Technical Document

JACE-9000 Install and Startup Guide

July 15, 2023

niagara4

JACE-9000 Install and Startup Guide

Tridium, Inc.
3951 Westerre Parkway, Suite 350
Richmond, Virginia 23233
U.S.A.

Confidentiality

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

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

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

Trademark notice

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

Copyright and patent notice

Contents

About this guide

This topic contains important information about the purpose, content, context, and intended audience for this document.

Product Documentation

This document is part of the Niagara technical documentation library. Released versions of Niagara software include a complete collection of technical information that is provided in both online help and PDF format. The information in this document is written primarily for Systems Integrators. To make the most of the information in this book, readers should have some training or previous experience with Niagara software, as well as experience working with JACE network controllers.

Document Content

This document describes the initial Niagara 4 software installation and configuration for a controller, using Workbench (versions Niagara 4.1 and later).

The information in this document is intended for an engineer, technician, or service person who is performing control system installation. All information in this document is also available in the in Workbench help system. For physical mounting and wiring details for any controller, please refer to its specific hardware installation document. This document does not cover station configuration or Niagara 4 components. For more information on these topics, please refer to online help and various other Niagara 4 software documents.

Document change log

Updates (changes and additions) to this document are listed below.

July 15, 2023

Initial document release.

Related documentation

Additional related information is available in the following document(s).

- *JACE-9000 Backup and Restore Guide*
- *Niagara Platform Guide*

Chapter 1   Preparation

Topics covered in this chapter

♦ Factory-shipped state
♦ Requirements
♦ Preparing to license without an Internet connection
♦ Preparing to commission the controller
♦ Opening a platform connection to the controller

In most cases, you perform the initial software installation and startup of the controller in your office, before physically mounting it in place at a job site. The remainder of this document assumes that you have the controller nearby, and are able to power it on and off as needed. After you complete the commissioning process described in this document, you can mount and wire the controller at the job site, making permanent mounting and wiring connections.

Niagara 4 uses the TLS (Transport Layer Security) protocol to provide communication authentication and encryption. It supports TLS versions 1.0, 1.1, 1.2, and 1.3. For details, refer to the *Niagara Station Security Guide*.

When using Workbench, the default **Open Platform** and **Open Station** operations initially assume a **Platform TLS Connection** and a **Fox TLS Connection**. This is intended to encourage TLS usage for all Niagara 4 platforms and stations. If necessary, you can change either connection type, and Workbench remembers this type to use on your next connection. You can change back to original settings again, as needed.

Factory-shipped state

The controller is configured at the factory with an IP address, HTTP port and platform credentials.

When shipped, a new controller is pre-configured with an IPv4 address in the range: `192.168.1.140` with a primary **LAN1** port. Its **LAN2** port is disabled. The unit's default subnet mask is: `255.255.255.0`. You change these IPv4 network settings during your startup commissioning of the controller.

When shipped, the controller's, platform daemon is configured to listen on HTTPS port 5011. Often, this is left at default. However, if a different port is needed for a platform connection, perhaps for firewall reasons, you can change this during the commissioning of the controller.

Controllers are shipped with default platform daemon (administrator) username, password, and passphrase credentials. Following are the default credentials.

Default credential	Value
username	admin
password	admin
passphrase	admin

Initially, you use the factory default credentials to open (to log in) a platform connection to the controller. Like the factory-assigned IP address, default credentials are temporary. During your startup commissioning, you must replace this platform admin account with at least one different platform admin user. Be sure to guard the credentials for such platform users closely.

NOTE: The Niagara 4 Commissioning Wizard does not allow you to commission and startup a controller while retaining the factory platform user.

microSD card

The microSD card is the primary storage medium for all data and configuration options related to the software installation. Since the microSD card can be easily removed and the data duplicated, files are stored in encrypted format and decoded on the fly as they are accessed.

Sensitive data include the following:

*   Credentials (OS and others)

*   Niagara key material

*   Certificates and their private key files

The system is designed to protect these data while at the same time allowing you to move a microSD card from a failed controller to a replacement controller.

Inserting or removing the microSD card

The optional microSD card that ships with a new controller is inserted in the unit prior to the mounting process. However, it is possible to move an SD card from one unit to another. For example, you might want to remove the card from a unit that suffered a hardware failure and install it in a replacement controller.

Prerequisites: All power to the controller is off. The controller has been removed from the DIN rail or screw-tab mounting. You have discharged any static electricity accumulated by touching a known, securely grounded object.

To insert the microSD card:

Step 1   Slide the microSD card shutter open.

The shutter should remain captive in the base, revealing the microSD card socket.
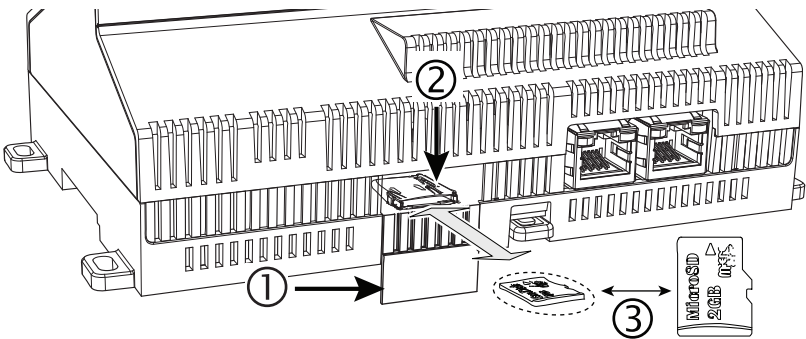
1	Shutter access to microSD card
2	Card socket
3	microSD card

Step 2   Make either of the following changes, as needed:

*   Insert the microSD card by sliding the card into the card socket, label side up, until the spring catch engages. If properly inserted, the card is behind the shutter track.

*   Remove the microSD card by pushing the card in until the spring release pushes the card partially out of the card socket. Grasp the card and pull it completely out of the unit. Store the card in a static free protective case.

Step 3   Carefully slide the card shutter back over the card socket opening until it clicks securely into place.

When properly closed, the shutter should not protrude behind the mounting base.

Requirements

These instructions assume that you have a PC that is running a licensed copy of NiagaraWorkbench and that the `installation tool` option was chosen and included as part of the Workbench installation. This option copies distribution files to the PC that are needed for commissioning various models of controllers.

Your PC must meet minimum hardware and operating system requirements. This includes a working Ethernet adapter with TCP/IP support (browser capable). An Ethernet TCP/IP connection to the controller is required to install Niagara software and configure other properties.

For this initial Ethernet connection, you can use either:

- An Ethernet patch cable connected directly between your PC and the controller (if your PC Ethernet port is not auto-sensing, you will need an Ethernet crossover cable), or

- A normal LAN connection, meaning that both your PC and the controller are physically connected to the same Ethernet hub or switch.

Preparing to license without an Internet connection

The controller license is required during commissioning. Typically, the license file for the controller already resides on the licensing server, where (if you have Internet connectivity) the Commissioning Wizard automatically retrieves it during the licensing step. If your Workbench PC will not have Internet connectivity when you are commissioning the JACE, you can still install the controller license during commissioning.

Prerequisites: A license for the controller (.lar file) was emailed to you.

Step 1   To make the file available to Workbench, copy the file to your `!security/licenses/inbox` folder

Step 2   Restart Workbench.

Preparing to commission the controller

To commission a new controller requires a connection using an Ethernet patch cable and TCP/IP configuration.

Prerequisites: You have installed a version of Niagara on the PC including its permanent license. The license file for the controller is on the licensing server and you have Internet access or you received the license via email and copied the file to the license inbox.

Step 1   Mount the controller on a rack or table in your office near your PC.

Please refer to the wiring details in the appropriate *JACE-9000 Controller (15885) Mounting and Wiring Guide* for information on temporary power wiring and Ethernet wiring connections.

CAUTION: The JACE-9000 is not compatible with a Power-Over-Ethernet (POE) network. Connecting the controller on a network segment which carries power causes the unit to fail (lockup). In that event, you must disconnect it from the POE network segment and cycle power to the unit.

Step 2   Attach one end of a standard category-5 Ethernet unshielded twisted pair (UTP) patch cable to the RJ-45 Ethernet connector for LAN1 (labeled PRI) on the JACE.

Step 3   Attach the other end of the patch cable to a network port or directly to an Ethernet hub.

Step 4   Power up the controller.

Step 5   Do one of the following:

- Record your PC's current IP settings, then re-assign your PC's IP address for its Ethernet NIC (network interface card). If necessary, refer to Windows online Help for details on configuring TCP/IP settings.

- Obtain a USB-to-Ethernet network adapter (second network interface card, or NIC), and use it with an Ethernet crossover cable to commission the controller. In this case, configure this

second NIC to use the settings in the remainder of this step.Use a serial shell mode connection to the controller to re-assign its factory IP address settings. After making this change and re-booting the controller, you can continue commissioning using Workbench. This requires a USB-to-USB—C adapter cable, VCP driver, and a special power-up mode for the controller.

VCP (Virtual COM Port) drivers cause a USB device to be shown as an additional COM port available to the PC. Using terminal emulation software, such as PuTTY or ClearTerminal, the PC can access the USB device in the same way as it would access a standard COM port. VCP driver downloads are available at www.ftdichip.com and other sites.

Step 6   For this initial connection to a factory-shipped JACE, configure your PC's NIC to use an IP address in the same subnet as the JACE, as well as a matching subnet mask.

Set the IP address in the range: `192.168.1.1` to `192.168.1.254`.

With a subnet mask of `255.255.255.0`.

NOTE: Do not assign your PC the identical IP address as the JACE's factory-assigned IP address.

Step 7   From your PC, start Workbench.

The Nav tree should be visible in the side bar area (left pane).

Step 8   If the Nav tree is not visible, from the menu bar, select **Window→Side Bars→ Nav**.

Opening a platform connection to the controller

A platform connection to any controller is required for most host-level operations. This includes installing Niagara core software and modules and performing various other platform tasks.

Prerequisites: The JACE has been powered up.

Step 1   From the menu bar, select **File→Open→Open Platform**.

The **Open Platform** window opens.
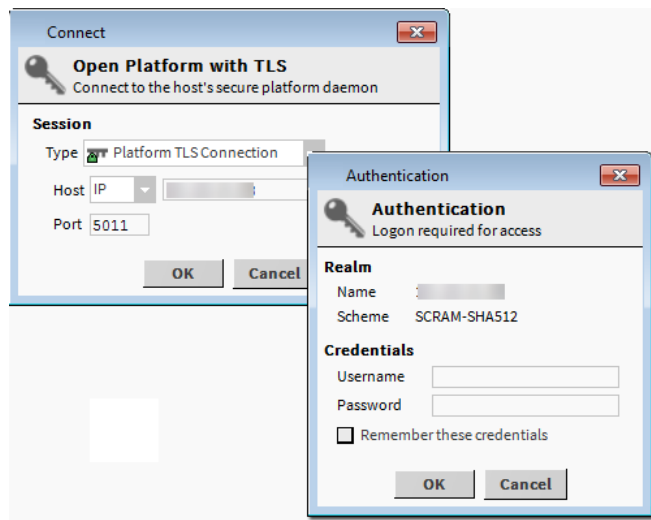
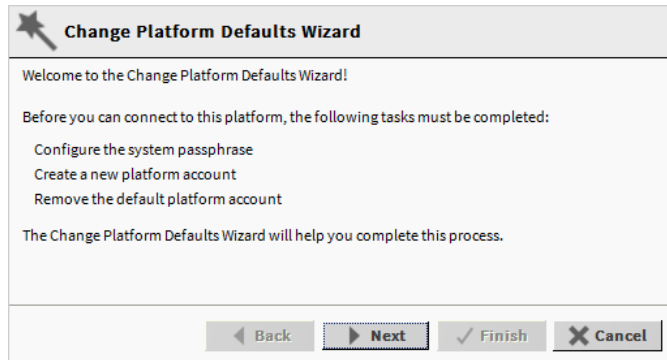Step 2   Complete the properties in the **Open Platform** window and click **OK**.

