabled, any station histories and/or schedules that are exported to BACnet do not count towards any history.limit or schedule.limit values in the license (if any).

bacnetAws

This provides added functionality as BACnet AWS Supervisor with BTL-certification, as described in the BACnet “Advanced Operator Workstation” specification (B-AWS). This is available for PC platforms only (not JACE platforms). The bacnet feature is also required in the license.

bacnetOws

This provides added functionality as BACnet OWS Supervisor with BTL-certification, as described in the BACnet “Operator Workstation” specification (B-OWS). This is available for PC platforms only (not JACE platforms).

fileDriver

This enables the File driver, used to import comma or tab delimited text files and convert into histories.

lonworks

This enables the Lonworks driver. Utilizing the driver also requires a LON interface on the JACE controller. Most JACE controller models require an optional Lonworks interface card to be installed.

modbusAsync

This enables the Modbus Master Serial driver. The JACE controller operates as the Modbus Master device communicating via an available serial port using either Modbus RTU or Modbus ASCII. The modbusCore and serial features are also required.

modbusCore

Required by a JACE controller or Modbus Supervisor host for any of the Modbus drivers (Async, Slave, TCP, TCP Slave).

modbusSlave

This enables the Modbus Slave Serial driver. The JACE controller operates as a Modbus Slave communicating via an available serial port using either Modbus RTU or ASCII to a Modbus Master device. The modbusCore and serial features are also required.

modbusTcp

This enables the Modbus Master TCP driver. The JACE controller or Modbus Supervisor operates as a Modbus Master device communicating via Modbus TCP/IP. The modbusCore feature is also required

modbusTcpSlave

This enables the Modbus Slave TCP driver. The JACE controller or Modbus Supervisor operates as a Modbus Slave device communicating via Modbus TCP/IP. The modbusCore feature is also required.

obixDriver

This enables the oBIX driver. The driver supports the oBIX protocol, which is M2M (Machine-to-Machine) communications via XML over TCP/IP.

<feature name="obixDriver" expiration="never" device.limit="none" export="true" history.limit="none" point.limit="none" schedule.limit="none"/>

export

export="true" When set to "true" this field enables oBIX server operation. When the field is set to "false" only oBIX client operation is permitted.

opc

Enables the OPC client driver, and is only available on Windows-based platforms because of the protocol's dependency of Windows.

niagaraDriver

Enables communication via the Fox protocol to other NiagaraStations, and allows creation of a NiagaraNetwork, including proxy points, importing/exporting histories and schedules, and routing alarms.

<feature name="niagaraDriver" expiration="never" virtual="true" schedule.limit="none" point.limit="none" history.limit="none" device.limit="none" parts="ENG-WORKSTATION"/>

rdbOracle

This enables the Relational Database Driver using the Oracle database format. This driver allows exporting of histories from the NiagaraStation to an Oracle database. The driver does not include the Oracle software, which must be purchased separately from a third party source.

<feature name="rdbOracle" expiration="never" parts="ENG-WORKSTATION"/>

rdbSqlServer

This enables the Relational Database Driver using the Microsoft SQL database format. This driver allows importing and exporting of histories to and from the NiagaraStation, and to and from a Microsoft SQL database. The driver does not include the Microsoft SQL software, which must be purchased separately from a third party source. The driver does work with the MSDE version which is free from Microsoft; however, the normal Microsoft imposed limitations on the MSDE version still apply.

<feature name="rdbSqlServer" expiration="never" history.limit="10" historyImport= "true" parts="ENG-WORKSTATION"/>

snmp

This enables the SNMP (Simple Network Management Protocol) driver, which allows sending and receiving SNMP messages.

<feature name="snmp" expiration="never" device.limit="none" history.limit="none" point.limit="500" schedule.limit="none"/>

videoDriver

Enables the Niagara Video Framework driver (modules nvideo, videoDriver, nDriver) that provide the foundation to integrate select commercial off-the-shelf video surveillance and recording systems into a Niagara station. Depending on the specific video hardware used, one or more vendor-specific license feature entries are also typically required.

Applications

Alphabetically, application types listed here include box, email, ldapv3, mobile, provisioning, search, template, station, web, and workbench. Applications station, web, and workbench have special importance, and are summarized first.

