

Technical Document

JACE NiagaraAX Install & Startup Guide

June 3, 2016



JACE NiagaraAX Install & 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, 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.

Copyright and patent notice

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

Copyright © 2016 Tridium, Inc. All rights reserved.

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

CONTENTS

About this guide	iii
Document change log	iii
Related documents	iv
Chapter 1 Overview	1
Commissioning notes	1
Factory-shipped state	3
IP address	3
HTTP port for platform access	3
Platform daemon credentials	3
Chapter 2 Preparation	5
Provide power and connectivity	5
Niagara and PC Requirements	5
Preparing to commission a new controller	5
Connect to the controller	6
Opening a platform connection to a controller	6
About converting a controller	7
About upgrading stations	8
Running the plat makeportable command	8
Chapter 3 Controller commissioning	11
Starting the Commissioning Wizard	11
Request or install software licenses	13
Set enabled runtime profiles	15
Install a station from the local computer	15
Install lexicons	17
Install/upgrade modules	18
Install/upgrade core software	20
Configure TCP/IP network settings	21
Replacing platform default user account	23
Review and finish the wizard	24
Chapter 4 About Platform Services	29
Host commissioning services	30
Power monitoring configuration	30
Configuring a controller with backup battery but no SRAM	31
Configuring a controller with SRAM and a backup battery	32
Configuring JACE-700	34
Managing PlatformServices properties	36
Properties unique to the JACE-700	39
Enabling or disabling SRAM support	39
Configuring controller serial port	40
Performing platform administration	42

Modem configuration 44

Chapter 5 Recovery tips45

 Reviewing TCP/IP changes..... 45

 System shell 46

 About system shell menu 46

 Update Network Settings 47

 About serial shell mode..... 49

 Connecting to a serial system shell 50

Index.....53

PREFACE

About this guide

This document covers the initial NiagaraAX software installation and configuration for a QNX-based JACE controller, using either Workbench AX-3.7, AX-3.7U1, AX-3.8, or AX-3.8U1.

Applicable controllers include the latest models (JACE-3E, JACE-6E, JACE-603, JACE-645, JACE-7), the JACE-6 and JACE-2 series (JACE-2/6), the JACE-7 series, the JACE-x02 Express (M2M JACE), as well as any earlier JACE-4/5 series. Also applicable are properly licensed JACE-8000 controllers (Niagara 4.1 or later) that are converted to run AX-3.8U1. For details on this conversion, see the *JACE-8000 Install and Startup Guide*.

The information in this document is intended for engineers, technicians, or service persons performing control system installation. All information in this document is also online in Niagara Workbench help, providing that the **docJaceStartup** module is installed.

This document does not cover station configuration of NiagaraAX components. For more information on these topics, refer to NiagaraAX online help and the *NiagaraAX User Guide*.

Terms "JACE-603" and "JACE-645" can apply to JACE-403 and JACE-545 controllers that have been outfitted with a "retrofit board". If such a controller needs to run Niagara R2Niagara R2 instead of NiagaraAX, please refer to the *T-RB-603 and T-RB-645 Retrofit Board Install Guide* in place of this document.

For physical mounting and wiring details for any JACE controller, please refer to its specific hardware installation document. For example, the *JACE-6 Mounting and Wiring Guide*.

Document change log

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

- June 3, 2016 — Edited for update release AX-3.8U1:
 - In About this guide, added update release AX-3.8U1 to the first paragraph. And in the second paragraph, added information about JACE-8000 controllers running AX-3.8U1.
 - In the Overview chapter under the heading "Commissioning notes," added the sections, "AX-3.8U1 specific commissioning notes" and "Data and security."
 - In the Preparation chapter, added several topics: "About converting a controller" which references appropriate documents for details and cautions about the loss of data that results from conversion. "About upgrading stations" which provides information about upgrading from earlier releases to AX-3.8U1. Specifically, provides details regarding AX-3.6U4 stations with the CryptoService, and using the `plat makeportable` command to convert AX-3.6 or AX-3.7 stations (which have reversible passwords encrypted with the keyring) to a portable encoding format so that they can be loaded in an existing AX-3.8U1 installation. Also, added the procedure, "Running the plat makeportable command".
 - Additional minor changes throughout including several updated images.
- December 4, 2015 — Minor corrections throughout.
- November 6, 2013 — Edited for the initial NiagaraAX-3.8 release (denoted as "AX-3.8" in this document):
 - A beginning section was edited and retitled JACE commissioning notes for AX-3.8 and AX-3.7U1, with new subsections AX-3.8 specific commissioning notes and Platform credentials notes for AX-3.8. Related to changes in AX-3.8, other document sections had new or expanded notes, including the following sections: "Connect to the JACE", "Start the Commissioning Wizard", and "Platform daemon authentication".

- May 31, 2013:
 - Edited for the security-oriented AX-3.7 "Update 1" release (AX-3.7U1, or build 3.7.105 or later), concurrent with (and required by) the newest JACE-3E series platform. The JACE controller has onboard SRAM like NPM6E-based controllers (JACE-6E, JACE-603, JACE-645), and platform commissioning for all these Hotspot JVM controllers is comparable.
 - Document changes include a new beginning section "JACE commissioning notes for update 1 release". Another change for AX-3.7U1 and later is in the module selection for a Hotspot JVM controller being configured for SSL—modules **cryptoCore** and **daemonCrypto** are no longer selected, only **platCrypto**. See "Select modules", including

NOTE: If upgrading a previously SSL-configured AX-3.7 Hotspot JACE to AX-3.7U1 or later, the Commissioning Wizard automatically takes care of these module location differences, by updating all modules in their proper locations, then removing the older **cryptoCore** and **daemonCrypto** modules from controller's `!modules` folder.

- Various other minor changes are in other sections—mostly as new or reworded "Cautions" or "Notes" relating to best security practices.

May 30, 2012:

- Reworked entire document to reflect NiagaraAX-3.7 changes to Workbench platform tools, including the platform Commissioning Wizard. Therefore, this is now a "versioned" document that applies to NiagaraAX Workbench starting in AX-3.7. Most screen captures were updated from the previous document, and various minor changes were made that are too numerous to mention.
- The basic focus of this document remains unchanged—to describe the commissioning of a new JACE using the platform Commissioning Wizard. See the Important Commissioning Wizard notes for a summary of some noticeable wizard changes, starting in AX-3.7. Included are the reordering (and lesser importance) of the "Install Lexicons" step, and some additional module information noted in the "Select modules" step. See Install lexicons and Select modules for related details.
- Starting in AX-3.7, a station's PowerMonitorService (platform service) has an improved default view (plugin), which is described and shown in various sections under the section JACE power monitoring configuration. With more SRAM-equipped JACE controllers becoming available, this configuration may have increased importance, along with the configuration described in the section JACE SRAM support enabling/disabling.

Related documents

Following is a list of related guides.

- *NiagaraAX Platform Guide*
- *NiagaraAX User Guide*
- *AX to N4 Migration Guide*
- *JACE-8000 Install and Startup Guide*

CHAPTER 1 OVERVIEW

TOPICS COVERED IN THIS CHAPTER

Commissioning notes

Factory-shipped state

As shipped from the factory, new JACE-3,-6,-7 series controllers are shipped with a bare minimum of core Niagara software to run a platform daemon, along with a Tridium certificate, but not all items needed to run any type of station. Using Workbench, you open a platform connection to the controller to begin the commissioning process.

You can also configure any properly licensed QNX-based "Hotspot JACE" for secure, encrypted (SSL or TLS) platform access, as well as SSL access for station (Fox) client connections or station browser (WebService) connections. Details are outside the scope of this document. See the *NiagaraAX SSL Connectivity Guide* for complete details.

Using a major software version of Workbench which matches that of the controller (AX-3.x), connect to the new controller and *commission it* to install the necessary core software, selected modules, license(s), and do other platform configuration. Some important related tasks include setting the controller's:

- IP network address, and related IP networking parameters
- Platform daemon user(s), for platform login
- Time and date (or simply sync with your PC's time).

This document provides step-by-step instructions for these and other tasks. To do this you use the platform Commissioning Wizard.

This wizard is the only way to install the needed Niagara core software in a controller. Most steps in the Commissioning Wizard are also available as separate platform views. For example, there is a **Software Manager**, **License Manager**, and many others. Using these views individually may be useful *after commissioning* a controller. For more details see the *NiagaraAX Platform Guide*.

NOTE: Always use the Commissioning Wizard to commission a new controller, as well as to upgrade any controller from one Niagara point release to another—and make sure a license file is available.

Commissioning notes

AX-3.8U1 specific commissioning notes

It is possible to convert JACE-8000 controllers (N4.1 or later with the added JACE-8000-AX license feature) to run AX-3.8U1. Note that you must run a conversion dist from Workbench (N4.1 or later) and on completion the controller is changed to the AX "clean" state. At this point, you must use the AX-3.8U1 Workbench to commission the controller. Refer to the JACE-8000 Install and Startup Guide for details on the conversion procedure.

CAUTION: 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.

Data and security

Conversion clears all data in the controller, including licenses and certificates, SSL certificates and key files, along with all station data and Niagara software. Only the controller's IP configuration is retained. Further, you must use the default platform credentials to regain access.