- `Type` defaults to **Platform TLS Connection**.
- `Host` defaults to **IP**. Do not change this, but enter the new controller's IP address.
- `Port` defaults to `5011`. Leave it at this default setting.

The **Authentication** window opens.

Step 3   Enter the Platform's default `Username` and `Password` and click **OK**.

For example, **Username** may default to admin. **Password** may default to admin.

If Workbench detects factory default credentials when connecting to a remote platform it launches the **Change Platform Defaults Wizard** (shown here) which forces you to change the factory defaults prior to completing the platform connection.

Change Platform Defaults Wizard

Welcome to the Change Platform Defaults Wizard!

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

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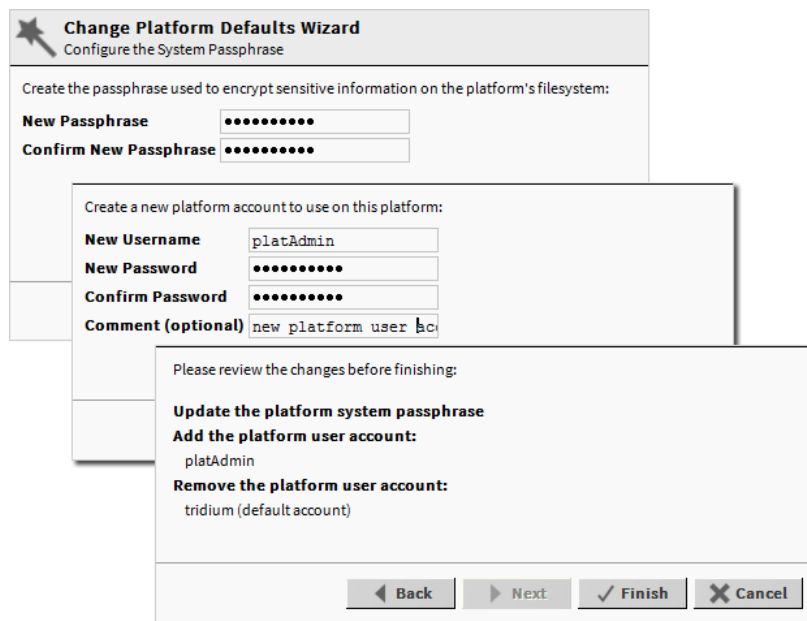Create a new platform account
Remove the default platform account

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

◀ Back   ▶ Next   ✓ Finish   ✗ Cancel

If this wizard does not display the platform connection completes.

Step 4   Do one of the following:

- If the **Change Platform Defaults Wizard** displays, click **Next** and step through creating a system passphrase, creating a new platform account, and removing the default platform account.

Change Platform Defaults Wizard
Configure the System Passphrase

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

New Passphrase   ●●●●●●●●●●
Confirm New Passphrase ●●●●●●●●●●

Create a new platform account to use on this platform:

New Username   platAdmin
New Password   ●●●●●●●●●●
Confirm Password   ●●●●●●●●●●
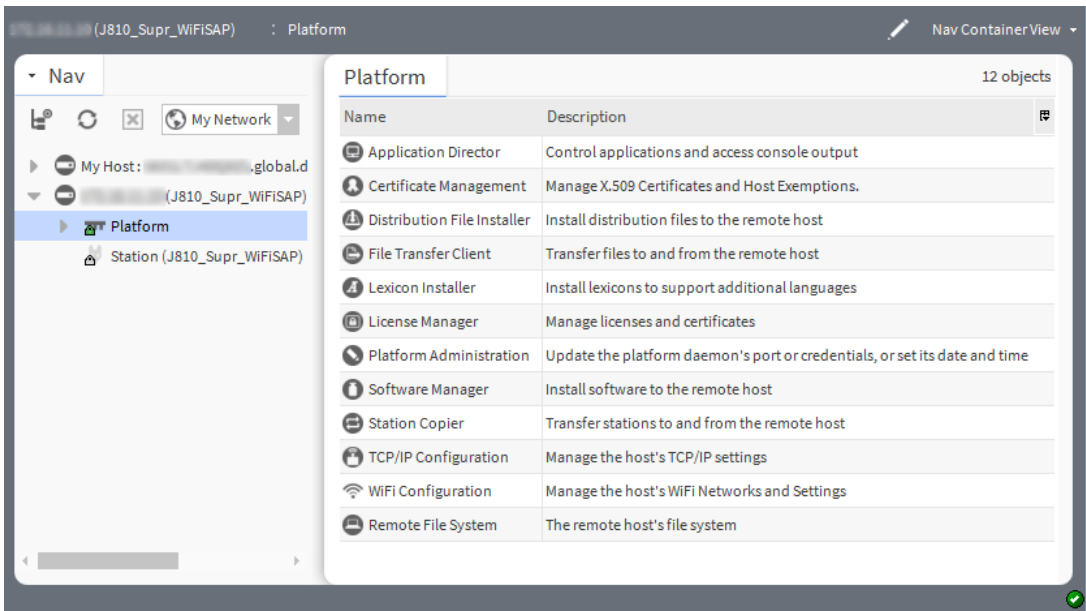**Comment (optional)** new platform user ac

Please review the changes before finishing:

Update the platform system passphrase
Add the platform user account:
    platAdmin
Remove the platform user account:
    tridium (default account)

◀ Back   ▶ Next   ✓ Finish   ✗ Cancel

- Click **Finish** to complete these changes.

On completion, the platform opens in the Nav tree, and its **Nav Container View** displays in the view pane.

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

After you open a platform connection, you can run the Commissioning Wizard.

Chapter 2   Commissioning

Topics covered in this chapter

♦ Starting the Commissioning Wizard
♦ Installing the controller licenses
♦ Preparing software to install
♦ Configuring TCP/IP settings
♦ Configuring the system passphrase
♦ Setting up platform users
♦ Reviewing and finishing the Commissioning Wizard

When you connect the controller for the first time, you first need to commission the controller. The commissioning of the controller loads drivers, configures password protection, installs the controller's license, sets up platform users, configures TCP/IP, and installs software modules. The Commissioning Wizard works for commissioning a new controller or upgrading an existing controller.

Commissioning steps include:

- Request or install software licenses—preselected for any new controller.

- Set enabled runtime profiles—preselected and read-only for any new unit.

- Install a station from the local computer—recommended. Optionally, you can install station(s) at a later time.

- Install lexicons to support additional languages—option to install file-based lexicon sets (alternative to lexicon modules). Typically, you leave this cleared—lexicon modules are required in N4.

- Install/upgrade modules—always preselected when you run the wizard. Used to select the software modules, and optionally any lexicon modules.

- Install/upgrade core software from distribution files—preselected and read-only for any new unit.

- Sync with my local system date and time—preselected in most cases (new JACE for example, where controller time may greatly differ from actual time).

- Configure TCP/IP network settings—recommended.

- Remove platform default user account—preselected and read-only for a new unit. You cannot commission a unit with the factory default platform user.

- Configure additional platform daemon users—recommended option if you require additional platform admin user accounts, with unique user names and passwords (all have full equal privileges).

Starting the Commissioning Wizard

This topic explains how to run the `Commissioning Wizard` using series of steps to configuring a host to run the stations.

Prerequisites: You are using Workbench and have opened a platform connection to the controller.

Step 1   To open the Commissioning Wizard, do one of the following.

- In the Nav tree, right-click **Platform→Commissioning Wizard**.

- In the Nav tree, expand **Platform→Platform Administration** and click **Commissioning**.

The **Commissioning** window opens.
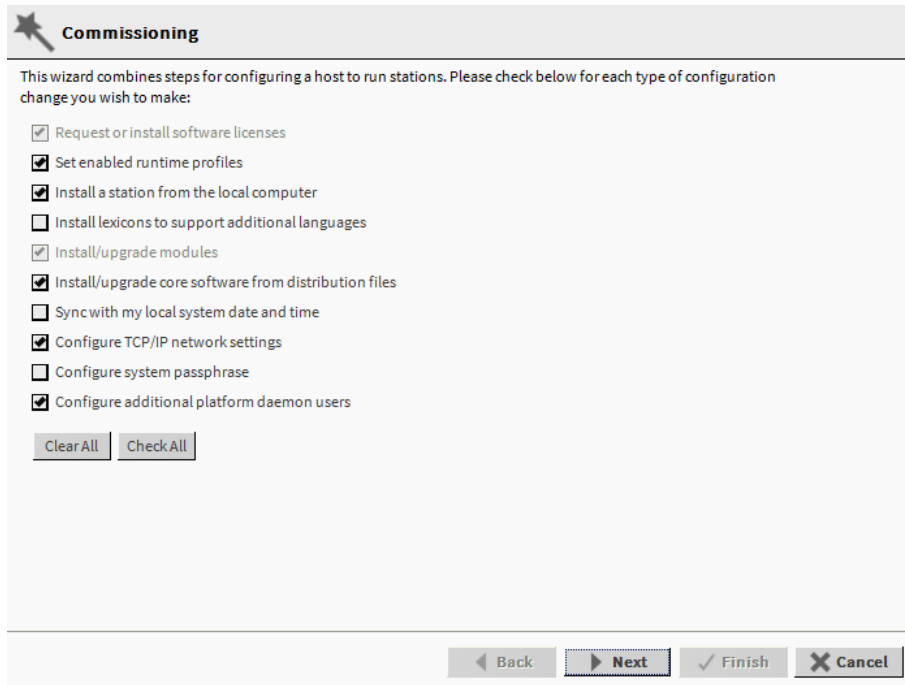
The screen capture shows the default selections for a new controller. By default, few steps are pre-selected. Steps are executed in the order listed in the wizard.

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

Step 2   Select **Check All** or **Clear All** to include or omit steps and click the **Next** to continue.

For a new controller, you typically accept all default selections.

During the license install step, the wizard checks to see if a `default` certificate is installed. This certificate is required by any Niagara host, to verify the license file. If other licenses are installed, additional certificates may also be required.
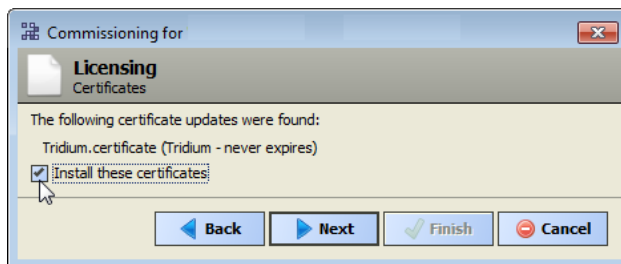
Step 3   Select **Install these certificates** and click **Next**.

The **Licensing** step opens.
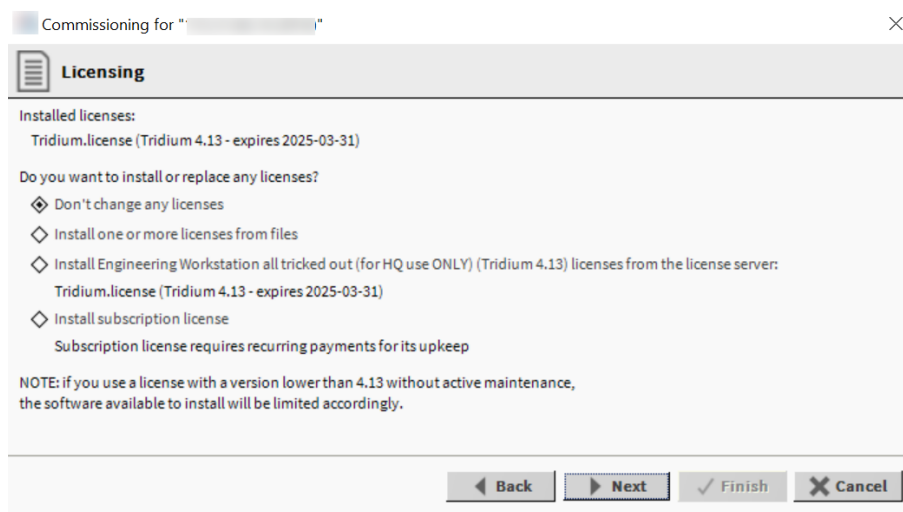
For license files validated against the Tridium certificate, installation can be automated from Workbench. All such purchased licenses, including controller, Supervisor and Workstation-only, are stored and available to Workbench through the licensing server.