Note:

The application feature “crypto”, as used in NiagaraAX licenses is no longer required. All Niagara 4 hosts are capable of TLS operation without this license feature.

station

Enables a station to be run, and is present in any JACE platform, as well as a Supervisor.

<feature name="station" expiration="2015-04-01" resource.limit="none" guestEnabled="true"/>

The station feature may not be present in a license for an engineering workstation (PC), unless specifically ordered with it. Optional attributes are listed below.

resource.limit

resource.limit="none": If the resource.limit flag is specified (in kRUs), then the station displays a warning on startup if the actual resource units exceed the limit resource units. If the limit is exceeded by 110% then the station will not boot at all. This limit is normally only specified in (NiagaraAX) SoftJACE license files.

Note:

In Niagara 4, the station feature attribute resource.limit is superseded by “global capacity” limits, using a licensing model that sets limits on the numbers of devices, points, histories, and so on that span across multiple drivers in the station. This allows a clearer measure of resource capacity in a license than the “resource limit” method. For more details, see the section “Global capacity licensing”.

guestEnabled

guestEnabled="true": Must be present and true, or else the station’s UserService has its built-in user “guest” hidden upon first station start up, as a security measure. Only hosts licensed as “demo hosts” can enable and use the guest user, therefore it is unavailable on any host with a “non-expiring” license.

web

The web feature must be present to start the WebService in a running station (to access the web server via a browser HTTP connection). If not licensed, the server is set to fault with appropriate faultCause.

Note:

Full Workbench can connect to a station (via Fox connection) even if the web feature is missing or expired.

<feature name="web" expiration="never" ui="true" ui.wb="true" ui.wb.admin="true"/>

ui

ui="true": This flag allows browser access to users with an HTML5 Hx Profile.

Note:

If ui="false", users cannot access the browser UI with either HTML5 Hx or Wb web profiles. No browser access is allowed, except for Spy pages.

ui.wb

ui.wb="true": This flag allows browser access to users with a Wb web profile.

Note:

If ui.wb="false", users with an HTML5 Hx web profile still have browser UI access, as long as ui= "true".

ui.wb.admin

ui.wb.admin="true": This flag allows browser users with a Wb web profile access to admin-only views on components, providing they have admin permissions on components with such views. Admin-only views include most types of views, except for property sheet views. For example, wire sheets and most manager views require this option. Browser access to such views is unavailable for any user with an HTML5 Hx web profile. Or, if this flag is false, such views are also unavailable to Wb web profile users.

Note:

If ui.wb.admin="false", users still have access to the station with a browser, subject to the “ui” and “ui.wb” flags. Property sheet views are available on components. Slot sheets may be available too, providing the user has admin-level permissions on components.

workbench

The workbench feature must be present to start the full version of Workbench (for example, a copy of Distech Controls Niagara Workbench or an OEM-specific Workbench-based application). If the admin flag is false, then all views requiring admin access are unavailable. This feature is included for PC platforms only, with the sole exception of the (NiagaraAX) SoftJACE.

```
<feature name="workbench" expiration="never"  admin="true"/>
```

box

This enables a host for Bajascript, a Javascript API (read and write) for Niagara data access from Javascript enabled environment like web browsers. Along with the mobile feature, this license feature is required for mobile application support.

```
<feature name="box" expiration="never" session.limit="none" parts="ENG-WORKSTATION"/>
```

Messaging features

The devices monitored by the system and the services that do the monitoring can communicate status, alarms and reports as needed using direct email and SMS messaging.

The system supports these features:

- The email feature enables a station to communicate with an SMTP server:

<feature name="email" expiration="never"/>

If the feature is not present, the system marks the EmailService and all incoming and outgoing accounts as in {fault}.

- The SMS messaging feature enables a station to send text messages to a phone.

ldapv3

This feature enables a host to use authentication schemes of LDAP and/or Kerberos for station users under the standard UserService. This allows users to be authenticated using LDAP in coordination with the site's existing Active Directory server or LDAPv3 server.