In the case of a new controller, this makes no difference. However, if you are migrating or converting an already-commissioned controller, make note of this.

Additionally, in the case where you are migrating a controller from AX to N4, the "AxtoN4" conversion dist file is not the same as a regular clean dist file. It is selectable only once. After conversion, at any point, you can choose to install a regular N4 clean dist file, to wipe the unit back to a near factory state. However, note in this case that any installed N4 licenses are retained, along with configured platform admin accounts and TCP/IP configuration.

For AX-3.8 and AX-3.7U1

After using AX-3.7U1 or later Workbench to commission a JACE and install a station, by default the station is now accessible in Workbench (open in Fox connection) only using AX-3.7U1 or later Workbench. Any earlier "non update" release of Workbench (for example, build 3.7.44) will be unable to open the station.

While this could be overridden in the JACE station (in a new "Legacy Authentication" property of its FoxService), doing so would compromise security. For related details, see the section "Fox Service properties" in the *Niagara Drivers Guide*.

Any other JACE commissioning operation affected by using either NiagaraAX-3.8 or AX-3.7U1 is noted in this document. Otherwise, the term AX-3.7 is simply used instead.

Note that AX-3.8 and AX-3.7U1 (and similar 2013 "update releases" for AX-3.6U4 and 3.5u4) handle station passwords in a way that affects system upgrades, and (for update releases) on-going station backup, copy, and restore functions. For more details, refer to the document *NiagaraAX 2013 Security Updates*.

AX-3.8 specific commissioning notes

When using AX-3.8 Workbench, note that default "Open Platform" and "Open Station" operations initially assume Platform SSL Connection and Fox SSL Connection types, respectively. This is intended to help encourage this SSL usage for all NiagaraAX platforms and stations—at least those that support this (all except "J9 JVM" QNX-based controllers, i.e. any JACE-2/4/5 series). If you change either connection type, Workbench "remembers" this type to use on your next connection.

Note any new JACE controller ships with a minimum load of core software, and requires a "non-SSL" platform connection for initial commissioning. This also applies to any JACE controller in which you installed a "clean dist" file ("Cleaning" from the platform Distribution File Installer view).

If needed, change the connection "Type" from a JACE Workbench "Open" dialog to a non-SSL connection type, at least until you have established regular connections and have configured and enabled SSL access. See the *NiagaraAX SSL Connectivity Guide* for complete details on the related tasks and concepts.

Platform credentials notes for AX-3.8

Note whenever you are using the AX-3.8 Commissioning Wizard, platform credentials are always handled as expected. If you are commissioning a controller for AX-3.8 from any earlier release, e.g. AX-3.7U1, AX-3.6, and so on (or from a "clean dist'd" unit in which you have already changed platform credentials), your non-default platform credentials are retained, or else set to whatever you specify in the AX-3.8 Commissioning Wizard's "Platform daemon authentication" step.

However, due to AX-3.8 security improvements in controller platform credentials, there may be confusion later regaining platform access after restoring a backup .dist file made from a controller running AX-3.8. Why? Because platform credentials are no longer stored in AX-3.8 station backup .dist files.

- If the controller was already running AX-3.8 before the backup .dist file install, its platform credentials will remain unchanged.
- However, if the controller was running any earlier release (including a "clean dist'ed" unit in which you have already changed platform credentials), any current platform credentials are reset to factory defaults. In this case, after the backup .dist file install, you need to reopen a platform connection using factory default credentials, and then "Update Authentication" from the Platform Administration view.

Factory-shipped state

The factory- shipped state of a controller has the following default settings for IP address, HTTP port and Platform credentials.

IP address

This topic discusses the controller's IP address.

When shipped, a new JACE-3,-6,-7 series controller is pre-configured with an IPv4 address in the range:

192.168.1.12n (*primary* LAN1 port; the LAN2 port is disabled).

where the last numeral (n) in the IP address matches the last numeral in the controller's *serial number*.

The default subnet mask is: 255.255.255.0

You change these IPv4 network settings during your startup commissioning of the controller.

HTTP port for platform access

When shipped, a controller's platform daemon is configured to listen on HTTP port 3011. Often, this is left at the 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.

Platform daemon credentials

Every controller is shipped with default platform daemon (administrator) credentials.

For example:

Username: tridium Password: niagara

Initially, you use these default credentials to open (log on) to a platform connection to a controller. Like the factory-assigned IP address, default credentials are *temporary*. Following conversion of the controller to, and 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*.

CHAPTER 2 PREPARATION

TOPICS COVERED IN THIS CHAPTER

Provide power and connectivity
Niagara and PC Requirements
Preparing to commission a new controller
Connect to the controller
About converting a controller
About upgrading stations

Consider the following areas to prepare before proceeding with commissioning: power, connectivity, software and PC requirements.

Provide power and connectivity

In most cases, you perform the initial Niagara software installation and startup of a controller (as described in this document) in your office, before physically mounting it in place at a job site.

Refer to your *JACE-xxx Mounting and Wiring Instructions* for details on making (temporary) power wiring and Ethernet wiring connections.

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 and PC Requirements

These instructions assume that you have a PC running a licensed copy of Workbench installed with the installation tool option, which copies the distribution files needed for commissioning various models of controllers. This document refers to this workstation as “your PC.”

NOTE: Your PC must meet minimum hardware/operating system requirements for Workbench workstation. This includes a working Ethernet adapter with TCP/IP support (browser capable). An Ethernet TCP/IP connection to one or more host controller(s) is required to install software and establish other parameters.

For this initial Ethernet connection, you can use either:

- An Ethernet patch cable connected directly between your PC and a 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 commission a new controller

This procedure documents how to prepare for new controller commissioning.

- Step 1 If not already installed, install the Niagara software on your PC, including its permanent license.
- Step 2 Typically, the license file for the controller already resides on the licensing server, where (if you have Internet connectivity) it is *automatically retrieved* during the licensing step of the Commissioning Wizard.

NOTE: If you were *emailed* a license archive (.lar file) or .license file for the controller, and you wish to use it instead of the online license server (for some reason, for example your workstation will not have Internet connectivity when you are commissioning the controller), make the file available to Workbench first, as follows:

- a. Copy the file to your !licenses/inbox folder.
 - b. Restart Workbench.
- Step 3 Attach one end of a standard category-5 Ethernet unshielded twisted pair (UTP) patch cable to the RJ-45 Ethernet connector for LAN1 on the controller.
- Step 4 Attach the other end of the patch cable to a network port or directly to an Ethernet hub.
- Step 5 Power up the controller.
- Step 6 Record you 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.

As an alternative to re-assigning your PC's IP address, you can do one of the following:

- Obtain a USB-to-Ethernet network adapter (*second* network interface card, or NIC), and use it with an Ethernet crossover cable to commission controllers. In this case, configure this second NIC to use the settings in the *remainder of this step*. This method offers an advantage over the serial shell method below, as you do not need to reboot a controller in a special mode, i.e. change its serial shell jumper.
- Use a serial shell mode connection to the controller to re-assign its factory IP address settings. After making this change and rebooting the controller, you can continue commissioning using Workbench. This requires proper serial cabling and a special power-up mode for the controller.

For this initial connection to a factory-shipped controller, configure your PC's NIC to use an IP address in the same subnet as the controller, 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 controller'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).

If not, from the menu bar, select **Window > Side Bars > Nav**.

Connect to the controller

Once the controller has powered up, you connect to it using the Workbench **Open Platform** menu option. A platform connection to any controller is required for *most host-level operations*. This includes installing core software and modules and performing various other platform tasks.

Opening a platform connection to a controller


A platform connection is required before running the Commissioning Wizard especially if you are upgrading a controller.

Step 1 From the menu bar, click **File > Open > Open Platform**.

The **Open Platform** window appears.

Step 2 Complete the fields in the **Open Platform** window as follows:

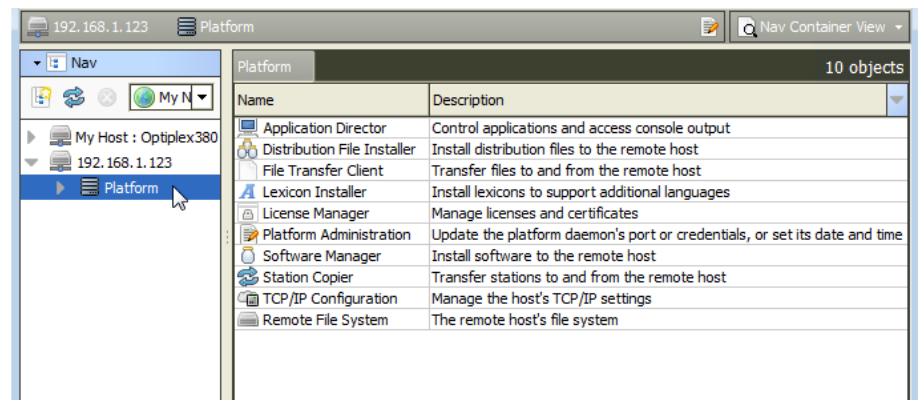
- **Type** — Select  **Platform Connection**, if not already selected.