If your PC currently has Internet connectivity while running a platform connection to any Niagara host, Workbench provides an install option to get and install the licenses for the host from the license server. When selected, Workbench silently searches the license server for a license with a matching Host ID of the target platform. When found, it selects the license(s) and advances to the next wizard step. For more details, refer to the *Niagara Platform Guide*.

Installing the controller licenses

Each controller requires at least one unique license that authorizes it to use Niagara. Other license files are not needed unless you use third-party module(s). If the PC doing the commissioning is connected to the Internet, the **Commissioning Wizard** can install all licenses automatically from the licensing server. This is the recommended method to install or update a license.

Prerequisites: You have at least one license file, specific to this controller, which is stored on the license server or you received a license for this controller via email. To install from the license server, you have Internet connectivity.

Step 1   Select the licensing option for the wizard to implement.

- `Don't change any licenses` This is the default choice.

- `Install one or more licenses from files`

- `Install licenses from the license server`

- `Install licenses from the workbench license database`

- `Install subscription license`

Step 2   To install a license from the server, select `Install licenses from the license server` and click **Next** to continue.

If the `Install licenses from the license server` option is not available in the wizard, Workbench has not detected Internet connectivity, and so cannot contact the licensing server.

When you select the license from the server, Workbench silently searches the license server for a license with a Host ID that matches the Host ID of the target platform. When found, it selects the license(s) and advances to the next wizard step. For more details, refer to the section "About the licensing server" in the *Niagara Platform Guide*.

Step 3   To install a license from your local Workbench database, select `Install licenses from the workbench license database`.

This option is not available if your local license database does not include a license for this controller.

Workbench locates the license, and the wizard advances to the next step.

Step 4   To install a license from a file, select `Install one or more licenses from files` and click **Next**.

The **Licensing** window opens.
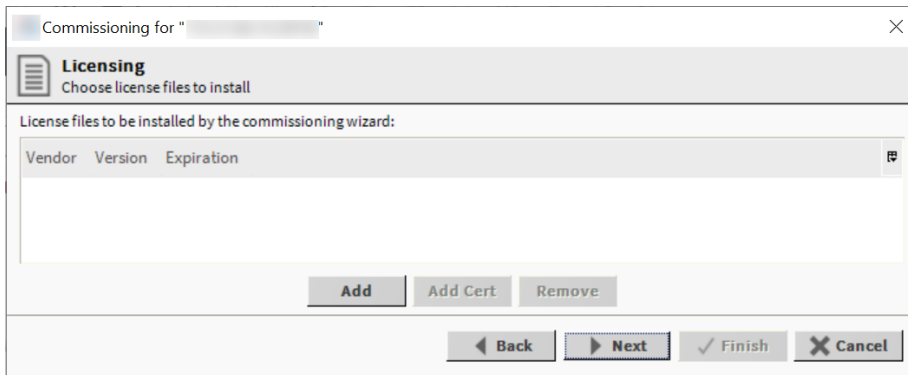
Step 5   Click the **Add** button.

The **Select File** window opens. If a license is not listed, navigate to its location using the Nav tree on the left.

The licensing tool prevents the selection of the wrong license (one with a different Host Id) when installing a license in the controller.

Step 6   Select the license file and click **OK**.

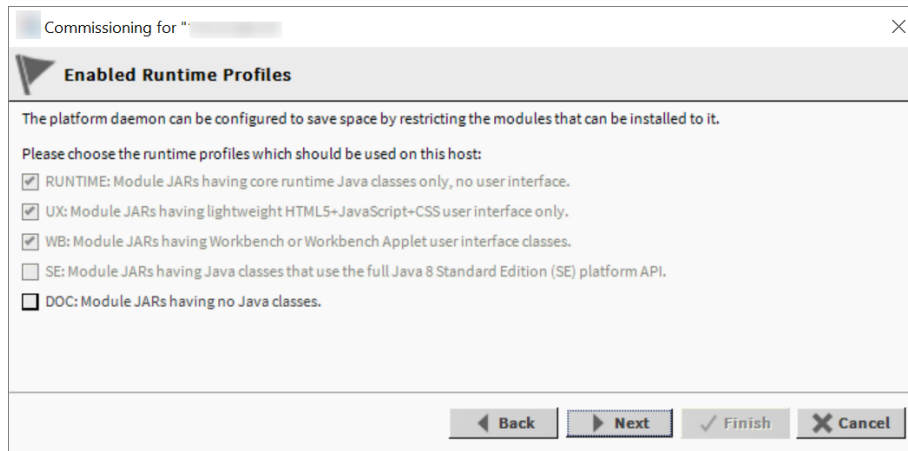Step 7   To add additional licenses, click **Add** again or, if all licenses are listed, click **Next** to continue.

Step 8   To install subscription license, Select `Install subscription license`.

The **info** window opens.
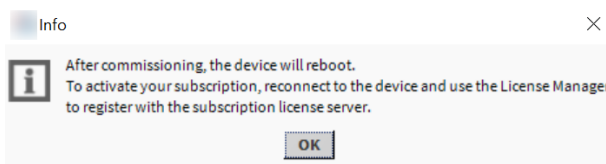
Step 9   To continue, click **OK** and click **Next**

The **Enable Runtime Profiles** step opens.

Preparing software to install

The topic explains installing software by stepping through the Commissioning Wizard. The next five wizard steps relate to installing software and a station.

Prerequisites: You are running the Commissioning Wizard and just completed the licensing step. If you plan to ask the wizard to install a station from your PC, you must know the station's passphrase.

The Enabled Runtime Profiles step saves space in the controller by restricting the modules that can be installed.

Step 1   Do one of the following.

- To install the documentation JAR files, leave the `DOC: Module JARs having to Java classes` box selected and click **Next** to continue.

- To save space on the controller, remove the check mark from this option box and click **Next**.

The other options are pre-configured for best results.

All Niagara 4 platforms require run time profiles. These runtime profiles should be used in the host:

- RUNTIME identifies the core modules with runtime Java classes only. These modules do not support the user interface.

- UX identifies bajaUX modules that support the user interface only.

- WB identifies the modules that support the Workbench user interface.

- SE identifies modules that support the full Java 8 Standard Edition. These are not available for QNX-based controllers.

- DOC identifies documentation modules. These are not recommended for file space reasons on a controller.

The **Station Installation** (Install a station from the local computer) window opens.

Step 2   Do one of the following:

- If this is a new controller and no station exists for it yet, click **Next**.

- If you are upgrading and the station already exists in the controller, select `Don't transfer station`.

- If you have the station on your PC, select the `Station` name and possibly give it a `New Name`.

Listed are station subfolders under in your Workbench **User Home**.

Step 3   If the station is on your PC, enter its `File Passphrase`.

If the passphrase for the local copy of the station is different from the remote host's system passphrase, you are prompted to enter the local copy's passphrase. If there is no passphrase mismatch, you are not prompted to enter one.

When you select the station, it automatically prompts to enter a passphrase.

Step 4   Select or clear the check boxes `START AFTER INSTALL`, `AUTO-START` and click **Next** to continue.

- `START AFTER INSTALL` starts the station immediately after it is copied. When you select this check box, the station is restarted at the end of commissioning, even if you do not reboot the controller.

- `AUTO-START` starts the station every time the platform daemon starts. In some commissioning scenarios, you may wish to disable (clear) both start options when installing a station, especially if commissioning ends in a reboot. This way the Commissioning Wizard installs the software modules needed by the station, along with all station files, but leaves the station idle.

    In this case, to start the station you must open a platform connection to the controller following the reboot and start the (now idle) station from the **Application Director** view. This allows you to see all standard output messages from the station as it transitions from idle to starting to started.

    If doing this, in the **Application Director** be sure to enable `AUTO-START` for the selected station. Otherwise, it will remain idle after the next controller reboot.

The **Station Installation** (Which station files are to be copied?) window opens.
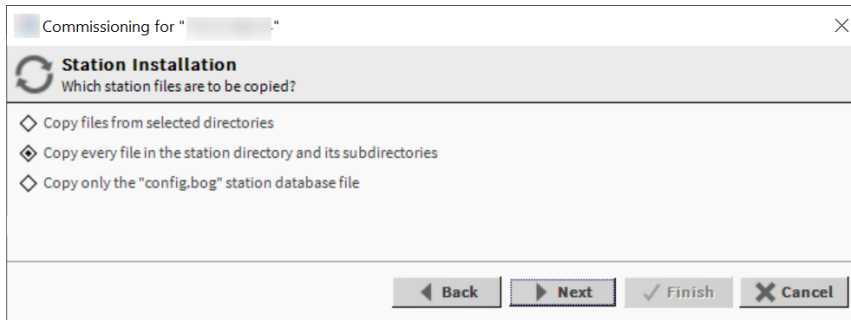
This window shows different options from which to copy station files.

- `Copy files from selected directories` specifies which subfolders under that local station that are copied. It opens a tree selection window upon **Next** button.
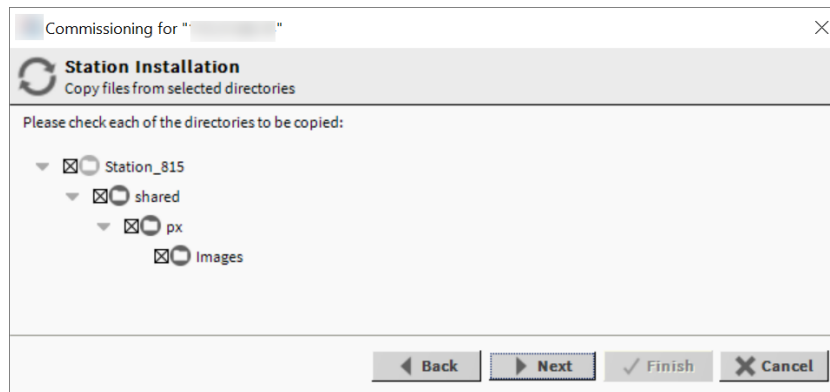
  - If you choose this, click folder controls to expand and contract as needed.

  - Selected folders are shown as X and unselected folders show an empty folder check box.

- `Copy every file in the station directory and its subdirectories`

  The default, and most typically used.

  NOTE: Copying identical alarm/history data to multiple controllers is not recommended. For this reason, Alarm and History data are not included (by default) in the station copying process.

- `Copy only the config.bog station database file`

  Copies only the station configuration (components), and not any supporting folders/files like px files, html files, and so forth.

Step 5   Select one of the options and click **Next**.

The **Lexicon Installation** step opens.
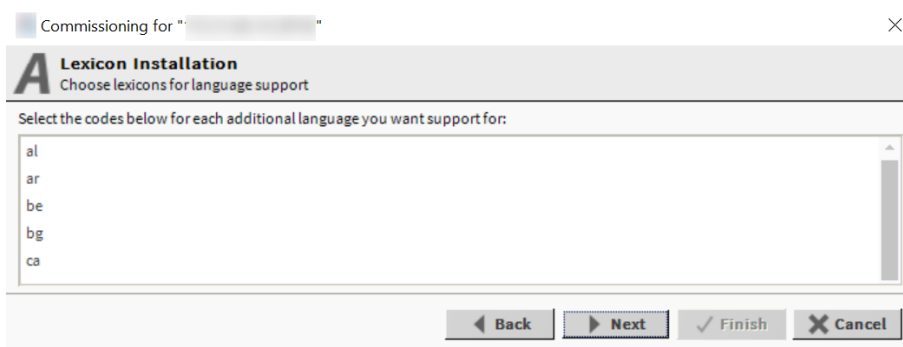
The table displays a list of language codes.