Note this departs from the former usage of special user services, such as "LdapUserService" or "LdapV3A-DUserService" in place of the standard UserService in NiagaraAX.

If the kerberos attribute is "true", the Niagara 4 host is licensed for Kerberos authentication with LDAPv3.

<feature name="ldapv3" expiration="never" kerberos="true" parts="ENG-WORKSTATION"/>

mobile

This enables the host to support the Mobile application framework, for station support of web browser access from mobile devices like cell phones or tablets. The host also requires to be licensed with the box feature for Bajascript support.

<feature name="mobile" expiration="never" history="true" schedule="true" alarm="true" px="true" propsheet="true" parts="ENG-WORKSTATION"/>

provisioning

This enables the operation of Niagara host provisioning, typically used to automate routine maintenance of Niagara system such as JACE software upgrades, file distribution and backups. It applies to a Supervisor platform only. Provisioning uses the BatchJobService and a "network extension model" (for example a "ProvisioningExt" under the NiagaraNetwork), sourced respectively from modules batchJob and provisioningNiagara.

<feature name="provisioning" expiration="never"/>

search

This enables the SearchService and the use searches in the station (New in Niagara 4). Without this feature, the SearchService remains in fault, and the "Quick Search box" and Search sidebar are unavailable.

The "local" attribute must be true to allow searches local to this station. The "system" attribute is for a future release of Niagara 4 (e.g. 4.1) where searches can span across multiple stations.

<feature name="search" local="true" system="true" expiration="never"/>

template

This enables the TemplateService and the use of templates in the station (New in Niagara 4). Without this feature, the TemplateService remains in fault, as well as templates.

<feature name="template" expiration="never"/>

Global capacity licensing

In Niagara 4, a new licensing model is more widely-used for some platforms, among them the newest JACE controller (JACE-8000): Global capacity licensing. Specific resources in the station are tracked using global counters, providing more flexibility in how resources are allocated.

Using a license feature named “globalCapacity”, the station keeps a global count of all networks, devices, proxy points, links, histories and schedules. When one of these resources goes over a licensed limit, the resource either goes into fatal fault or becomes inactive.

The content of any particular global capacity license depends on the feature purchased for the controller.

Example of globalCapacity feature entry

<feature name="globalCapacity" expiration="2016-04-01" point.limit="1250" device.limit="50" excludedDevices="ndio;nrio;niagaraDriver" excludedPoints="ndio;nrio;niagaraDriver"/>

The example above sets global limits on points (1250) and devices (50), but no limits on networks, links, histories, or schedules. The excludedDevices and excludedPoints attributes mean that there is no limit on the number of devices and points from these modules: ndio, nrio or niagaraDriver.

A more restrictive global capacity example feature could look like below.

<feature name="globalCapacity" expiration="never" network.limit="3" device.limit="25" point.limit="500" link.limit="400" history.limit="125" schedule.limit="10" excludedNetworks="nrio" excludedDevices="nrio" excludedPoints="nrio"/>

The example above indicates:

- A limit of three networks of any kind
- A limit of 25 devices of any kind,
- A limit of 500 points of any kind
- A limit of 400 links of any kind.
- A limit of 124 histories and 10 schedules of any kind.

Attributes allow for excludedNetworks, excludedDevices, and excludedPoints, each as a comma-separated list of modules. This means that there is no limit for nrio networks, Devices and ports. Any modules in these attributes are excluded from the respective global capacity limit. However all links, histories, and schedules from these modules are not excluded from any other global capacity counts.

Note:

All stations include an AuditHistory and LogHistory, which are included in the history limit.

Capacity licensing operation and recount

Often you delete as well as add resources in the process of engineering a station. It is important to note that capacity licensing never decrements any resource counter. This could result in inaccurate counts over a long period of time.

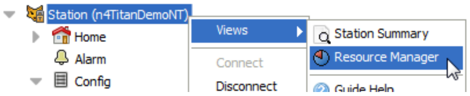
Note:

Therefore, any resource created with an over-capacity error will never get out of fault; you must delete it. Global capacity counts are corrected on station restart. However since this is often inconvenient, a global capacity recount is done approximately every 10 minutes to correct any inflated counts. You can always see the recount status, along with the current global licensing counts and limits in the station’s Resource Manager view (or “spy” view). See the next section “Checking capacity licensing status”.