NOTE: Workbench may default to a secure  **Platform SSL/TLS Connection**. If so, for any *new* controller, change type to a regular (non-SSL/TLS) platform connection. After conversion, you should always use the recommended SSL/TLS platform connection.

- **Host** — Leave set at the default **IP**, and type in the default IP address of the new controller.
- **Port** — Leave at default 3011.
- Credentials, which may be:
 - **Username** — Type in default username, for example: tridium
 - **Password** — Type in default password, for example: niagara

Step 3 Click the **OK** button to accept all settings.

The platform opens in the tree, and its Nav Container View displays in the view pane.



CAUTION: When commissioning a new controller, you should always change platform credentials from defaults! Note that the **Commissioning Wizard** includes a step for this (“Platform daemon authentication”), which you should not omit. A controller installed with default platform credentials is extremely susceptible to unauthorized access. If using AX-3.8 be sure to see “Platform credentials notes.”

NOTE: After you commission a controller and it reboots, in future platform sessions you must login using any new (changed) parameters, such as IP address, Port, Credentials. If you changed your PC's IP address in order to connect to the controller's factory-assigned IP address, you must first reconfigure your PC to the appropriate TCP/IP settings (to communicate to the now-commissioned controller).

About converting a controller

It is possible to convert certain AX controllers (JACE-3,-6,-7 series) to install as Niagara 4 devices. Similarly, you can convert a properly licensed JACE-8000 (N4.1 or later) controller to run AX-3.8U1. However, in order to do either of those things you must first convert the controller

(via clean dist or conversion dist) to the appropriate target software release before running the Commissioning Wizard.

Refer to the following documents for more information:

- For details on converting from AX to N4, see the *AX to N4 Migration Guide*
- For details on converting a JACE-8000 to run AX-3.8U1, see the *JACE-8000 Install and Startup Guide*

CAUTION: Conversion erases all licenses, certificates, and configuration data in the unit except TCP/IP configuration. Prior to converting, you should successfully backup the controller's station, have a license specific to the unit, and also (if applicable) export any SSL/TLS certificate Trust Stores and Private Key Stores in use.

About upgrading stations

If upgrading a station from a prior release to AX-3.8 you may encounter incompatibility issues due to security enhancements in AX-3.8. Preparatory steps described here facilitate such upgrades.

AX-3.6U4 stations with CryptoService

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.

Stations with non-portable password encoding

For any AX-3.6 or AX-3.7 station, which has reversible passwords encrypted with the keyring, the station cannot be copied to an existing AX-3.8 installation without first converting the passwords to a portable encoding format. In AX-3.8U1, running the "plat makeportable" command converts a station's non-portable passwords and copies the converted station to the AX-3.8U1 stations directory. For details, see "Running the plat makeportable command".

Running the plat makeportable command

Use this command to convert AX-3.6 or AX-3.7 stations with non-portable password encoding to a portable encoding format in order to load in AX-3.8U1 installations.

Prerequisites:

- An installation of AX-3.8U1,
- The AX-3.6 or AX-3.7 station directories you wish to convert
- The security directories from the station's source installation

Perform the following steps:

Step 1 Open a **Console** for the AX-3.8U1 installation.

Step 2 Type the following command:

```
plat makeportable path/to/source targetName path/to/security
```

For example:

```
plat makeportable C:\Niagara\Niagara-3.6.406\stations\
stationToConvert convertedStation
C:\Niagara\Niagara-3.6.406\security
```

NOTE:

- If you leave the `securityDir` option blank the code assumes that the source station is in an existing Niagara installation and attempts to find that installation's security directory.
 - If you leave the `target` option blank the code assumes that the target station should have the same name as the source station.
 - If there is an existing station in the AX-3.8U1 installation with the same name as the target station, using the `-o` flag overwrites the existing station.
-

After running the command, the converted station is in the AX-3.8U1 stations directory with all reversible passwords converted to a portable format.

NOTE: If the following message is logged when running the command, the most likely cause is that the station was encrypted with a security directory other than the one specified: `WARNING [09:42:50 10-Feb-16 EST] [makeportable] Could not convert password slot:/Drivers/NiagaraNetwork/station/clientConnection/password:javax.crypto.BadPaddingException: pad block corrupted`

Usage notes

usage:

```
plat makeportable <flags> <sourceStationDir> [target] [securityDir]
```

parameters:

`sourceStationDir` the station directory to convert

`target` the name of the target station.
Defaults to the name of the source station.

`securityDir` the security directory of the source station.
Defaults to `<sourceStationDir>/../../security`

optional flags:

```
-o                overwrite existing destStationDir
-llocale:<x>      set the default locale (en_US)
-@<option>       pass option to Java VM
-buildreg        force rebuild of the registry
```


CHAPTER 3 CONTROLLER COMMISSIONING

TOPICS COVERED IN THIS CHAPTER

Starting the Commissioning Wizard
Request or install software licenses
Set enabled runtime profiles
Install a station from the local computer
Install lexicons
Install/upgrade modules
Install/upgrade core software
Configure TCP/IP network settings
Replacing platform default user account
Review and finish the wizard

Use the Commissioning Wizard when installing a *new* host or upgrading an existing host.

The Commissioning Wizard provides a checklist method to perform essential (and often one-time) platform tasks.

Launch the Commissioning Wizard by right-clicking the **Platform** node in the Nav tree or by clicking the **Commissioning** button in the **Platform Administration** view.

Before starting the commissioning process, note the following points:

- Throughout the wizard's windows, use the buttons **Back** and **Next**, as needed, to retrace (or skip) steps and advance to the next step. Also, the **Cancel** button exits the wizard after your confirmation—no operations are performed as a result.
- Before committing to the final sequence of steps, the wizard provides a summary for you to review.

Starting the Commissioning Wizard

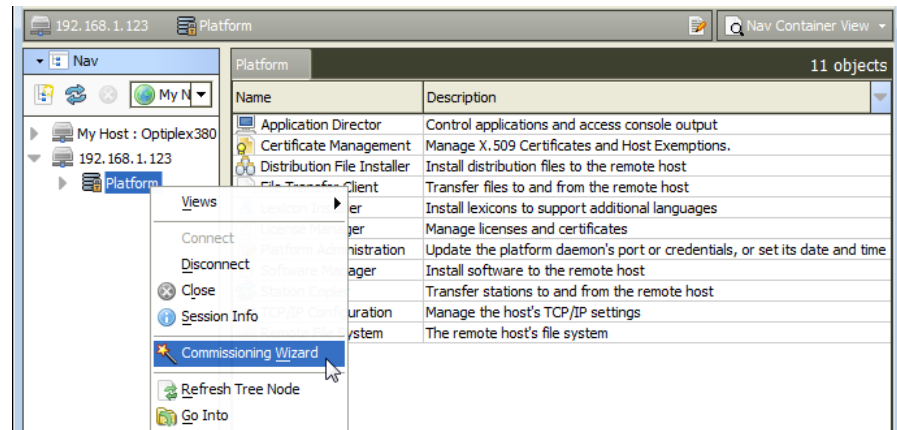
The **Commissioning Wizard** runs a series of steps to guide you through all the needed information.

Prerequisites:

- The major software version level of the remote host controller to be commissioned must match that of the Workbench version that you use. For example, you can commission a Niagara 4 controller only with the Niagara 4.x Workbench, and commission a NiagaraAX-3.x controller only with the AX-3.x Workbench.
- Your PC has internet access

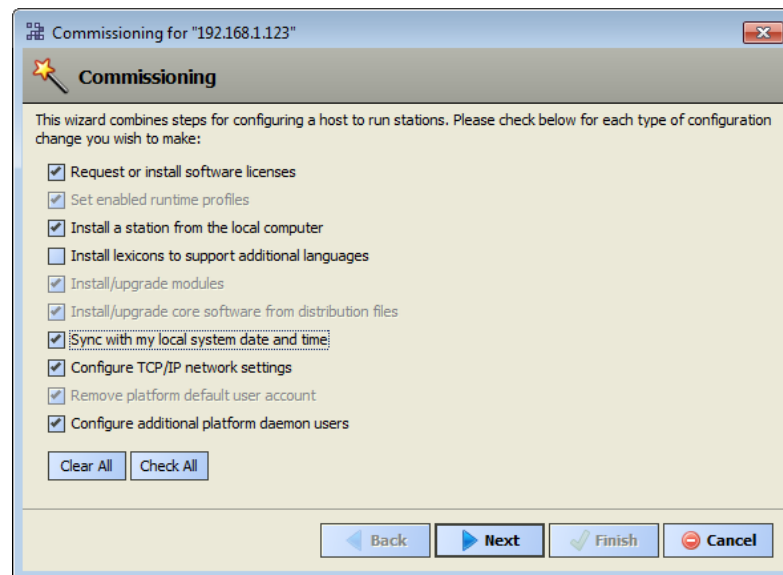
Step 1 Using Workbench on your PC, make a platform connection to the remote host.

The **Platform** home window opens.



Step 2 In the Nav tree, right-click **Platform** > **Commissioning Wizard**.

The **Commissioning for "<IP address>"** window opens for the remote controller, which it identifies by the controller's IP address.