Step 6   To use a language other than English, select the language code from the list and click **Next**.

A popup **Rebuilding software list** window briefly displays the dependencies of the controller compared with the available software modules in your PC's software database. Then it opens the **Software Installation** step.

This table lists the available modules including their status, for example `Out of Date`. During commissioning, you add to the software modules that are preselected for installation. Sometimes you may not make any changes, as the wizard preselects all necessary core modules, plus any additional modules needed by the station you previously specified in the Install Station step.

A red text descriptor qualifies each core module:

* Install required platform module

* Install required for runtime profile

* Install module required by station

    By default, these modules are at the top of the list. You cannot deselect them.

You can select additional modules to install by clicking selection boxes. The description for each is in blue text, and displays as either:

* Not Installed (if not selected)

* Install (if selected)

You can select additional modules, including a few not directly related to the contents of the station selected for installation. Examples include lexicon module(s) and some modules related to **Platform Services**. Or, you may know that the controller will need one or more modules in the future (say for a driver), and you wish to install them now.

In general, do not select modules if you are not sure they are needed. You can manage software modules later, using the **Software Manager**. Also, if you install a station later, the **Station Copier** will automatically prompt for confirmation to install any additional modules deemed necessary.

For cases described below, install the following additional module(s) to enable options.

* Select either (or both) theme-related modules: `themeLucid-ux`, `themeZebra-ux`, depending on how station users are assigned to Web Profiles (for example, Default Hx Profile, Hx Theme= Lucid).

* If a station requires the `Hardware Scan Service` in its **PlatformServices**, select the appropriate `platHwScanType` modules. For example, select `platHwScanTitan-rt` and `-wb` modules.

- Standard lexicon modules are listed using a module name with this convention:

  `niagaraLexiconLc-rt`

  where `Lc` is a two-character language code, such as `Fr` for French or `Es` for Spanish. It is also possible to make custom lexicon modules using Workbench lexicon tools (which can have different names).

  To reset the selection of modules to the original collection, click the **Reset** button.

Step 7   Do one of the following:

- To sort the list alphabetically, click the Module header in the table. To return to the default sort order, click the table's (blank) description header.

- To review the list of modules, click each module's check box to be updated (☒) and click **Next**.

- Click **Upgrade All Out of Date** to upgrade all the modules at a time and click **Next**.

- To reset the selection of modules to the original collection, click the **Reset** button and click **Next**.

- Use the scroll bar to review the list.


NOTE: The **Software Manager** view and **Commissioning Wizard**'s **Software Installation** step include signature status icons in the Installed Version and Available Version columns indicating the signature status of the installed and available modules. Attempting to install modules with signature warnings (indicated by a yellow 🛡 icon) opens a signature warning window, and attempting to install modules with signature errors (indicated by a red ❌ icon) causes the installation to fail. For details refer to, the *Niagara Third Party Module Signing* guide.

When you click **Upgrade All Out of Date**, the status of the selected modules changes to identify the software version to be installed.
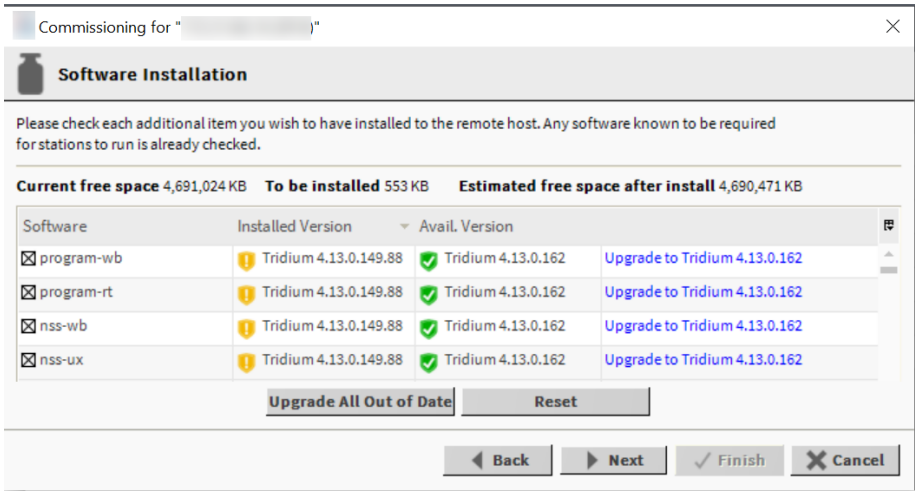
Next, the **Distribution File Installation** step opens.
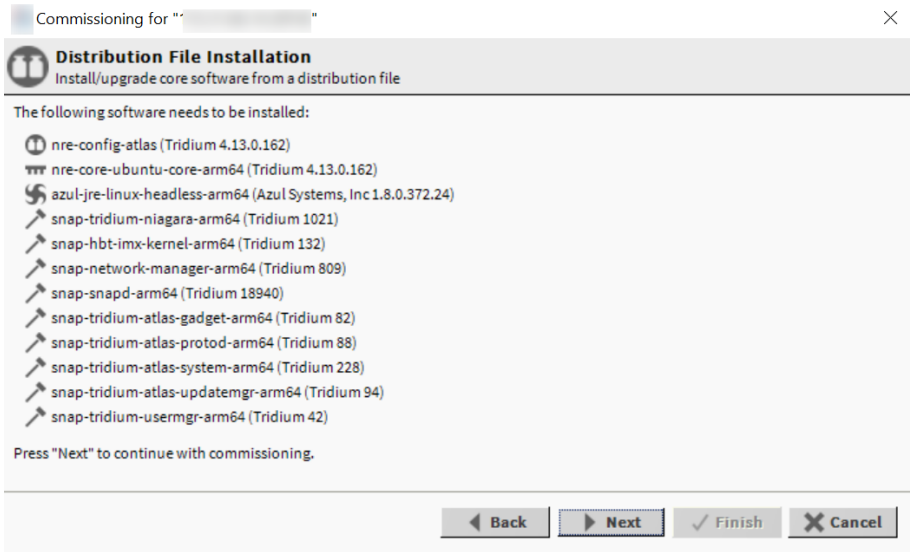
Step 8   Review the file installation list and click **Next** to continue.

The **TCP/IP Configuration** step opens.

Host Name defaults to the name of the remote controller.

Configuring TCP/IP settings

These steps allow changes in the TCP/IP settings for the platform to configure the IP address and TCP port parameters for the remote controller.

Prerequisites: You are stepping through the Commissioning Wizard.

Step 1   To change the Host Name, enter the new name.

If a **Host Name** is entered, typically the name is unique for the domain. In some installations, changing **Host Name** may result in unintended impacts on the network, depending on how the DHCP or DNS servers are configured. If in doubt, leave **Host Name** at its default setting.

Step 2   To change the contents of the **Hosts File**, click the control ⩬.

The file opens.

The format of this file is a standard TCP/IP hosts file, where each line associates a particular IP address with a known **Hosts File**. Each entry should be on an individual line. The IP address should be placed in the first column, followed by the corresponding **Host Name**. The IP address and the **Host Name** should be separated by at least one space. The **Undo Changes** button resets all settings (all Interfaces) back to the original pre-step values.

Step 3   To add a new line, click at the end of the last line, press **Enter** and type the required data on the new line.

Step 4   To enable use of IPv6, click the check box and configure any applicable IPv4 and IPv6 settings.

Use IPv6 limits the station to receive only IPv6 requests.

Step 5   Review the **Interface 1** settings and do one of the following:

If you are enabling more than one LAN port (applicable to LAN1, LAN2, and WiFi) then the IP address for each must be configured 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.

- Click **IPv4 Settings** tab, which includes the temporary factory-shipped IP address. Assign the JACE a unique IPv4 address for the network you are installing it on. No other device on this network should use this same IP address. Include the appropriate subnet mask used by the network.

- If the network supports DHCP, you can enable it (click **DHCP Enabled**). In this case, the IP address and subnet mask properties become read only. in general (for stability, static IP addressing is recommended over DHCP. If DHCP is preferred, an IP Address Reservation should be entered for the controller in the DHCP Server. The controller IP address should not change.

  CAUTION: Do not enable DHCP unless you are certain that the network has DHCP servers! Otherwise, the controller may become unreachable over the network.

  If your JACE has a wireless option that you plan to use for enterprise network connections, do not enable DHCP here. Instead, you need to configure the WiFi adapter for JACE DHCP as described in the appropriate controller WiFi Guide, for example JACE-8000 WiFi Guide.

Step 6   Review the **Interface 2** details.

JACE-8000 and JACE-9000 controllers have two Ethernet ports, where **Interface 2** is available for configuring the secondary (LAN2) Ethernet port. By default, this port is disabled, that is without a default address. The intended usage for this port, as for the secondary LAN port, as follows:

- To isolate a driver's Ethernet traffic from the primary (LAN1) interface, or

- To create a private network by daisy chaining multiple IP devices off of the controller's secondary LAN port.This scenario requires that you configure the LAN2 port as a DHCP server in the **DHCPDv4 Settings** tab.

- In some cases, LAN2 may be set up with a standard, fixed, IP address that is used only by a company's service technician, when on site. This allows access to the controller without disconnecting it from the customer's network, or without connecting the technician's service PC to the customer's network (which might go against local IT security policies).

  If enabling LAN2, you must specify another (network) static IP address and the appropriate subnet mask, that is a different subnet mask for each enabled LAN port IP address.

- The controller does not provide IP routing or a bridging operation between different Interfaces (LAN ports or WiFi).

Step 7   To enable the secondary Ethernet port **Interface 2**, expand **Interface 2** and select the `Adapter Enabled` check box.

Step 8   To set up the secondary Ethernet port (**Interface 2**) as a DHCP client, select the **Enabled** check box on the **IPv4Settings** tab.

Make sure that the **DHCPDv4** is not enabled on the **DHCPDv4 Settings** tab.

Step 9   To set up the secondary Ethernet port (**Interface 2**) as a DHCP server, make sure that the **DHCP** check box is not selected on the **IPv4 Settings** tab, configure the port with a static IP address, and configure the properties in **DHCPDv4 Settings**.

For example:

- `Subnet`: 192.168.111.0

- `Netmask`: 255.255.255.0

- `Client range low`: 192.168.111.15

- `Max. number of clients`: 10

Based on the example above, client IP pool is 192.168.111.15 to 192.168.111.24

- `Default Lease Time` (in hours, minutes, and seconds) configures the a DHCPIP address lease. Before it expires, the lease must be renewed.

- `Max Lease Time` (in hours, minutes, and seconds), configures a DHCPIP address lease.

- `Subnet` defines the subnet of IP addresses assigned by the DHCP server. Configure this to assign addresses on a different subnet than that used in other LAN or Access Point configurations, otherwise the ports will not function correctly.

- `Netmask` defines the IP addresses assigned by the DHCP Server.

- `Client Range Low` defines the lowest IP address for the range. The order of assigning IPs from the Access Point DHCP is indeterminate.

The adapter IP should be in the same subnet, but not in the range of addresses defined here.

- `Max Number of Clients` defines the maximum number of clients that can attach at a given time.

Step 10   Under **IPv4 Settings** tab, enter the IPv4 address and subnet mask.

For example,

- `IPv4 Address`: 192.168.111.1

- **IPv4 subnet mask**: 255.255.255.0

  Make sure that the secondary Ethernet port's (**Interface 2**) IP address is outside the DHCP server's client IP pool.