Checking capacity licensing status

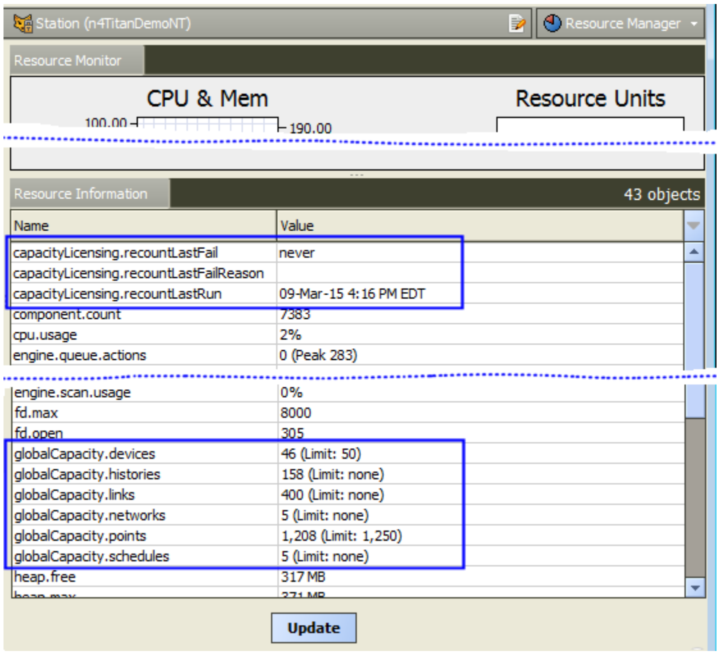
Any station running on a platform with global capacity licensing keeps a running tally on all corresponding resources in the Resource Manager view.

Figure 138: Accessing a station's Resource Manager view



In Workbench, right-click the opened Station, and select Views→ Resource Manager. Any station with global capacity licensing has specific entries in the lower "Resource Information" table.

Figure 139: Example entries for global capacity licensing in a station's Resource Manager view.



Name	Value
capacityLicensing.recountLastFail	never
capacityLicensing.recountLastFailReason	
capacityLicensing.recountLastRun	09-Mar-15 4:16 PM EDT
component.count	7383
cpu.usage	2%
engine.queue.actions	0 (Peak 283)
engine.scan.usage	0%
fd.max	8000
fd.open	305
globalCapacity.devices	46 (Limit: 50)
globalCapacity.histories	158 (Limit: none)
globalCapacity.links	400 (Limit: none)
globalCapacity.networks	5 (Limit: none)
globalCapacity.points	1,208 (Limit: 1,250)
globalCapacity.schedules	5 (Limit: none)
heap.free	317 MB
heap.max	371 MB

As shown above, there are three "capacityLicensing.recount" statistics, including a timestamp for when the global capacity recount last ran.

Another group of "globalCapacity.resource" statuses show the current counts along with respective license limits (if any). The station view above reflects the first globalCapacity example given, namely:

<feature name="globalCapacity" expiration="2016-04-01" point.limit="1250" device.limit="50" excludedDevices="ndio;nrio;niagaraDriver" excludedPoints="ndio;nrio;niagaraDriver"/>

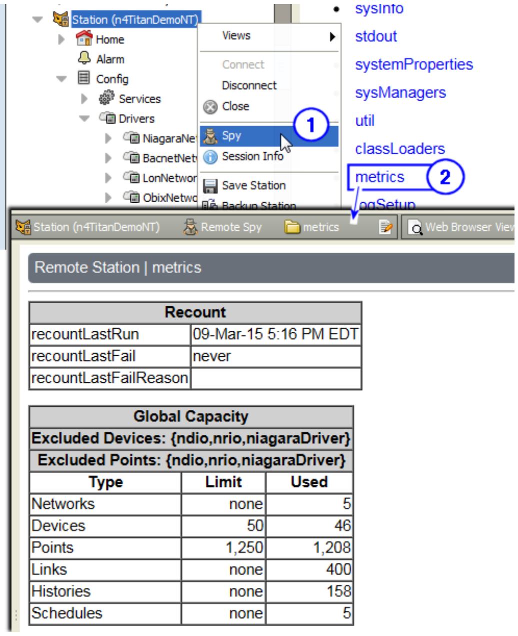
where global limits exist only on devices (Limit: 50) and proxy points (Limit: 1,250) with ndio, nrio and niagaraDriver devices and points being excluded from any limits.