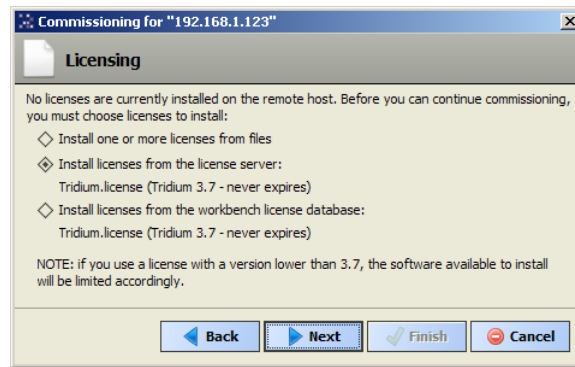


By default, all steps are preselected except **Install lexicons to support additional languages** (for file-based lexicons). Steps are executed in the order listed in this **Commissioning** window.

Step 3 As needed, click to include or omit steps and click **Next**.

For a new controllers, you typically *accept all default selections*.

The Licensing step opens.



- 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 controller 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 admin 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).

Request or install software licenses

This step retrieves one or more licenses from the licensing server and installs them on the host controller. For license files validated against the Tridium certificate, installation can be automated from Workbench. All such purchased licenses (including host controller, Supervisor, or workstation-only) are stored and available through the licensing server.

Prerequisites: A minimum of one license is *always* needed. Typically, other licenses are not needed unless you are using third-party module(s). In this case, you can also install those license files during this same commissioning step, either automatically, or by selecting to install from files.

Step 1 Select **Install licenses from the license server**.

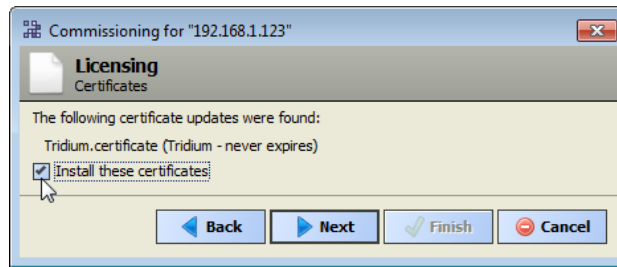
Workbench silently searches the web portal for a license with the matching *Host ID* of the target platform. When found, it selects the license(s) and advances to the next wizard step.

If the license server option does not appear, Workbench has *not* detected Internet connectivity, and so cannot contact the licensing server.

Step 2 If you do not have internet access choose one of two options:

- If you already have a license for this controller in your local license database, select the *last* option to install from your the database. This option is missing if your local license database does not include a license for this controller.
- If you have the license file(s) in another location, use the procedure, **Installing or updating licenses from files**. If necessary, you can install license(s) later, either from your local license database or from license files.

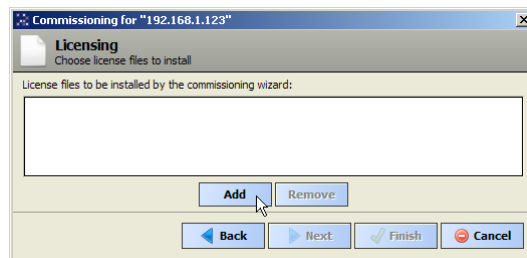
The wizard locates the license(s) that match the *Host ID* of the target platform, and advances to the next step.



Step 3 Select **Install these certificates** and click **Next**.

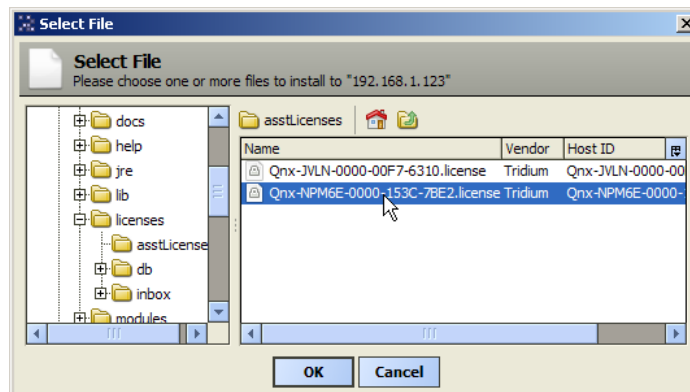
Step 4 Select **Install one or more licenses from files** and click **Next**.

The **Choose license files to install** step opens.



Step 5 Click **Add**.

A **Select File** window opens. By default, the system lists the files in your `licenses` subfolder. This includes your Workbench license). If you previously pointed Workbench to another location, the system lists the license files in that location instead.



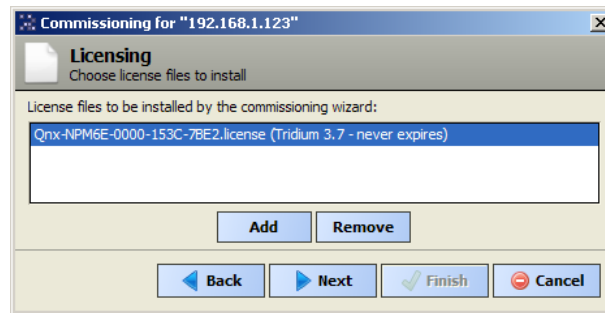
Step 6 Do one of the following and click **OK**.

- If you see the license you need, click it to select it. To select more than one license hold the **Ctrl** key while you click.
- If a license is not listed, navigate to its location using the left-pane folder tree controls, and click the license to select it.

NOTE: The licensing tool prevents selection of a wrong license (different hostid) to install in the JACE.

Step 7 If necessary, click the **Add** button again to add additional license files.

Step 8 When all needed licenses are listed in the **Choose license files** window, click **Next** to go to continue.

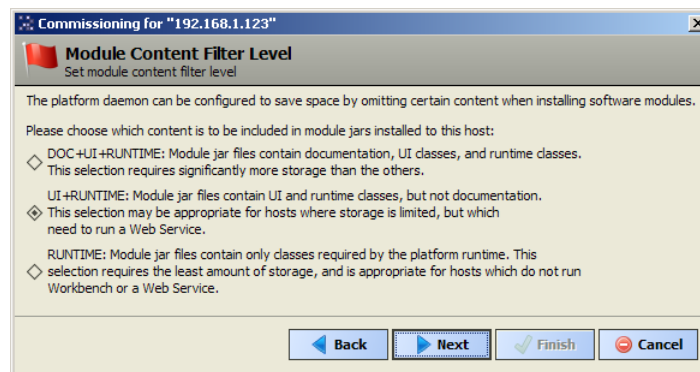


For more licensing information, refer to the section the *NiagaraAX Platform Guide*.

Set enabled runtime profiles

Module content filter level affects how much storage space is used when installing modules. Usually, the default (preselected) level is appropriate for the opened platform.

Step 1 Click the desired level of content in modules to be installed in this controller:



Module content level is one of the following:

- **DOC+UI+RUNTIME** — Typically not appropriate for any QNX-based platform.
- **UI+RUNTIME** — Required if the platform is to run the Web Service.
- **RUNTIME** — Typically best for any QNX-based platform not running the Web Service.

NOTE: Following commissioning, you can also *change* the enabled runtime profiles, working from the **Platform Administration** view. For details, see the *NiagaraAX Platform Guide*.

Step 2 Click the **Next** button for the next step.

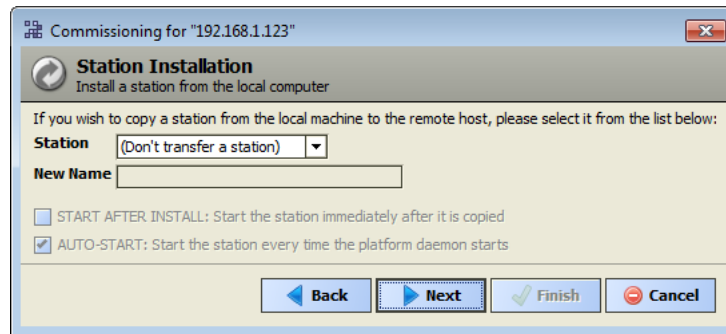
Install a station from the local computer

If you have a specific station database ready to install in the host, you can specify it at this step in the wizard. This step is recommended.

Prerequisites: The station database for this host exists and is available on the computer.

Figure 1. Station Installation dialog (default)

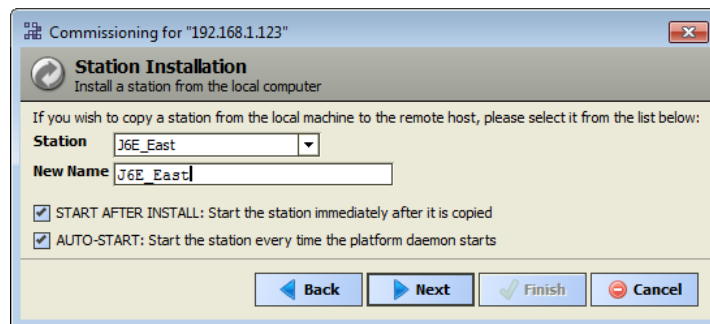
Step 1 To install an existing station, select the station from the drop-down list or, accept the default (Don't transfer a station) and click **Next**.