Step 11 To disable a DHCP server running on the secondary Ethernet port (**Interface 2**): Under **DHCPDv4 Settings** Tab, uncheck the **DHCPDv4** check box. For the network settings to take effect, save and reboot the controller.

These network settings will take effect when you finish the Commissioning Wizard and reboot the controller.

Step 12 To continue, click **Next**.

The **System Passphrase** step opens.

Configuring the system passphrase

All Niagara platforms have a system passphrase used to protect and encrypt the system information in the platform's file systems. Using the **Platform Administration** view or runing through the Commissioning Wizard, you can set up this passphrase.

Prerequisites: You are stepping through the Commissioning Wizard. You know the controller's current passphrase.

Step 1 To set up a new passphrase, enter the default **Current Passphrase** for the controller.

Step 2 Enter the **New Passphrase** and confirm it.

Create a strong passphrase with a minimum of 10 characters including: at least one uppercase character, at least one lowercase character, and at least one digit. Entry characters display only as asterisks (*). An error popup window reminds you if you attempt to enter a passphrase that does not meet the minimum rules:

- Use both upper and lower case.
- Include numeric digits (a minimum of one).
- Include special characters.
- Don't use dictionary words.
- Don't use company name.
- Don't make the passphrase the same as the user name.
- Don't use common numbers like telephone, address, birthday, and so on.

Step 3 Make a note of the new passphrase and guard it carefully!

CAUTION: If you lose the system passphrase, you will lose access to the controller's encrypted data.

You can change the system passphrase using the **Platform Administration** tool.

Step 4   Click **Next** to continue.

The **Create a new platform user account** window opens.

Setting up platform users

The Commissioning Wizard prevents commissioning a controller that retains the factory-default platform user account. In this Commissioning Wizard step, you specify platform login credentials (user name and password) to replace the factory-default platform user in this controller.

Prerequisites: You are stepping through the Commissioning Wizard.

Step 1   Enter the desired `User Name` with which to log in to the platform.

This name must be different from the default name. It can have a maximum of 14 alphanumeric characters (`a - z, A - Z, 0 - 9`), where the first character must be alphabetic and following characters either alphanumeric or an underscore (_).

Step 2   Enter and confirm the `Password`.

Create a strong password with a minimum of 10 characters including: at least one uppercase character, at least one lowercase character, and at least one digit. Entry characters display only as asterisks (*). An error popup window reminds you if you attempt to enter a passphrase that does not meet the minimum rules:

- Use both upper and lower case.

- Include numeric digits (a minimum of one).

- Include special characters.

- Don't use dictionary words.

- Don't use company name.

- Don't make the password same as the user name.

- Don't use common numbers like telephone, address, birthday, and so on.

User name and password entries are case sensitive. If you are not changing the controller's IP address during commissioning, the credentials for your replacement platform user are remembered in the current session. This can simplify platform reconnection to the controller after it reboots from commissioning. This is useful in a migration scenario. However, if you are changing the IP address during commissioning, you need to remember/re-enter the new credentials for a platform user in order to reconnect. Always make careful note of any changed platform credentials, and guard them closely—as they provide the highest security level access to any Niagara platform.

Step 3   In the (optional) `Comment` property, enter an alphanumeric descriptor for this platform admin user and click **Next**.

This alphanumeric descriptor displays in the **Users** table and helps differentiate users if you have more than one platform user. You cannot edit this property after adding a user, unlike with a user's password.

If, at the beginning of commissioning, you selected to `Configure additional platform daemon users`, the **Platform user account information** window opens.
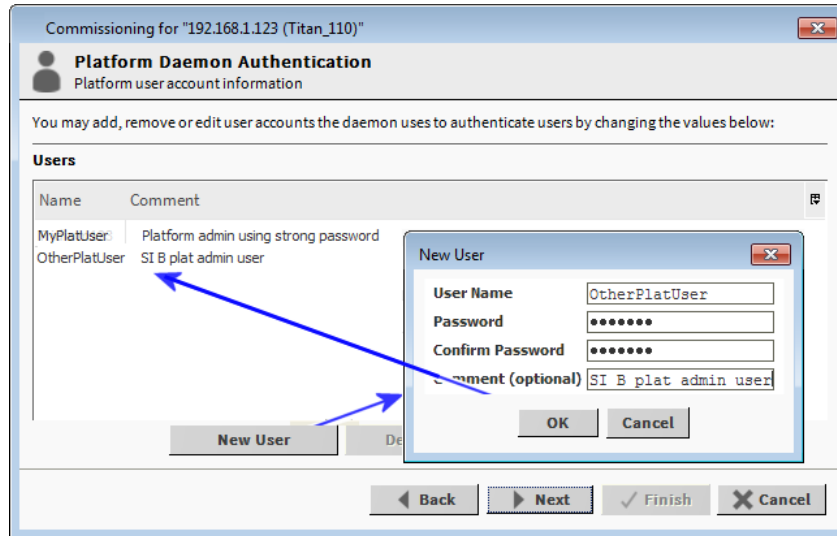
The **Users** table in this window shows the replacement user you just created.

Step 4   To create another user, click **New User**, fill in this user's credentials, click **OK**.

You can also use this step to delete users and change user passwords. You can access this same configuration via the **User Accounts** button in the **Platform Administration** view, which is available any time after commissioning.

Step 5   To add another user, repeat these steps or else click the **Next** button for the final commissioning step.

Step 6   Make a note of all platform user credentials and guard them carefully.

Consider the platform daemon as the highest-level of access to the controller.

If you lose or forget these credentials, you may be unable to complete commissioning and start up this controller. In this case, you can restore the factory default platform user, provided you can serially connect to the controller (make a serial shell connection), then press and hold the **SHUT DOWN** button as you power up the device.

Step 7   To continue, press **Next**.

The **Completing Commissioning** window opens.
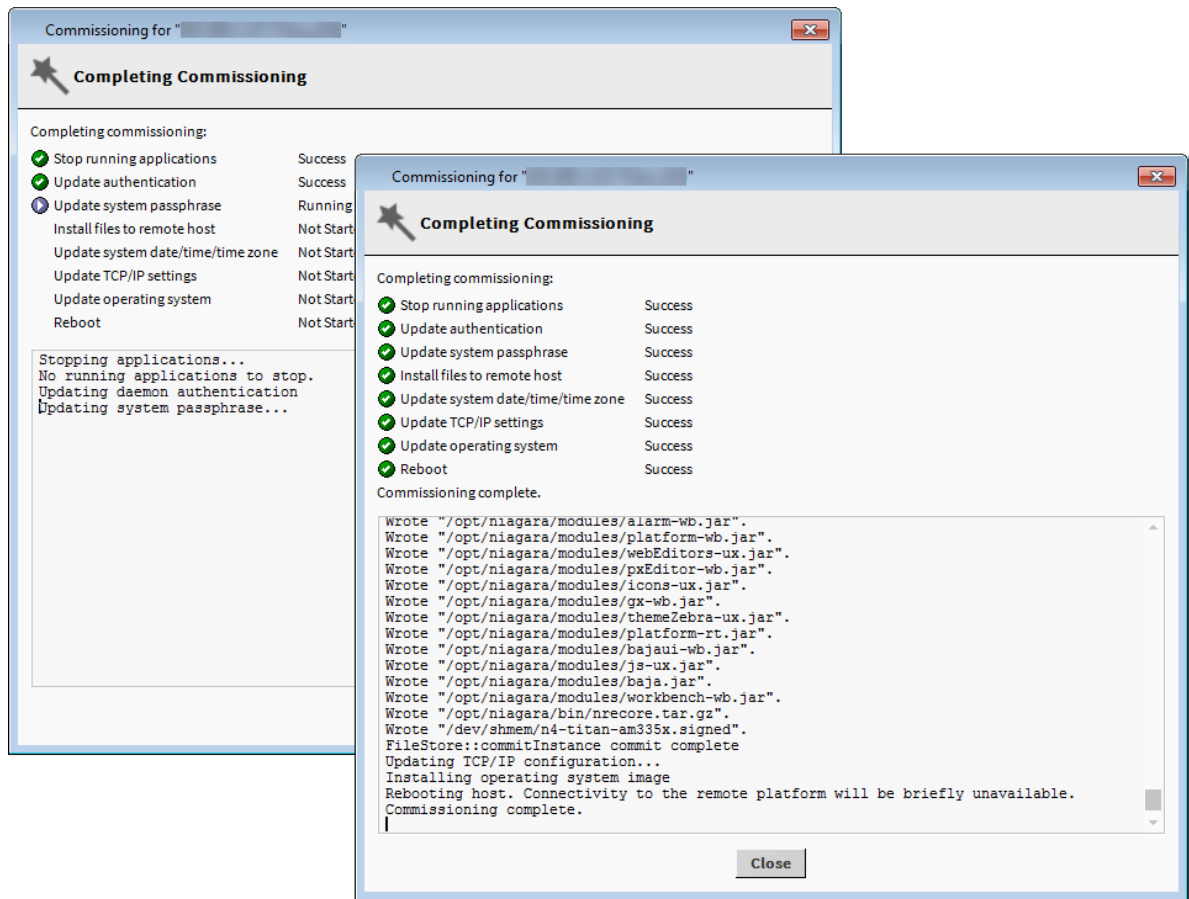
Reviewing and finishing the Commissioning Wizard

The Commissioning Wizard displays a summary of all the actions to be performed by the wizard.

**Prerequisites:** You are stepping through the Commissioning Wizard.

Step 1   Read through the summary of changes, using the scroll bar to see the steps near the end.

Step 2   If any change is needed, click the **Back** button until the step window to change opens, make the change and click the **Next** button until this review window opens again.

Step 3   If no change is needed, click **Finish**.

The Commissioning Wizard commissions the controller. While the wizard works it posts progress updates in a **Completing Commissioning** widow. When completed, the wizard reboots the controller, and makes a **Close** button available.

Do not remove power from the controller during this reboot, which may take up to seven or more minutes to complete. Removing power could make the unit unrecoverable. If desired (and convenient), you can use a serial shell connection to the controller to monitor progress as files are installed and the unit is prepared.

Note that firmware upgrades occur before the platform daemon starts in the controller. Therefore, it is safe to interrupt power any time after you can re-open a platform connection to the controller.

Step 4   To exit the wizard, click the **Close** button.

When the controller reboots, your platform connection to it closes.
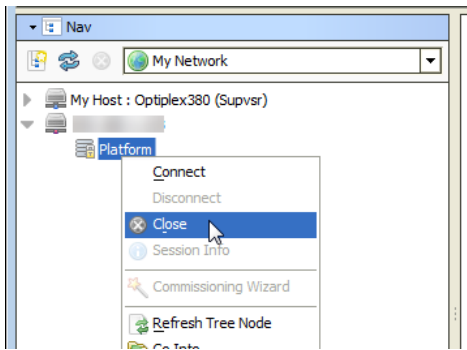
Notice that in the Nav tree, the platform instance for that JACE is now dimmed.

Step 5   Assuming that you changed the JACE's IP address during commissioning, right-click and close that platform instance, as this would make that connection instance invalid.

Step 6   Do one of the following:

- If you did not change its IP address, after several minutes you should be able to double-click the platform instance again to reconnect.

- Open a platform connection using the controller's new (changed) IP address.
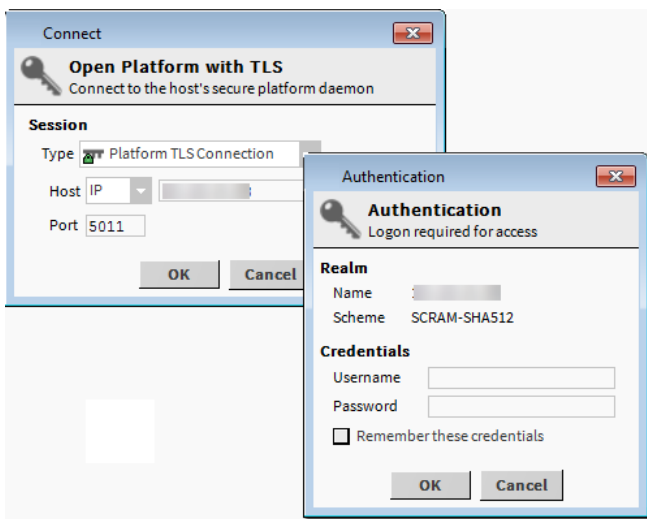
Going forward, you must access the controller by its new (assigned) IP address. Workbench keeps a history of TCP/IP changes made.