Alternatively, if you are a super user, you can get this same information from the right-click spy page on a station, at the following location: Spy→ metrics.

Note:

Special permission is required to view spy pages.

Figure 140: Capacity licensing information in the station Spy pages



Remote Station | metrics

Recount	
recountLastRun	09-Mar-15 5:16 PM EDT
recountLastFail	never
recountLastFailReason	

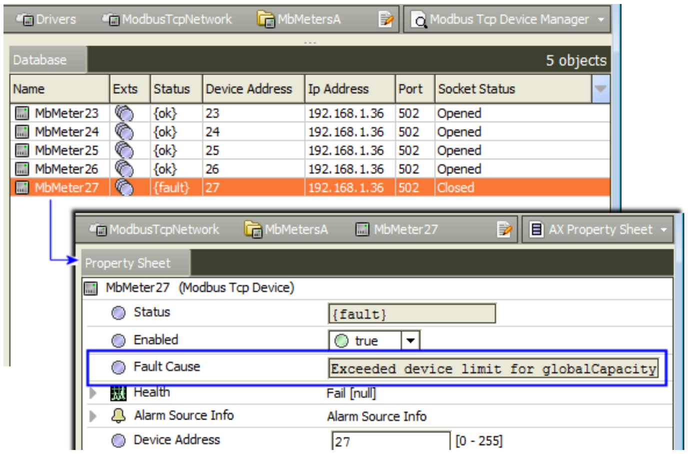
Global Capacity		
Excluded Devices: {ndio,nrio,niagaraDriver}		
Excluded Points: {ndio,nrio,niagaraDriver}		
Type	**Limit**	**Used**
Networks	none	5
Devices	50	46
Points	1,250	1,208
Links	none	400
Histories	none	158
Schedules	none	5

Information in the spy page above matches the Resource Manager view example shown, with the exception of the “recountLastRun” timestamp shown (one hour later).

Capacity licensing fault notifications

Added components that exceed global capacity limits provide a “Fault Cause” explaining the reason. In the prior example, where there are 46 global existing devices globally, if five (5) new ModbusTcpDevices are added this results in a fault, as 51 devices is one over the 50 limit.

Figure 141: Example of an added device exceeding the global capacity device limit



Name	Exts	Status	Device Address	Ip Address	Port	Socket Status
MbMeter23		{ok}	23	192.168.1.36	502	Opened
MbMeter24		{ok}	24	192.168.1.36	502	Opened
MbMeter25		{ok}	25	192.168.1.36	502	Opened
MbMeter26		{ok}	26	192.168.1.36	502	Opened
MbMeter27		{fault}	27	192.168.1.36	502	Closed

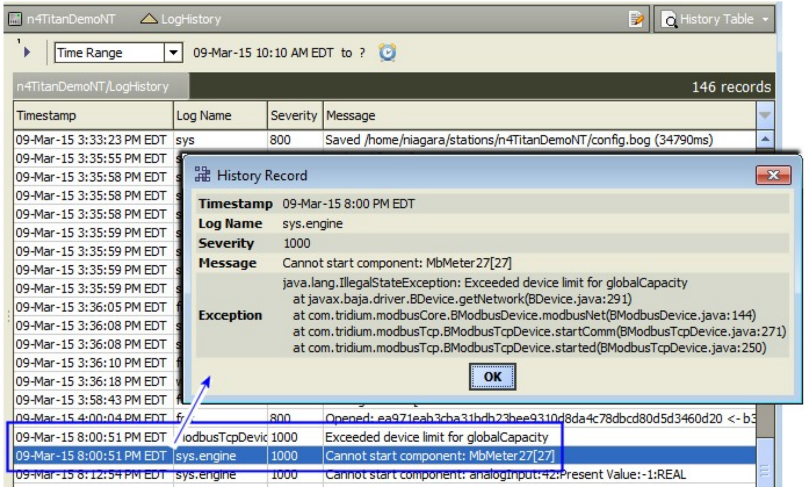
MbMeter27 (Modbus Tcp Device)