Station lists the subfolders under your PC's local stations folder.

You can create a station later using the **New Station Wizard**, and install it using the platform's **Station Copier**. Or you can select an existing station to install using the **Station Copier**.)

If you select a station, the following additional options are available:



- **New Name**

Either leave at same station name as local copy, or type in a new station name.

- **START AFTER INSTALL**

If enabled (the default), and a reboot is *not* included at the end of commissioning, when commissioning completes the station is restarted. In cases where commissioning ends in a reboot, such as if commissioning a new controller (installing core software) and/or changing TCP/IP settings, the next "AUTO-START" setting determines if the installed station is started following the reboot.

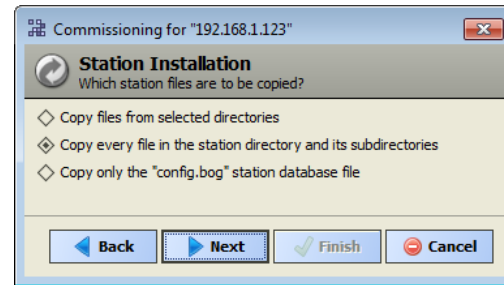
- **AUTO-START**

If enabled (the default), the station starts every time you reboot the host. This is recommended.

NOTE: 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 software modules needed by the station are installed (along with all station files), but the station is idle. To start the station you must reopen a platform connection to the controller following the reboot, starting 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 you are doing this in the **Application Director**, be sure to enable **AUTO-START** on the selected station. Otherwise, it remains "idle" after the next controller reboot.

Step 2 Click the **Next** button to continue.

The Commissioning Wizard asks which station files to copy, where you can select *one* of the following:



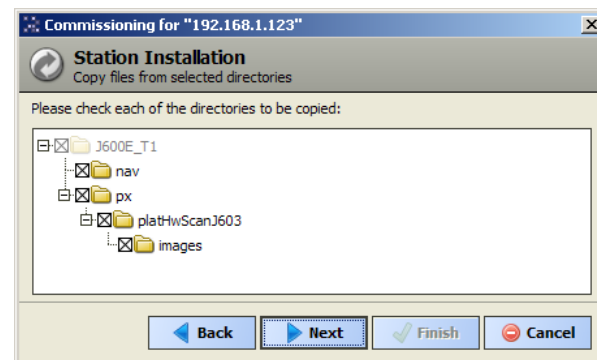
Step 3 Select one of the following:

- **Copy files from selected directories** allows you to specify which subfolders under that local station to copy by opening a folder chooser.
- **Copy every file in the station directory and its subdirectories** is the most typical option. It may be *unavailable* (missing) if the source station folder contains alarm and/or history data. In this case, you should choose the first option (copy files from selected directories), and decide if copying the alarm and/or history data is appropriate.

NOTE: The valid use case for this option is when migrating a controller. However, copying the identical alarm/history data to *multiple* controllers is a *bad practice*.

- **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 4 If you selected **Copy files from selected directories**, click folder controls to expand and contract as needed.



Selected folders appear with an "X" and unselected folders show an empty folder box.

Step 5 Click the **Next** button for the next step (or if skipping that step, go to "Select modules").

Install lexicons

This step installs one or more text-based lexicon file sets in the host controller to support additional languages. 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 Workbench.

Prerequisites: The lexicon file(s) to install are in the !lexicons folder under your Niagara-AX Workbench home folder

NOTE: In some domestic (U.S.) installations, an English lexicon ("en") is added and configured to globally "customize" items such as property descriptions in Workbench. For complete details on working with lexicons, refer to the *NiagaraAX Lexicon Guide*.

In order to select lexicons (file sets), they must be under a !lexicons subdirectory of your NiagaraAX Workbench home folder. Note that starting in AX-3.7, the Workbench installation no longer includes such lexicon file sets (along with your selection of them)—instead "standard" lexicons are now distributed as jar'ed software modules, which you select and install in the next step.

However, if you copied such lexicons from a previous NiagaraAX Workbench release, they will be available to install in this step. Typically you customize (edit) them using the Lexicon Editor in Workbench. Afterwards, you install them in host platforms, so that each has the proper changes.

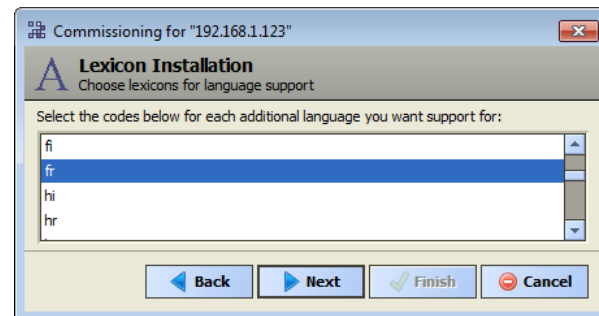
Perform the following steps:

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.

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



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.

Install/upgrade modules

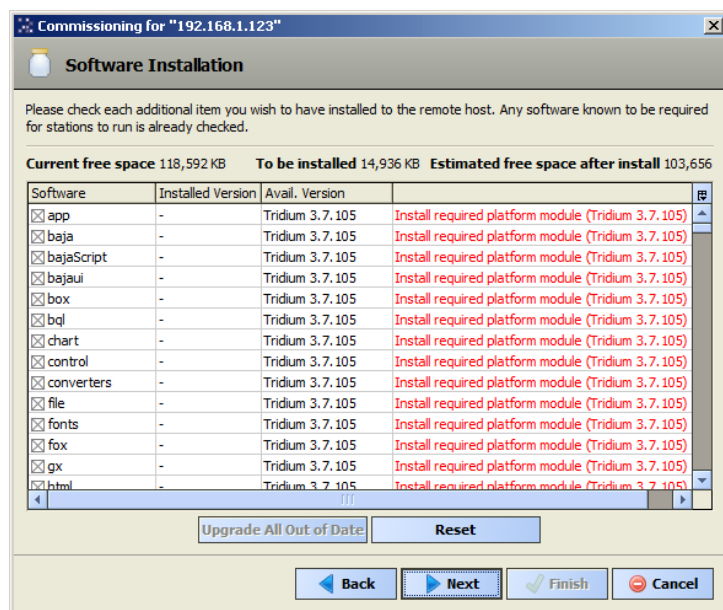
Always preselected, whenever the wizard is run, this step selects the software modules, and optionally any lexicon modules to install.

As the step begins, the wizard identifies the dependencies required by the controller compared against the available software modules in your Workbench PC's software database. A brief pop-up message displays, "Rebuilding software list." During commissioning, you add to the software modules that are preselected for installation. Sometimes you may not need to make any changes, as the wizard may preselect all the necessary core modules, plus any additional modules needed by the station you previously specified in the Install Station step.

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

Perform the following steps:

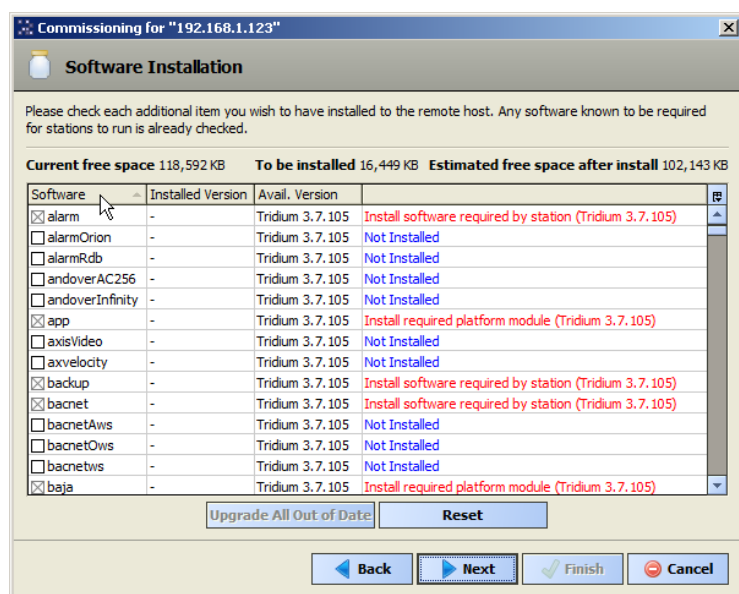
Step 1 Review the list of available modules.



This list is long and requires you to use the scroll bar. Each selected module has an “X” in its selection box.

In addition, note the following:

- Modules preselected because they are core modules or station database modules each have a *red text* descriptor. By default, these modules are at the top of the list and you cannot deselect them.
- To re-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 reset the selection of modules to the original collection, click the **Reset** button.



The image above shows the window after modules were selected and the list resorted alphabetically.

- Step 2 To select additional modules to install, click the selection boxes.

The description for each is in *blue text*. In general, do not select modules if you are not sure they are needed. You can manage software modules anytime later, using the **Software Manager**. Also, if you install a station later, the **Station Copier** automatically prompts for confirmation to install any additional modules deemed necessary.

- Step 3 If JACE-6 or JACE-7 controller is equipped with the SRAM option card (for battery-less operation), select the `platDataRecovery` modules for installation

This module provides the Data Recovery Service in the station's **PlatformServices**.