Use the credentials for the new platform user you created to replace the factory-default platform user, or if you created additional platform users, log in with the credentials you created for one of them.

Step 7   If you changed your PC's IP address to commission the controller, be sure to reconfigure your PC's TCP/IP settings back to appropriate settings to communicate with it. Otherwise, you will be unable to connect to the PC to commission another controller.

Chapter 3   Platform services and administration

Topics covered in this chapter

♦ Changing the date, time and time zone using PlatformServices
♦ Enabling and disabling SRAM support in the DataRecoveryService
♦ Performing platform administration

A few platform configuration features are not directly accessible in the Workbench platform connection via the **Commissioning Wizard**. Instead, to access these features, you must install a station on the controller (any station). The **Commissioning Wizard** also performs most, but sometimes not all, needed configuration for a new controller platform. There are several items you should review (and optionally change) in a follow-up platform connection to each controller, using the **Platform Administration** view.

Figure 1   Example of a controller station's Platform Services
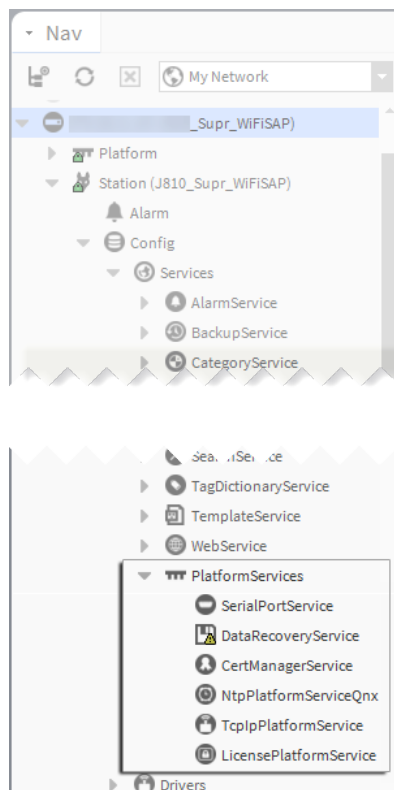
PlatformServices are different from all other components in a station in the following ways:

- The **PlatformServices** node acts as the station interface to specifics about the host platform (whether controller or a PC).

- Niagara builds these services dynamically at station runtime—you do not see **PlatformServices** in an offline station.

- Any changes you make to **PlatformServices** or its child services are not stored in the station database. Instead, changes are stored in other files on the host platform, such as its platform.bog file.

    NOTE: Do not attempt to edit the platform.bog directly; always use **PlatformServices** views.

These services support installations where all configuration must be possible using only a browser connection (and not Workbench connected to the controller platform daemon). Included services are:

- **TcpIpService** provides station (Fox) access to windows used to configure TCP/IP settings.
- **LicenseService** for managing platform licenses.
- **CertManagerService** for managing PKI certificate stores and/or allowed host exceptions, used in certificate-based (TLS) connections between the station/platform and other hosts. For details, see the *Niagara Station Security Guide*.
- **DataRecoveryService** for the operation and monitoring of ongoing SRAM backups for most (SRAM-equipped) JACE controllers. It includes a `Service Enabled` configuration property, which you can disable, if needed. This is viable only if a backup battery is installed, or the unit is powered by an external UPS.

The **Platform Administration** view is one of several views for any platform, listed under the **Platform** node in the Nav tree and in the platform's **Nav Container View**. This view provides a text summary of the JACE's current software configuration, including its model number, OS level, JVM version, installed modules, lexicons, licenses, certificates, and so on.

Figure 2   Platform Administration is one of several platform views
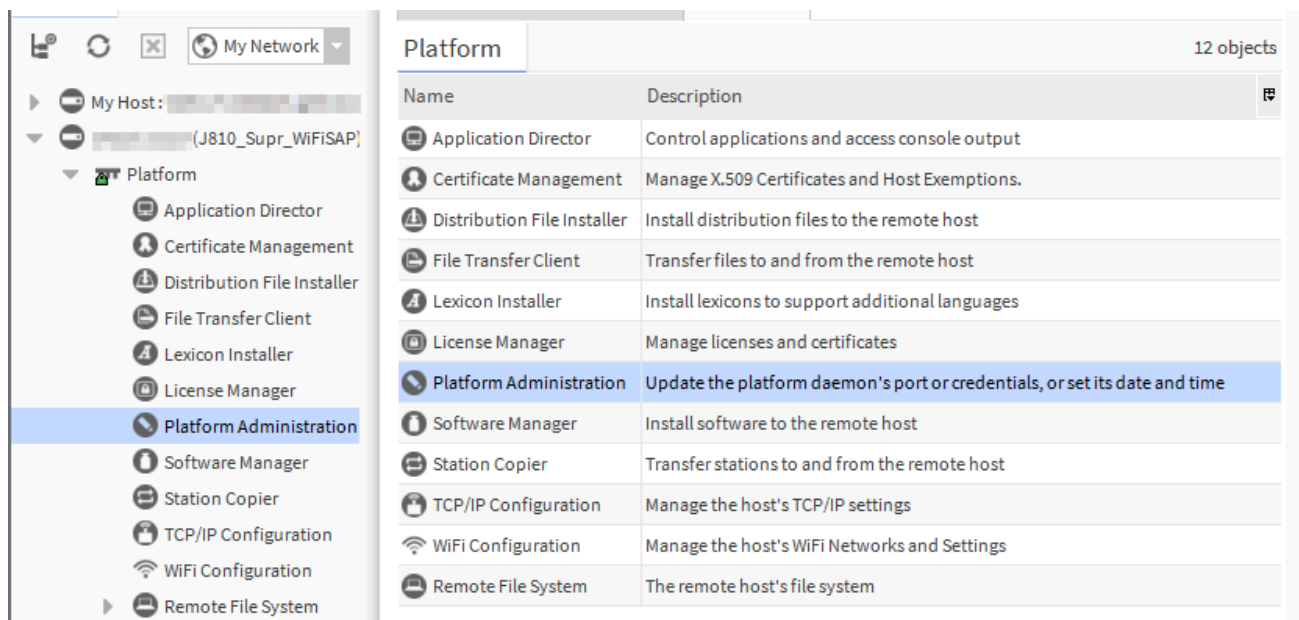
Platform Administration

View Details	
User Accounts	
System Passphrase	
Change HTTP Port	
Change TLS Settings	
Change Date/Time	
Advanced Options	
Change Output Settings	
View Daemon Output	
View System Log	
Configure Runtime Profiles	
Configure NRE Memory	
Backup	
Commissioning	
Reboot	

Baja Version	Tridium 4.1.25.0
Daemon Version	4.1.25.0
System Home	/opt/niagara
User Home	/home/niagara
Host	_____Supr_WiFiSAP)
Daemon HTTP Port	3011
Daemon HTTPS Port	5011
Host ID	
Model	TITAN
Product	JACE-8000
Local Date	23-Oct-15
Local Time	13:45 Eastern Daylight Time
Local Time Zone	America/New_York (-5/-4)
Operating System	qnx-jace-n4-titan-am335x (4.1.25.0)
Niagara Runtime	nre-core-qnx-armle-v7 (4.1.25.0)
Architecture	armle-v7
Enabled Runtime Profiles	rt,ux,wb
Java Virtual Machine	oracle-jre-compact3-qnx-arm (Oracle Corporation 1.8.0.33.1)
Niagara Stations Enabled	enabled
Number of CPUs	1
Current CPU Usage	5%
Overall CPU Usage	2%

Filesystem	Total	Free	Files	Max Files
/	3,492,848 KB	3,295,570 KB	331	109152
/mnt/aram0	393,215 KB	393,052 KB	0	0
/mnt/ram0	8,192 KB	8,126 KB	0	0

Physical RAM	Total	Free
	1,048,576 KB	91,436 KB

Other Parts	
	n4-titan-am335x (4.0.1)

You may wish to review and configure the parent container's **PlatformServices** and **PlatformAdministration** properties using Workbench.

The *Niagara Platform Guide* documents the **PlatformServices** and **PlatformAdministration** properties.

Changing the date, time and time zone using PlatformServices

You may change the date, time and time zone using **Platform→PlatformAdministration→Change Date/Time**. This procedure, however, uses the station's **PlatformServices** instead. Access to **PlatformServices** properties is useful if the installation requires access using a browser only.

Prerequisites: You are running Workbench and are connected to the controller station.

Step 1   In the Nav tree, double-click **Config→Services→PlatformServices**.

The **Platform Service Container Plugin** opens.

Some properties in this view are read-only. Other configuration properties can be edited. A group of three config properties adjust the time, date, and time zone settings for the host controller.

Step 2   Configure `System Time`, `Date`, `Time Zone` and click **Save**.

You should leave the remaining properties at their default values, unless otherwise directed by systems engineering.

The framework writes any configuration changes to the host controller platform.

The *Niagara Platform Guide* documents all **PlatformServices** properties.

Enabling and disabling SRAM support in the DataRecoveryService

SRAM support is provided by the **DataRecoveryService**, a platform service that applies to SRAM-equipped JACE controllers.

Prerequisites: You are using Workbench and are connected to a remote station.

Step 1   In the Nav tree, expand the station's **Services→PlatformServices**, and double-click **DataRecoveryService**.

The **Data Recovery Service Editor** window opens.

By default, the `Service Enabled` property is `true`. This is appropriate since the controller has no backup battery installed.

Step 2   If a battery-less controller is powered from a battery-backed UPS, you could also choose to set `Service Enabled` to `false`.

If you set `Service Enable` to `false`, the **DataRecoveryService** no longer records runtime database changes to SRAM but depends entirely on its backup battery to preserve station data upon a power loss!

Step 3   To write the configuration to the host platform, click **Save**.

You are prompted to reboot now to apply the changes.

Step 4   To reboot with the change in the **DataRecoveryService** (disabled or enabled) made effective, click **Yes**.

Performing platform administration

The **Commissioning Wizard** performs most platform configuration tasks. After running the wizard, you may review and change configuration options using the **Platform Administration** view.

Prerequisites:

The JACE controller is already commissioned using the Commissioning Wizard. You have admin rights to configure the platform.
You have admin rights to configure the platform.

Step 1   Using Workbench, open a platform connection to the JACE controller. Use the platform credentials you specified when creating a platform user while commissioning the controller.

Step 2   Right-click **Platform**, double-click **Platform Administration** and enter your platform credentials.

The **Platform Administration** view opens.

Step 3   Click one of the buttons.

Included in this view are commands and related windows in which you can:

- Set the date and time in the controller.

- Change the HTTP port used by the controller for the platform daemon (platform server). The default port is 3011.

- Change TLS settings used by the controller for secure platformssl access, including configured state, platformssl port (HTTPS Port), PKI certificate, and TLS protocol. The default port is 5011. Refer to the *Niagara Station Security Guide* for complete details.

- Enable or disable SFTP (Secure File Transfer Protocol) and SSH (Secure Shell) access to the JACE controller. By default, such access is disabled, where both protocols use TCP port 22.

  CAUTION: Although SFTP and SSH are more secure than FTP and Telnet access, enabling still poses security risks. We strongly recommend you keep this access disabled, unless otherwise directed by Systems Engineering. Upon completion of any use, such access should be disabled once again.

- View daemon output and change logging levels.