Status	{fault}
Enabled	true
Fault Cause	Exceeded device limit for globalCapacity
Health	Fail [null]
Alarm Source Info	Alarm Source Info
Device Address	27 [0 - 255]

As shown above, the property sheet of the device shows this reason in Fault Cause. You must delete this (or any) component with a similar fault cause. Otherwise it remains in fault.

Note that corresponding events are also entered in the station’s LogHistory, as shown here.

Figure 142: LogHistory entries from exceeding globalCapacity



09-Mar-15 10:10 AM EDT to ?

n4TitanDemoNT/LogHistory — 146 records

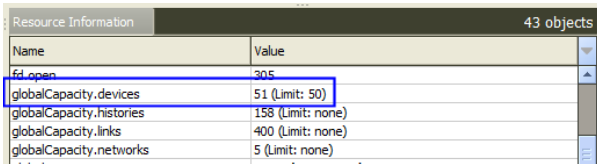
Timestamp	Log Name	Severity	Message
09-Mar-15 3:33:23 PM EDT	sys	800	Saved /home/niagara/stations/n4TitanDemoNT/config.bog (34790ms)
09-Mar-15 3:35:55 PM EDT	s		
09-Mar-15 3:35:58 PM EDT	s		
09-Mar-15 3:35:58 PM EDT	s		
09-Mar-15 3:35:58 PM EDT	s		
09-Mar-15 3:35:59 PM EDT	s		
09-Mar-15 3:35:59 PM EDT	s		
09-Mar-15 3:35:59 PM EDT	s		
09-Mar-15 3:35:59 PM EDT	s		
09-Mar-15 3:36:05 PM EDT	f		
09-Mar-15 3:36:08 PM EDT	s		
09-Mar-15 3:36:08 PM EDT	s		
09-Mar-15 3:36:10 PM EDT	f		
09-Mar-15 3:36:18 PM EDT	w		
09-Mar-15 3:58:43 PM EDT	f		
09-Mar-15 4:00:04 PM EDT	f	800	Opened: ea971eab3cba31bdb23bee9310d8da4c78dbcd80d5d3460d20 <- b3
09-Mar-15 8:00:51 PM EDT	iodbusTcpDevic	1000	Exceeded device limit for globalCapacity
09-Mar-15 8:00:51 PM EDT	sys.engine	1000	Cannot start component: MbMeter27[27]
09-Mar-15 8:12:54 PM EDT	sys.engine	1000	Cannot start component: analogInput:42:Present Value:-1:REAL

History Record

Timestamp	09-Mar-15 8:00 PM EDT
Log Name	sys.engine
Severity	1000
Message	Cannot start component: MbMeter27[27]
Exception	java.lang.IllegalStateException: Exceeded device limit for globalCapacity at javax.baja.driver.BDevice.getNetwork(BDevice.java:291) at com.tridium.modbusCore.BModbusDevice.modbusNet(BModbusDevice.java:144) at com.tridium.modbusTcp.BModbusTcpDevice.startComm(BModbusTcpDevice.java:271) at com.tridium.modbusTcp.BModbusTcpDevice.started(BModbusTcpDevice.java:250)

As shown below, the globalCapacity count for any exceeded resource appears in the corresponding entry in the station’s Resource Manager.

Figure 143: Example globalCapacity entry for a resource over license limit

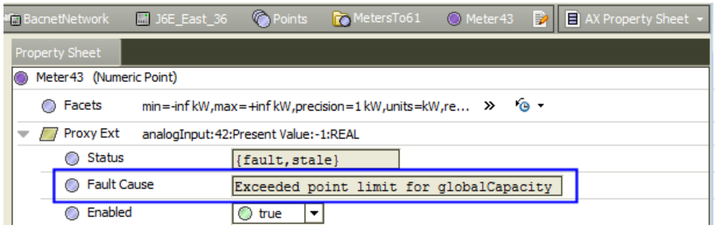

Resource Information — 43 objects

Name	Value
fd.open	305
globalCapacity.devices	51 (Limit: 50)
globalCapacity.histories	158 (Limit: none)
globalCapacity.links	400 (Limit: none)
globalCapacity.networks	5 (Limit: none)

Note that the necessary deletion of an over-limit device (51) does not decrement the count back at that time. Instead, a periodic recount (about every 10 seconds) or station restart is needed for this.