If you are running JACE-3E or any NPM6E-based controller, such as JACE-6E, JACE-603, or JACE-645, this module are unnecessary to select. They are automatically included in the core config distribution file for those platforms.

- Step 4 For any installed station to have the Hardware Scan Service in its **PlatformServices**, select the appropriate `platHwScanType` modules.

For example, select `platHwScanNpm` modules if commissioning JACE-3E, JACE-6, or JACE-6E.

See *Engineering Notes* for more information about the Hardware Scan Service.

- Step 5 To add language support, select a lexicon module.

Standard lexicon modules appear listed using a module name convention of:

`niagaraLexiconLc`

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 use different naming).

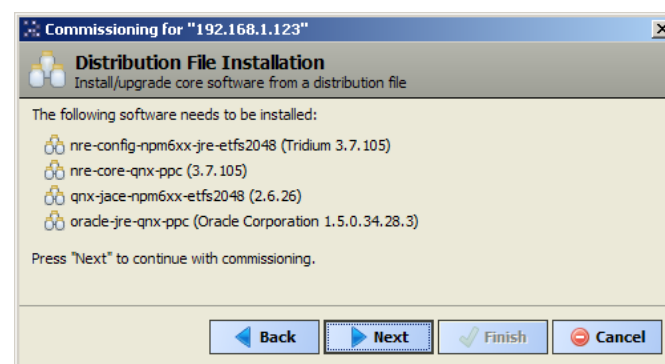
- Step 6 Click the **Next** button to go to the next step

Install/upgrade core software

The core software to install at this step depends on platform dependencies and available software modules.

- Step 1 If you have not already done so, click **Next** to advance to the **Distribution File Installation** step.

At step, the wizard compares the platform dependencies against the distribution (dist) files available in your PC's software database. The result is a list of the dist file(s) that need to be selected for installation.



- Step 2 Click **Next** to select the distribution files.

The wizard synchronizes the software with the local system date and time.

Configure TCP/IP network settings

This step sets up the properties required for client stations to connect to this server. IPv6 support is available, however this document focuses on IPv4 configuration. For details on IPv6, refer to the *NiagaraAX Platform Guide*.

Step 1 If you have not already done so, click **Next**.

The **TCP/IP configuration** window opens.

The screenshot shows the 'TCP/IP configuration' window titled 'Commissioning for "192.168.1.123"'. The window is divided into several sections for configuring network settings.

- Host Name:** NFM6E-East
- Hosts File:** A dropdown menu.
- Use IPv6:** A checkbox labeled 'Yes'.
- DNS Domain:** Workgroup
- IPv4 Gateway:** 10.10.8.1
- DNSv4 Servers:** 8.8.8.8 and 8.8.4.4
- IPv6 Gateway:** (Empty field)
- DNSv6 Servers:** (Empty field)
- Interfaces:**
 - Interface 1:**
 - ID:** en0
 - Description:** Onboard Ethernet Adapter en0
 - Physical Address:** 00:01:F0:8D:7A:06
 - Adapter Enabled:** ☒ Enabled
 - IPv4 Settings:**
 - DHCPv4:** ☐ Enabled
 - IPv4 Address:** 10.10.8.88
 - IPv4 Subnet Mask:** 255.255.255.0
 - DHCPv4 Server:** n/a
 - DHCPv4 Lease Granted:** n/a
 - DHCPv4 Lease Expires:** n/a
 - IPv6 Settings:** (Tabbed view)
 - Interface 2:** (Dropdown menu)

At the bottom of the window, there are buttons for 'Undo Changes', 'Back', 'Next', 'Finish', and 'Cancel'.


Step 2 Review, and if needed adjust other TCP/IP settings, which (in usual order of importance) include:

- **Hostname** —The default may be “localhost,” or enter another name you want to use for this host.

NOTE: In some installations, changing hostname may result in unintended impacts on the network, depending on how the DHCP or DNS servers are configured. If in doubt, leave hostname at default.

- **Hosts File** — Click control to expand edit field. Format is a standard TCP/IP hosts file, where each line associates a particular IP address with a known host

name. 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.

- **Use IPv6** — Enable if using this feature.
- **DNS Domain** — Enter the name of network domain, or if not applicable, leave blank.
- **IPv4 Gateway** — The IP address for the device that forwards packets to other networks or subnets.
- **DNSv4 Servers** — Click the  add button for a field to enter the IPv4 address of one or more DNS servers.
- **IPv6 Gateway** — Use this if you enabled **Use IPv6**.

Step 3 To add a line, click at the end of the last line and press **Enter**.

Step 4 Type in the required data on the new line.

To return to see all TCP/IP settings, click the control to contract the edit field when done.

Step 5 Review the settings for **Interface 1** on the **IPv4 Settings** tab, which include the temporary factory-shipped IP address.

Step 6 Do one of the following:

- If the network supports DHCP, enable it (click **DHCP Enabled**). In this case, the **IPv4 Address** and **Subnet Mask** fields become read only.
- Otherwise, a the host a unique **IPv4 Address** for the network you are installing it on. No other device on this network should use this same address. Include the appropriate **Subnet Mask** used by the network.

CAUTION: In general (for stability), static IP addressing is recommended over DHCP. *Do not enable DHCP unless you are certain that the network has DHCP servers!* Otherwise, the host may become *unreachable over the network*.

Step 7 To define a second interface, click the down arrows.

NOTE: JACE-3,-6,-7 controllers have two Ethernet ports, where **Interface 2** is available for configuring the LAN2 (secondary) Ethernet port. By default, this port is *disabled*, that is without a default address. Intended usage is for:

- Isolating a driver's Ethernet traffic from the primary (LAN1) interface, OR
- 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 host without disconnecting it from the network, or without connecting the technician's service PC to the customer's network (which might go against local IT security policies).

In any case, only *one* LAN port can be set as DHCP. If enabling LAN2, you typically specify another (network) static IP address and the appropriate subnet mask.

Also note the following:

- If enabling both LAN ports, the LAN1 IP address and LAN2 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 host *does not* provide IP routing or bridging operations between different Interfaces (LAN ports, GPRS, dialup).
-

Step 8 To reset all settings (all interfaces) back to their original pre-step values, click **Undo Changes**.

Step 9 Click the **Next** button to go to the next step.

Replacing platform default user account

At the platform daemon authentication step, you specify platform login credentials (user name and password) for this controller. To proceed, enter a different user name, along with a "strong" password (currently, this means a minimum of 8 characters, including at least one digit). You see this window only in the initial commissioning of a new host controller, or possibly at some future point after installing a clean dist file.

NOTE: The image shown here reflects "factory default" platform credentials—which you should always change. See the Caution below for details, and if using AX-3.8, see "Platform credentials notes for AX-3.8".

CAUTION: Be sure to change default platform credentials (user name=tridium, password=niagara). Consider the platform daemon as the highest-level access to the controller. Furthermore, make careful note of your entries. If you lose or forget these credentials, you may be unable to complete the commissioning and startup of this controller. In this case, you can restore platform credentials to factory defaults, providing you can serially connect to the JACE (make serial shell connection)—pressing a key at the prompted time during boot up. See “About JACE serial shell mode”.

Perform the following steps:

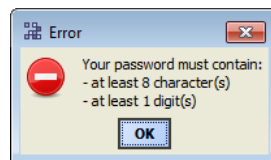
Step 1 In the **User Name** field, type in the desired user name for platform login.

This name can be 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 In the **Password** fields, type in a *strong password*.

User name and password entries are *case sensitive*.

A *strong password* is required (it must *match* in both password fields). Entry characters display only in asterisks (*). Password must be a *minimum of 8 characters*, using *at least one digit* (numeral). An error popup reminds you if attempt to enter a password that does not meet minimum rules.



NOTE: Some basic guidelines on strong passwords: 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 same as the user name. Don't use common numbers like telephone, address, birthday, and so on.

If you are not changing the controller's IP address during commissioning, the credentials for your replacement platform user are remembered in the current Workbench session. This can simplify platform re-connection to the controller after it reboots from commissioning. This is useful in a migration scenario.

However, you changed the IP address, you need to remember/re-enter the new credentials for a platform user in order to reconnect. .

Step 3 Make a careful note of your platform user credentials, and guard them carefully!

The platform daemon is the highest-level access to the host controller.

If you lose or forget these credentials, you may be unable to complete the commissioning and startup of this host. In this case, you can restore the factory default platform user, providing you can serially connect to the host (make serial shell connection), and press a key at the prompted time during host boot up following a power cycle.