- Enable debug access for temporary browser access to platform daemon diagnostic tools

- Perform other platform tasks initially performed with the Commissioning Wizard, such modifying platform admin users (User Accounts), configuring runtime profiles, and so on.

The *Niagara Platform Guide* documents each object.

Step 4   What to do next depends on the object you selected.

Chapter 4   System shell

Topics covered in this chapter

♦ About the JACE-9000 system shell menu
♦ Connecting to the controller system shell
♦ Updating network settings using JACE-9000 system shell
♦ Updating system time using the system shell (JACE-9000)

All controllers have a system shell that provides low-level access to a few basic platform settings. Using a special power-up mode and a serial connection via an appropriate type USB cable connected to the controller, you can access this system shell from your PC. System shell is also available via SSH (Secure Shell) provided that SSH is enabled in the controller.

Typical usage is for initial controller setup, troubleshooting, or to create or restore a backup. Also, in the case of IP address mis-configuration, you can use the serial system shell to regain access to the unit.

Depending on your preference, you may wish to use the serial shell to set the controller IP address as an alternative to reconfiguring your PC's IP address in Windows (to initially connect to a new controller). If done as the first step, afterwards you could connect normally (Ethernet/IP) and perform all the other Niagara software installation and platform configuration using Workbench and the **Commissioning Wizard**. This method would save you from having to re-configure your PC's IP address settings in Windows: first to connect to the controller as shipped from the factory, and then back again to its original settings.

The following topics provide more details.

About the JACE-9000 system shell menu

The system shell of the controller provides simple, menu-driven, text-prompt access to basic Niagara platform settings, including IP network settings, platform credentials, system time, and enabling/disabling SFTP/SSH and Telnet, as well as creating or restoring system backups. Also, you can use it to perform a TCP/IP ping from the controller to another host.

Changes issued in the system shell become immediately effective, except for IP address settings (Update Network Settings). You must reboot the controller for any changed network settings to become effective.

If SSH is enabled in the controller, you can also access the controller's system shell using a remote terminal session using SSH. Platform login is still required (just as with the controller powered up in serial shell mode).

CAUTION: Be careful when changing items from the system shell, in particular platform account (login credentials, system passphrase) and network settings. If you change platform login credentials and then lose or forget them, you may need to restore the factory default settings and possibly lose any non-backed up data.

Following, is an example of the system shell menu when connected to a JACE-9000.

Figure 3   System shell menu (serial shell or Telnet access)

```
-------------------------------------------------
1    Update System Time
2    Update Network Settings
3    Ping Host
4    System Diagnostic Options
5    Change Current User Password
6    Change System Passphrase
7    Create SD Backup
8    Restore SD Backup
9    Reboot
L    Logout
```

```
Enter Choice :
```
To select a menu option, type the associated number (`1` to `9`) or `L` for logout, then press `Enter`.

For example,

- type `2` (Update Network Settings) to recover IP access, or to set the IP settings of a new controller.
- type `6` (Change System Passphrase) to change the system passphrase of the unit. You might do this if swapping in a microSD card from a previously configured unit, in order to change the passphrase of the unit to match the passphrase that is already stored on the card.

Connecting to the controller system shell

The following procedure provides steps to use the system shell. Examples provided use the PuTTY terminal emulation program.

Prerequisites: You have physical access to the controller and you have a USB cable that connects to your PC and to a:

- MicroUSB port on a JACE-8000
- USB-C port on a JACE-9000

Step 1   Connect the USB cable between the controller's DEBUG port and the USB port you are using on your PC.

Step 2   On your PC, start your terminal emulation software.

For example to start PuTTY from the Windows Start menu, this is typically **Programs PuTTY**.

Step 3   In the **PuTTY Configuration** tree, expand **Connection** and click **Serial**.

Step 4   Set the serial line to connect to your PC's (USB) COM port, for example, **COM3**.

You can examine Ports in Windows Device Manager to determine which serial port is in use on the PC.

Step 5   Set the `Configure the serial line` properties as follows:

- **`Speed (baud)`:** `115200`
- **`Data bits`:** `8`
- **`Stop bits`:** `1`
- **`Parity`:** None
- **`Flow control`:** None

Step 6   In the **PuTTY Configuration** tree, click **Session** and then click the `Connection type` as `Serial`.

(Optional) You can

When you start PuTTY again to serially connect to the JACE, select this name and click **Load**.

Step 7   (Optional) To save this configuration and reuse (load) it in a future PuTTY to controller serial session, type in a connection name in the `Saved Sessions` property (for example, "SerialController-Connect", and click **Save**.

Step 8   At the bottom of the **PuTTY Configuration** window, click **Open**.

A terminal window opens.

NOTE: If you do not see a login prompt, press the **Enter** key and it should display a login prompt in the window.

Step 9   At the login prompt, enter a platform user name and password, and, if prompted, enter the platform's system passphrase.

Step 10   When finished making platform changes from the system shell, do one of the following:

- If no changes, or reboot is not necessary, type L to Logout.
- If changes require rebooting, select the Reboot option, type y at the Are you sure you want to reboot [y/n] prompt, and press **Enter**.

    The terminal (PuTTY) window displays shutdown-related text.

Step 11   Click the **Close** control (upper right corner) in the terminal session (PuTTY) window and click **OK** in the **PuTTY Exit Confirmation** popup window.

Step 12   Unplug the USB connector from the JACE's DEBUG port.

Updating network settings using JACE-9000 system shell

Using system shell to update network settings prompts you for each setting sequentially, starting with hostname.

Prerequisites: You have connected to the controller using the system shell.

Step 1   To access most of the same IP networking options available in the **Commissioning Wizard** step that configures TCP/IP settings, select system shell menu option 2.

    The Network Configuration Utility displays. Following is an example of the flow with some fictional addresses:

```
Enter Choice : 2

Network Configuration Utility

Enter new value, '.' to clear the field or '' to keep existing value
Hostname < TechDocsJ9 > :
Save these settings  [Y/n]? y
Committing to disk ...

NET1 Ethernet interface en0
  IPv4 address (clear to use DHCP) < nnn.nn.nn.nn > :
  IPv4 subnet mask < 255.255.252.0 > :
  IPv4 Domain :
  Primary IPv4 DNS Server :
  Secondary IPv4 DNS Server :
  IPv4 Route < nnn.nn.nn.n > :
  Enable IPv6 addressing on this adapter  [Y/n]?
  IPv6 address in CIDR notation address/prefix-length (clear to use DHCP) :
  IPv6 Domain :
  Primary IPv6 DNS Server :
  Secondary IPv6 DNS Server :
  IPv6 Route :

Configure Secondary Ethernet interface  [Y/n]? n

 Confirm new configuration
network:
    version: 2
    renderer: NetworkManager
    ethernets:
        en0:
            match:
                driver: imx-dwmac
            set-name: en0
            dhcp4: false
            dhcp6: true
            link-local:
```

```
          - ipv6
       addresses:
          - 172.31.66.14/22
       routes:
          - to: default
            via: 172.31.64.1
  en1:
       match:
            driver: fec
       set-name: en1
       dhcp4: false
       dhcp6: false
       link-local: []
       activation-mode: manual
```

`Save these settings  [Y/n]?`

Step 2   As each option displays, configure it and conclude by pressing **Y** to save the settings.

After you save the network settings, they do not become active until you perform a reboot of the controller.

Step 3   On the main system shell menu, selecting **Reboot**, option `6`.

System shell reboots the controller.

Updating system time using the system shell (JACE-9000)

If the commissioning process has not been completed yet, it is often important to set the current date and time.

Prerequisites: You have connected to the controller using the system shell.

Step 1   To access date and time, select system shell menu option `1 Update System Time`.

The screen displays the following controller current date/time and clock synchronization information:

- Local time
- Universal time (UTC)
- RTC (real time clock) time
- Time zone
- System clock synchronization status
- NTP service status
- RTC in local TZ (time zone) status (yes/no)

A prompt dispays, asking for new UTC date and time in the following format:

- `YYYY-MM-DD` for year, month, and day
- `HH:MM:SS` for hour, minute, and second

Step 2   Enter date and time in the required format and press **Enter** to save the changes.

If the the time information is successfully changed, a confirmation message appears on the screen.

Step 3   Press Enter to return to the shell main menu.

Chapter 5   Troubleshooting

Topics covered in this chapter

♦ Shutting down the controller
♦ Resolving a passphrase mismatch
♦ Reviewing a controller's TCP/IP changes
♦ Reviewing a PC's TCP/IP changes
♦ Restoring factory defaults (JACE-9000)

During commissioning, it is possible to run into problems. For instance, you may type an IP address incorrectly when entering it, and as a result be unable to regain access. This chapter provides information that can help with troubleshooting or general controller operations.

Shutting down the controller

This procedure safely prepares the controller before you remove power.

Prerequisites: The controller is powered on. Any running devices (HVAC, boiler, meter, etc) have been set in a standby mode.

Step 1   Press and hold the **SHUT DOWN** button until the **SHUT DOWN** LED flashes (about 5 seconds).

NOTE: Releasing the button after the flashing LED starts confirms that the button press is intentional.
After about 10 seconds, the **BEAT** LED is no longer lit, indicating that the shut down preparation process is complete.

Step 2   Remove power from the controller.

Shut down is complete.

Resolving a passphrase mismatch

If a controller fails, you can remove its SD or microSD card and insert it into a replacement unit and keep your business running. However, the removable card contains the system passphrase for the original unit, which does not match the passphrase for a replacement unit. This results in a boot sequence failing due to a pass-phrase mismatch indicated by a Stat LED flashing with a 50% duty cycle and a 1 second period.

Prerequisites: A controller has failed. You removed its memory card and inserted it into a replacement unit, but the replacement unit will not boot due to a passphrase missmatch. You are working in Workbench running on a PC that is on the same network as the controller. You know the passphrase for the original controller.

If you are monitoring the debug port, this notification banner opens in the serial shell.

Figure 4   System passphrase mismatch warning in the serial shell

NOTE: The following shows a JACE-8000 - shell connection. JACE-9000 message is similar.

```
*******************************************************************************¶
WARNING:¶
Unable·to·decrypt·critical·system·info·due·to·system·passphrase·mismatch¶
Normal·boot·process·cannot·proceed.·Niagara·daemon,·SSH·and¶
networking·are·disabled·while·in·this·state.¶
¶
This·can·be·caused·by·moving·SD·card·from·one·unit·to·another.¶
Login·and·update·the·system·passphrase·to·match·original·unit,·then¶
reboot¶
*******************************************************************************¤
```

This warning prompts you to log in using platform credentials and update the system passphrase via the serial connection.

Step 1   Make a serial connection to the unit's DEBUG port.

Step 2   Log in to the controller via the serial connection.

The **System Decrypt Failure Menu** opens with the following options:

1 `Update system passphrase`

2 `Remove all encrypted data`

3 `Reboot`

4 `Logout`

Step 3   Choose `Update system passphrase.`

Step 4   Enter the system passphrase for the original controller.

Pre-configuring (via a serial connection) the replacement controller with a system passphrase that matches the one stored on the removable memory card (which you swapped out from the original unit) facilitates commissioning the replacement unit. In this situation, the commissioning process does not prompt for a passphrase since it detects a passphrase match.

Reviewing a controller's TCP/IP changes

The Commissioning Wizard and platform's TCP/IP Configuration object configure controller TCP/IP settings. Workbench records TCP/IP before and after the change values in an `ipchanges.bog` file. If necessary, you can review these changes.