Similar component faults and error logs apply to networks, points, links, and schedules.

Figure 144: Example globalCapacity fault for proxy point



Meter43 (Numeric Point)

Facets	min=-inf kW,max=+inf kW,precision=1 kW,units=kW,re...
Proxy Ext	analogInput:42:Present Value:-1:REAL
Status	{fault,stale}
Fault Cause	Exceeded point limit for globalCapacity
Enabled	true

As shown above, the ProxyExt for a proxy point shows a Fault Cause reason. The property sheet of a network in global capacity fault is similar; it shows the Fault Cause reason: Exceeded network limit for globalCapacity. This applies also to a schedule in global capacity fault; it shows the Fault Cause reason: Exceeded schedule limit for globalCapacity.

Exceeding the globalCapacity link limit produces a popup Capacity Licensing window on the wire sheet or active view, saying “Exceeded Link Limit”, and the link is not functional.

Histories exceeding globalCapacity limits can manifest in different ways. See the next section, “Capacity licensing notes about histories”.

Capacity licensing notes about histories

Histories in the station are being counted. If the number of histories in the station is greater than the global capacity limit, then the resource counter in the station prevents more histories from being created.

In the default History Ext Manager view on the HistoryService, you see a table of all history extensions along with the state of each (enabled, disabled, fault). Included is a total count of all history extensions. However, there is no easy, intuitive way to get a count of those in a particular state or set of states. An extension in a fault state with a Fault Cause of Exceeded history limit" indicates a related problem. Simply disabling such an extension does not fix the issue. You must delete the history in the history database, which cannot be done from the HistoryService.

You delete histories from the Database Maintenance view of the History space; but note there are no counts available there. If you delete one or more histories to reduce history count, you must wait until the periodic recount (approximately every 10 seconds) comes around to see the reduced count. However, you cannot delete the history extension that created the history from there. So it is likely that the history is going to be recreated in the future, unless you delete or modify the history extension that created the history database table.

Note that in addition to history extensions in the same station, other items can create histories, including:

- History imports in the same station
- History exports in another station
- AuditHistory service
- LogHistory service

These activities add to the count. This is the reason why a station quickly exceeds its history limit.

CHAPTER 6 TIME ZONES

The following topics are covered in this chapter:

- Time zones and terminology
- Selecting a time zone

Platform configuration of a Niagara host includes specifying its time zone. This affects both real time clock accuracy used in station control, and also how timestamps appear in items like histories and alarms. This chapter provides details on time zone selection in Niagara 4, including the currently used “historical time zone database.”

Note:

Workbench provides a special “Time Zone Database Tool” that lets you explore the historical time zone database on the local host.

Time zones and terminology

A time zone is a region in the world that uses the same standard time, often referred to as the local time. There are many different time zones, owing to the combinations of geographic locations and political/cultural differences. Time zones calculate their local time as an offset from UTC (Coordinated Universal Time). In addition, many time zones apply DST (Daylight Saving Time).

UTC

Coordinated Universal Time (UTC) is the recognized atomic-clock standard of reference time, largely replacing GMT (Greenwich Mean Time) as reference time. Time zones are commonly expressed as negative or positive offsets from UTC time.

DST

Daylight Saving Time (DST) is used as a means of maximizing daylight hours during normal waking hours, and is used by many (but no means all) time zones. DST is a twice-yearly event acting upon local time, as follows:

- Start of DST adds an offset (typically 1 hour) to local time. During this period of the year, local time may be called “daylight time.”
- End of DST removes the DST offset from local time. During this period of the year, local time may be called “standard time.”