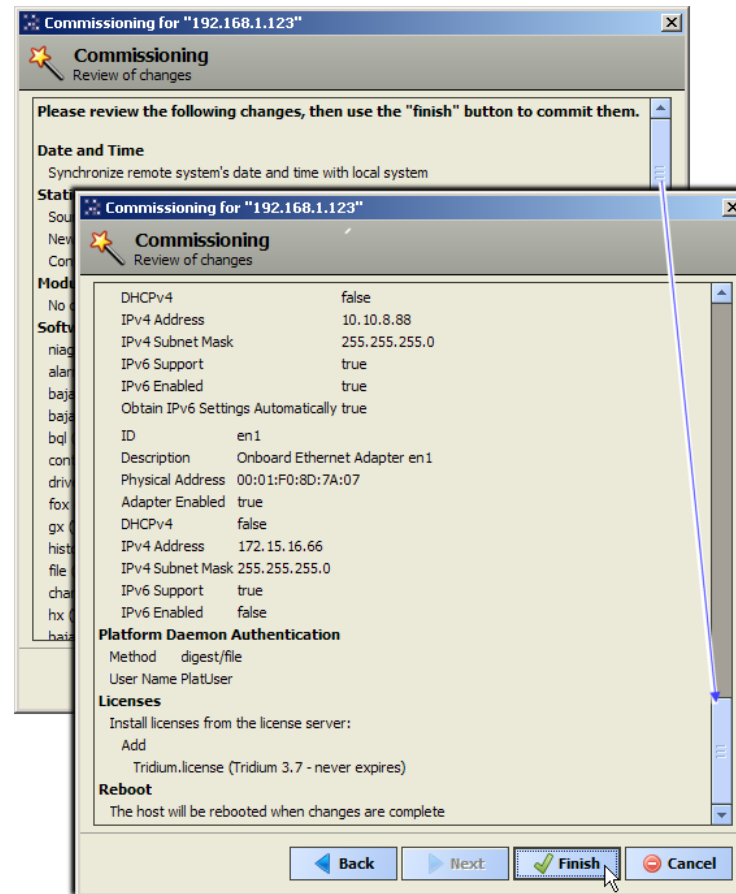
Step 4 Click the **Next** button. You typically proceed to the final commissioning (review changes) step.

Review and finish the wizard

The final step in the Commissioning Wizard provides a review of changes, as shown below.

Step 1 If you have not already done so, click **Next**.

The wizard displays a summary of all the changes to be made.

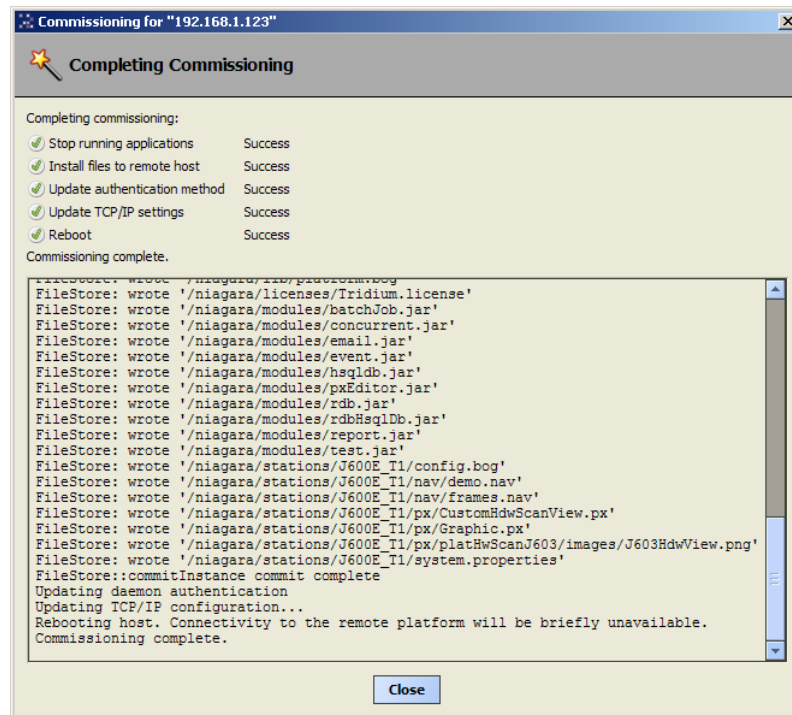


Step 2 Read through the changes, using the scroll bar to see those steps near the end.

Step 3 Do one of the following:

- If any change is needed, click the **Back** button until the step window appears, make the change, and click **Next** until this review window opens again.
- When no changes are needed, click **Finish** to initiate the rest of the Commissioning Wizard.

While the wizard is working, it posts progress updates a **Completing Commissioning** window.



When completed, the wizard reboots the host controller, and makes a **Close** button available.

CAUTION: 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.

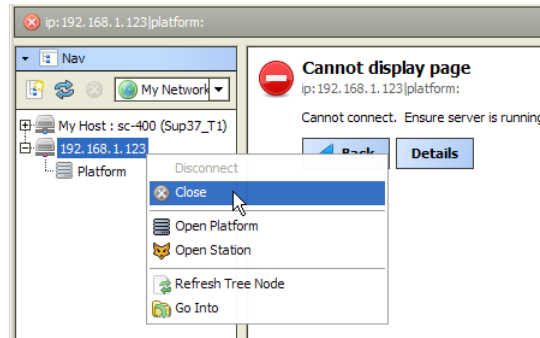
If applicable, possible automatic firmware upgrades” to any attached IO-16 or IO-34 modules (NDIO) may occur during this reboot. It is critical that such firmware upgrades complete without interruption—otherwise, IO modules could also be “bricked”.

IO firmware upgrades occur *before* the platform daemon starts. Therefore, it is safe to interrupt power anytime after you can re-open a platform connection to the controller.

Step 4 Click the **Close** button to exit the wizard.

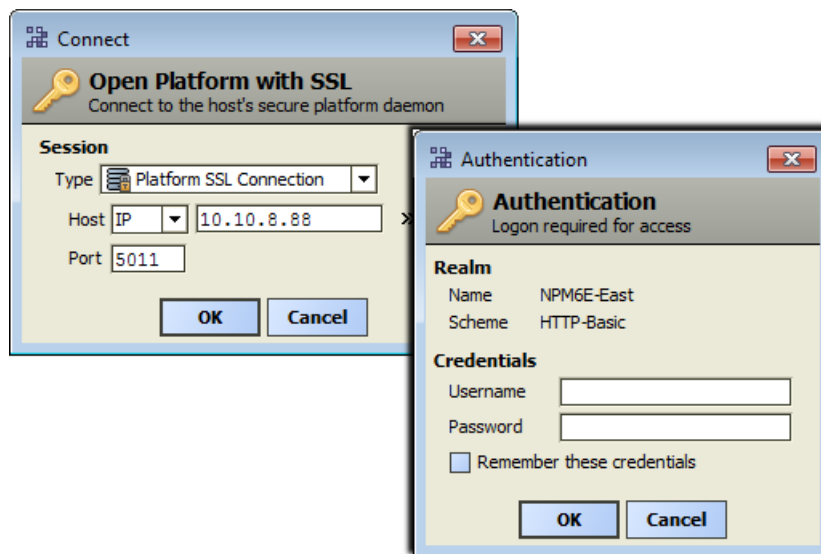
When the host reboots, your platform connection to it drops. Notice that in the Nav tree, the platform instance for that controller is dimmed .

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



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

NOTE: Going forward, you must access the host controller by its new (assigned) IP address. Your Workbench keeps a history of TCP/IP changes made.



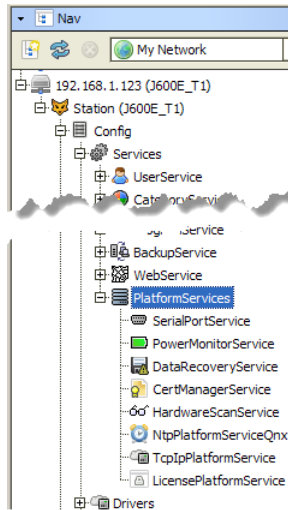
Also, you must use the credentials for the new platform user you created (to replace the factory-default platform user), or if you created additional platform users, credentials for one of them. If you changed your PC's IP address in order to commission the host controller, you usually need to reconfigure your PC's TCP/IP settings *back* to appropriate settings (now) to communicate with it. Otherwise, you will be unable to connect to it for other commissioning.

CHAPTER 4 ABOUT PLATFORM SERVICES

TOPICS COVERED IN THIS CHAPTER

Host commissioning services
Power monitoring configuration
Managing PlatformServices properties
Properties unique to the JACE-700
Enabling or disabling SRAM support
Configuring controller serial port
Performing platform administration
Modem configuration

Under its **Services** container, every station has a **PlatformServices** container. A few platform configuration items in a host are not directly accessible in a Workbench platform connection to a controller—that is, via the Commissioning Wizard or any of the platform views. Instead, you must have a station installed on the host (any station), and the station must be running.



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 host controller or a PC).
- It is built *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 `platform.bog` directly; always use PlatformServices' views.

Included services are a **TcpIpService** and **LicenseService**, which provide station (Fox) access to windows used in platform views, for instance the **TCP/IP Configuration** window. These services support installations where *all* configuration must be possible using only a browser connection (and not Workbench connected to the host's platform daemon).

Using Workbench, you open a station (Fox) connection to that station, and configure these platform-related items by accessing services under the station's **PlatformServices** container.

Host commissioning services

For any QNX-based host, the following child platform services in the station's PlatformServices are of chief importance when commissioning a new controller.