Prerequisites: You are working in Workbench with a connection to the remote controller.
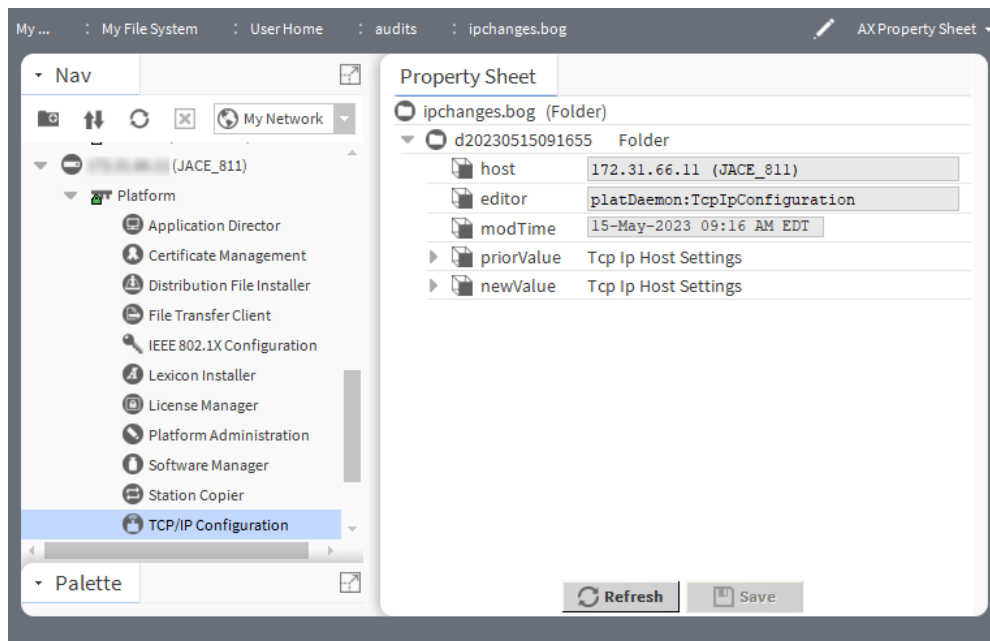
Step 1   Expand **Platform** and double-click **TCP/IP Configuration**.

TCP/IP Configuration view opens.
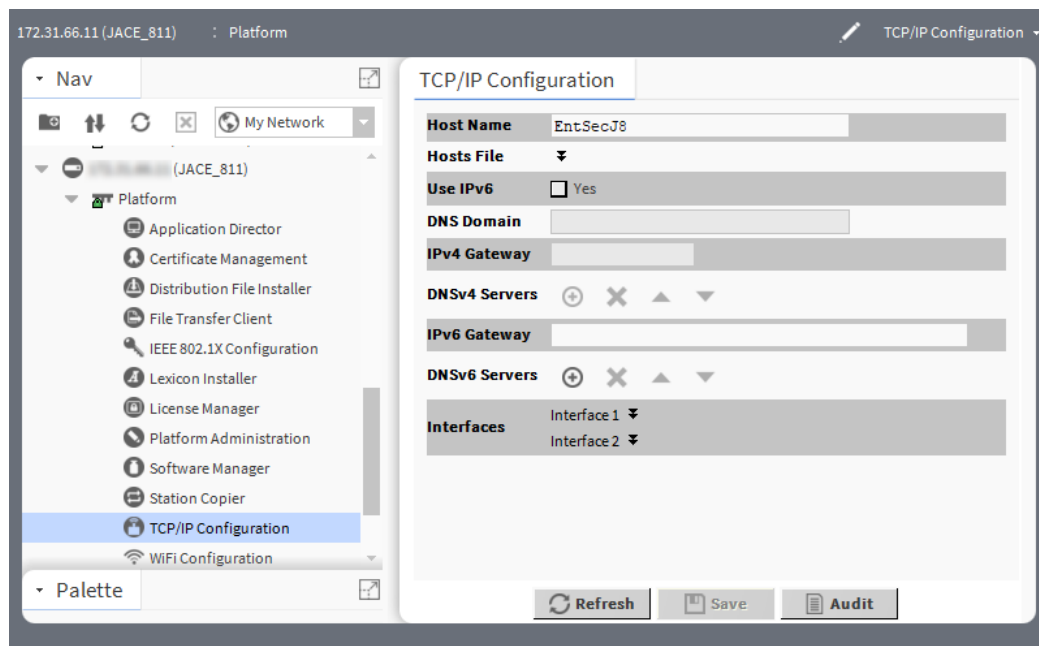
Step 2   Click the **Audit** button.

The `ipchanges.bog` folder's **AX Property Sheet** opens.

Child folders are date-named using the following convention:

<yyyymmddhhmmss>, where the variable name contains year, month, day, hours, minutes, seconds; for example, d20250113153640 for 2025 Jan 13 3:36pm and 40 seconds.

- **priorValue** reports the TCP/IP settings that existed before the change.
- **newValue** reports the TCP/IP settings that existed after the change.

Step 3   Expand the folder and expand either **priorValue** or **newValue**.

The included decoded **modTime** value is easier to read. For example, 13-Jan-2024 03:36 PM EST instead of d20150113153640).

Reviewing a PC's TCP/IP changes

You configure a PC's TCP/IP settings using Windows. Workbench records TCP/IP before and after the change values in an ipchanges.bog file. If necessary, you can review these changes.

Prerequisites: You are working in Workbench with a connection to your PC.

Step 1   In the Nav tree, expand **My Host→My File System→User Home→ipchanges.bog**.

Child folders are date-named using the following convention:

<yyyymmddhhmmss>, where the variable name contains year, month, day, hours, minutes, seconds; for example, d20250113153640 for 2025 Jan 13 3:36pm and 40 seconds.

Step 2   To expand a folder, right-click and select **Views→Property Sheet**.

The **AX Property Sheet** for the folder opens.
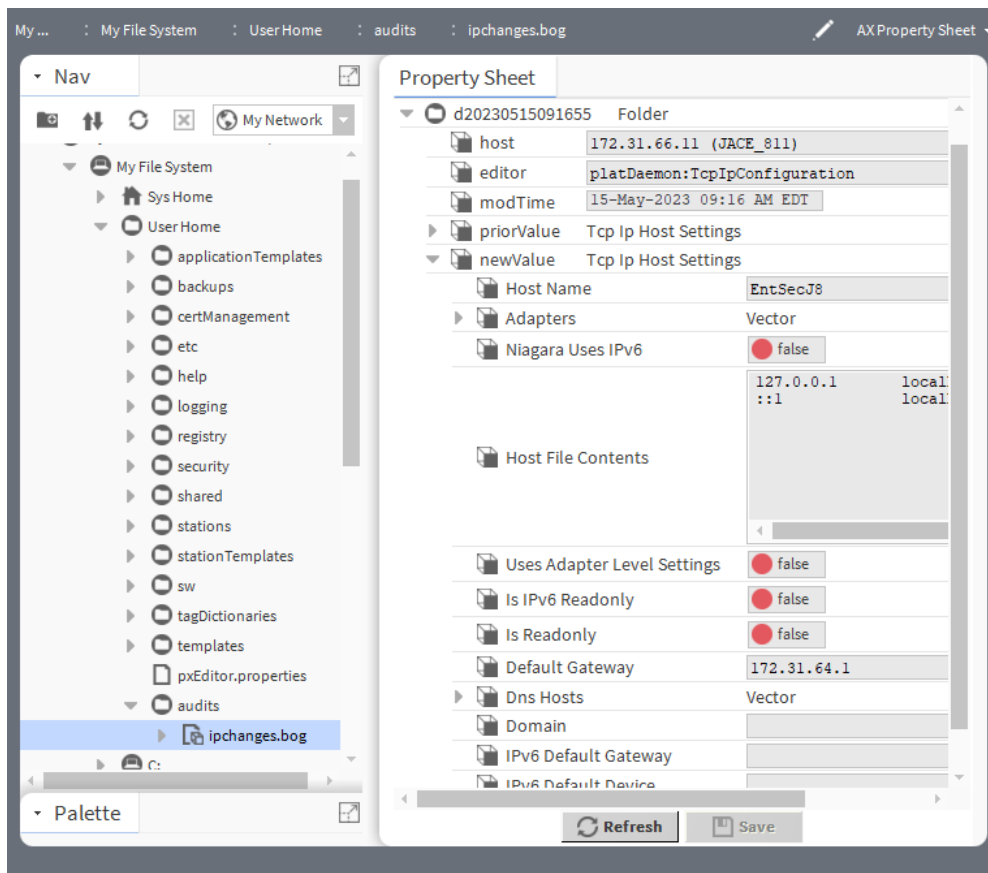
The included decoded `modTime` value is easier to read. For example, `13-Jan-2024 03:36 PM EST` instead of `d20150113153640`).

Under each folder are two properties:

- `priorValue` reports the TCP/IP settings that existed before the change.
- `newValue` reports the TCP/IP settings that existed after the change.

Step 3   Expand a `priorValue` or `newValue` to see the reported settings.

Restoring factory defaults (JACE-9000)

The process of recovering factory defaults deletes all platform and station data, and returns the controller to the state it was in when it shipped from the factory. If you cannot commission the controller because you made an error when entering the default platform daemon credentials or passphrase, you can restore factory defaults and start again. Also, when decommissioning a controller, a best practice is to recover the factory defaults, which removes the platform and station data from the controller. This procedure uses a terminal emulator program to access the controller's system shell menu.

Prerequisites:

- You have administrator-level platform credentials.
- You have backed up all data from the controller.
- If you are planning a "power—on" reboot using the serial shell menu
  - The controller's **DEBUG** port is connected to your PC using a USB-to-micro USB cable.
  - Power is currently applied to the controller.

– You are logged into to the controller serial shell using a terminal emulator (system shell program), such as PuTTY and the serial shell menu is visible on your PC.

CAUTION: Recovering factory defaults removes all platform and station data from the device. Make sure this is what you intend before you follow this procedure.
To reset a JACE-9000 to factory default state:

Step 1   With the outer panel cover open, press and hold the **SHUT DOWN** button on the JACE-9000 contol panel.
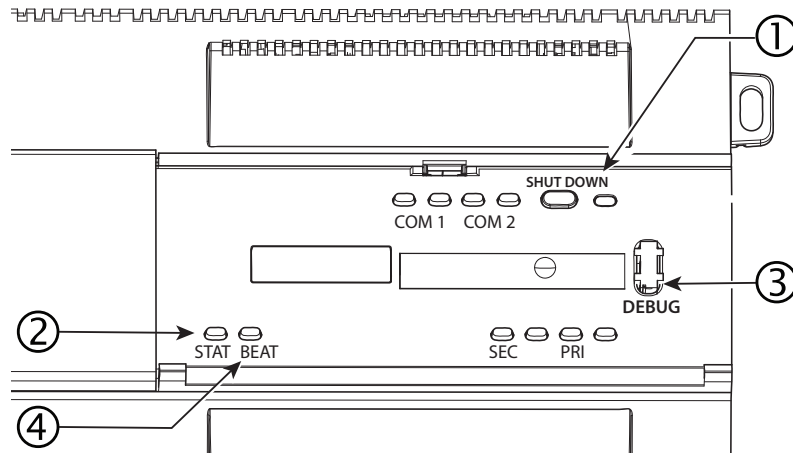
1	**SHUT DOWN** shuts down the controller and serves as the factory defaults recovery button.
2	**STAT** (status LED) blinks during recovery of factory defaults.
3	**DEBUG** port is a USB-C port for serial debug communications between the controller and serial shell running in the PC.
4	**BEAT** (Yellow); heartbeat LED that blinks at 1Hz during normal operation. Refer to "BEAT (Heartbeat) LED" section for details.

Step 2   While still pressing the **SHUT DOWN** button, reboot the controller using one of the following actions:

- Add power to a powered off controller.
- Choose option **9 Reboot** from the serial shell menu and enter "Y" at the confirmation prompt.

Reboot is initiated.

Step 3   Release the **SHUT DOWN** button 5 seconds after reboot is initiated.

Factory default restoration process begins.

When the **BEAT** LED blinks at normal rate the process is complete.

To setup the restored controller platform you will need to login to the serial shell using factory default credentials.

Index