Any time zone using DST has specific rules that define the exact days and times when DST starts and ends. These rules vary widely from zone to zone, since DST policies are set by national and regional governments. Also, DST policies are subject to change for this same reason—as in the recent 2007 change for all U.S. time zones that observe DST.

In the 2007 U.S. DST changes, the DST start time was changed to “first Sunday on or after the 8th in March” (from “first Sunday on or after the 1st in April” for 2006 and prior years). The DST end time was changed to “first Sunday on or after the 1st in November” (from “last Sunday in October” for 2006 and prior years).

Note:

A change in DST rules for a time zone can cause issues in Niagara when displaying historical data (histories and alarm records), particularly when applying new (current) DST rules to records collected using prior (old) DST rules. For more details, see the section “About the historical time zone database”.

Selecting a time zone

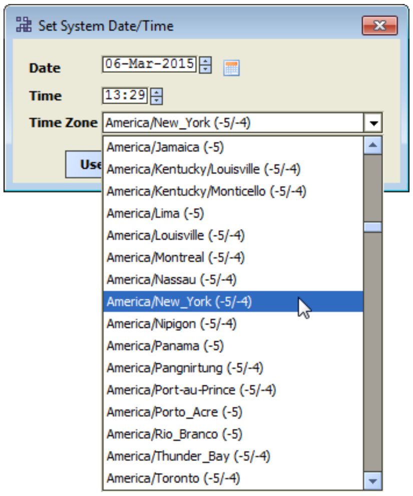
Platform configuration of a Niagara host includes the setting of date and time, which includes specifying its local time zone.

Note:

For any Niagara 4 Windows host, you must use Windows tools to specify a time zone and/or change date and time. Such tasks, as well as TCP/IP configuration on a Windows host, are read-only.

Typically, you specify time zone in a JACE controller during its initial commissioning in a platform connection, when running the Commissioning Wizard. Or, you can do this at any time using the Platform Administration view (function “Change Date/Time”).

Figure 145: Selecting time zone from Change Date/Time selection in Platform Administration View



Date 06-Mar-2015

Time 13:29

Time Zone America/New_York (-5/-4)

After a station is installed and running, you can also specify a JACE’s time zone using one of the station’s PlatformService views (“Platform Service Container Plugin” or “System Date and Time Editor”).

In any case, time zones appear on a selection list with a format such as:

Zone ID (± hours UTC offset DST,± hours UTC offset UST).

For example:

America/Chicago (-6,-5) Europe/Berlin (+1,+2) Asia/Tokyo (+9)

Note there is no DST observance in Japan, so the selection with zone ID “Asia/Tokyo” shows only the UTC offset of +9 hours. This selection list of time zones is from a historical “time zone database”.

Note:

Unlike in NiagaraAX, in Niagara 4 there is no separately maintained “timezones.jar” distributed in Niagara builds for a time zone database, nor associated entries in a platform’s system.properties file. Instead, time zones are directly sourced from the Java VM (virtual machine) in the host platform.

This means there is no longer a workflow for updating time zone definitions independently from Java updates that may be included in Niagara 4 updates.

About historical time zone database

The Java-sourced time zone database has a “historical perspective,” where a history of changes for applicable time zones is stored. Thus, multiple definitions for a time zone may exist, including past definitions as well as its current definition.

This allows display of a station’s time stamped data (histories and alarms) collected in time zones under “prior rules” (typically DST-related) to display with the original (and correct) collected time.

Note:

On all Niagara 4 JACE controller platforms, the Java-sourced time zone database is historically accurate only back to year 2010. Any pre-2010 historical data is displayed using 2010 rules. This was done to improve Java heap usage on these platforms.

However, note the Java-sourced time zone database on Windows Niagara 4 platforms extends further back, for example, to year 1995.

In Workbench, select Tools→ Time Zone Database Tool to navigate the Java time zone database, where you can explore DST rules for any timezone. If a local station is running on the same host (Supervisor), this is time zone database that is utilized.

LG Customer Information Center, Commercial Products

1-888-865-3026 USA

Follow the prompts for commercial A/C products and parts.

LG Electronics, U.S.A., Inc.
Commercial Air Conditioning Division
4300 North Point Parkway
Alpharetta, Georgia 30022
www.lghvac.com