- **PowerMonitoringService** — Holds properties for configuration and status of the controller's battery monitoring and primary power monitoring, and power-fail shutdown.
- **DataRecoveryService** — For operation/monitoring of the ongoing SRAM backups for most (SRAM-equipped) controllers. It includes a **Service Enabled** *configuration* property, such that you can disable it, if needed. This is viable only if a backup battery is installed, or the unit is powered by an external UPS.
- **CertManagerService** — For management of PKI certificate stores and/or allowed host exceptions, used in certificate-based, secure TLS connections between the station/platform and other hosts. For details, see the *Station Security Guide*.
- **SerialPortService** — Holds properties for the status of serial ports. Typically, this platform service is important only if an older (JACE-403 or JACE-545) series platform, to access "Port Config" properties. In this case configuration may be needed because one or more ports may be "dual-duty", that is either RS-232 or RS-485.

Also, you may wish to review the parent container's **PlatformServices** properties and adjust, if needed. The following are two such examples.

- For any SRAM-equipped JACE-3,-6,-7 controller that is installed without any backup battery, you *must* adjust its **Battery Present** property from (the default) `true` to `false`.
- **PlatformServices** in JACE-700 (JACE-7 series) station includes properties for an onboard tamper switch CI.

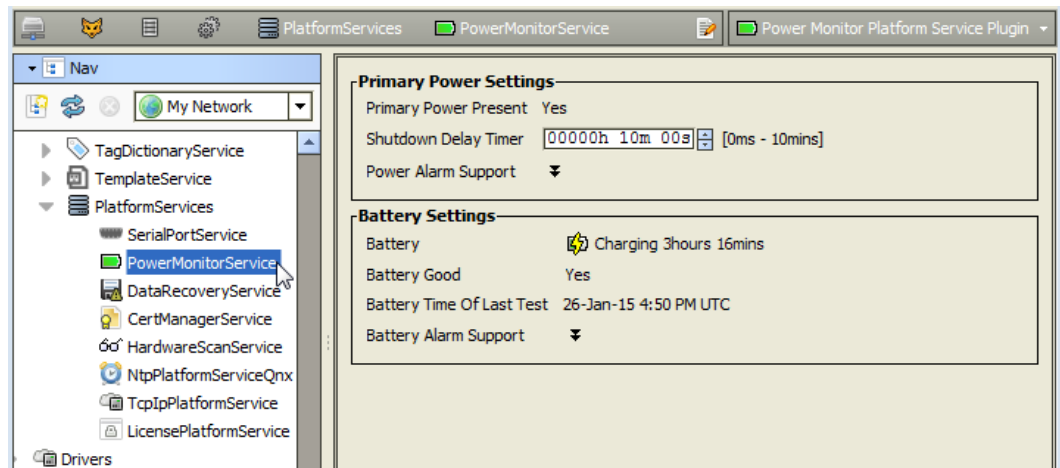
Power monitoring configuration

A host controller's power monitoring options may require adjustment from default settings. These properties define the controller's backup-battery monitoring and AC power-fail shutdown routines.

An NPM6E-based controller has on-board SRAM or SRAM option card, the **PowerMonitorService** under its station's **PlatformServices** offers several backup options.

For details on the **DataRecoveryService**, refer to the *Data Recovery Service Guide*.

To review and configure power monitoring options, expand the station's **PlatformServices** and double-click on the **PowerMonitorService**.

Figure 2. PowerMonitorService default view in JACE-6E station

- If you are commissioning a controller without installed SRAM, see the procedure “Configuring a controller with backup battery but no SRAM”.
- If you are commissioning any controller equipped with SRAM and a backup battery, see “Configuring a controller with SRAM and a backup battery”..

NOTE: For any SRAM-equipped controller that is installed without a battery, there is no power monitoring. Instead, see “Managing PlatformServices properties”.

- If you are commissioning JACE-7 series controller, a special **PowerMonitorService** applies, with several configuration options. Some of these relate to onboard contact inputs (CIs) intended to monitor normally-closed alarm contacts on an external UPS. This controller also supports (charges and monitors) an optional, external 12V sealed lead-acid battery. See “Configuring JACE-700” and also tamper switch CI details for a JACE-700.

Configuring a controller with backup battery but no SRAM

This procedure configures shutdown delay and battery alarms.

Prerequisites: A station in the controller is running and open in Workbench.

- Step 1 In the Nav tree, click **Services > PlatformServices**, and double-click **PowerMonitorService**.

The **Power Monitor Platform Service** view opens in the view pane.

- Step 2 As needed, change configuration properties, which include:

- **Shutdown Delay Timer**

Defines the period that the controller waits between detecting loss of AC power and performing a graceful shutdown (backs up database and powers board off). Depending on controller model, using either a nickel metal hydride (NiMH) battery or sealed lead-acid (SLA) battery, this varies:

- For JACE-6 models (NiMH), the default value is 30 seconds. The valid range is 0 to 60 seconds (1 minute), maximum.

NOTE: Unless you specifically need a longer shutdown delay, the default 30 seconds can be the best option, especially if you are experiencing multiple power outages that occur in quick succession. In this case, the NiMH battery may not become fully recharged, introducing a greater risk of the controller being unable to complete a graceful shutdown upon loss of power.

- For JACE-603 and JACE-645 models (Sla), the default period is 10 minutes, with a range is 0 to 15 minutes. Generally, for these models, the default value is recommended, as longer periods mean more time running on battery power. Otherwise, in some scenarios, with multiple lengthy power failures in succession, the battery may become completely discharged.
- **Power Alarm Support**
Expand this property (▼) to access additional properties that define how the station handles primary power alarms, including the alarm class to use and other alarm source information properties.
- **Battery Alarm Support**
Expand this property (▼) to access additional properties that define how the station handles battery alarms, including the alarm class to use and other alarm source information properties. Several settings reflect read-only status properties:
 - **Primary Power Present** — Boolean, displays Yes (true) if AC power is currently supplied to the controller.
 - **Battery** — container shows two values concatenated on a single line:
 - **State** — (with icon) is an enumerated descriptor, which is typically Idle if fully charged, else Charging, Discharging, or Unknown.
 - If this indicator displays Charging, it also displays the estimated remaining charge time until fully charged (Charge Time Left).
 - **Battery Good** — Boolean, displays Yes (true) if the last controller backup battery test was good.
 - **Battery Time of Last Test** - provides a timestamp (in AbsTime format) of the last battery test performed by the controller.

Step 3 Click **Save** to write the configuration to host platform (controller).

Configuring a controller with SRAM and a backup battery

This applies to any SRAM-equipped controller that also has a backup battery installed. Controller types are JACE-3E, JACE-6E, any other NPM6E-based type (JACE-603, JACE-645), or any other model with an SRAM option card. If the controller is installed without a battery, do not use this procedure. Instead, use the procedure “Managing PlatformServices properties”.

Prerequisites: The controller is licensed with the dataRecovery feature. A station in the controller is running and open in Workbench.

Step 1 In the Nav tree, click **Services > PlatformServices**, and double-click **PowerMonitorService**

The **Power Monitor Platform Service** view opens in the view pane.

Step 2 As needed, change configuration properties, which include:

- **Shutdown Delay Timer**

Defines the period that the controller waits between detecting loss of AC power and performing a *graceful shutdown* (backs up database and powers board off).

Depending on controller model, using either a nickel metal hydride (NiMH) battery or sealed lead-acid (SLA) battery, this varies.

- For models with a NiMH backup battery or SRAM option card, the default value is 10 minutes, with a valid range of:
 - 0 to 10 minutes, maximum— providing the **DataRecoveryService** is enabled, *else*:
 - 0 to 60 seconds (1 minute maximum) — if the **DataRecoveryService** is disabled or absent.

If the controller's **DataRecoveryService** (for SRAM support) is enabled and operating, and the NiMH battery is known to be good, the default (and maximum) Shutdown Delay value of 10 minutes is typically reasonable. This provides extra time for continuous operation during a power outage of up to 10 minutes.

The NiMH battery charge is monitored during this delay period, and if necessary, the system initiates a shutdown *before* this timer expires. Further, even if the battery had insufficient charge to complete a graceful shutdown, the **DataRecoveryService** would successfully restore the runtime station data from SRAM upon controller bootup (when power is restored).

- For models with a sealed lead-acid (SLA) battery, such as JACE-603 or JACE-645, the default period is 10 minutes, with a range from 0 to 15 minutes maximum.

Again, providing the SLA battery is known to be good and the station's **DataRecoveryService** is enabled and running, the default (maximum) shutdown delay of 15 minutes is typically reasonable, for reasons noted above.

In either case, the **Battery Present** property in the station's **PlatformServices** container must be set to `true` (the default).

Furthermore, if, at some point, you disable the station's **DataRecoveryService**, (either set its **Service Enabled** property to `false`, or uninstall its `plat-DataRecovery` module), it is recommended that you first set the **Shutdown Delay** no higher than the default of 30 seconds (NiMH) or 1 minute (SLA).

- **Battery Alarm Support**
- Expand this property (🔗) to access additional properties that define how the station handles battery alarms, including the alarm class to use and other alarm source information properties. Several settings reflect read-only status properties.
- **Power Alarm Support**
- Expand this property (🔗) to access additional properties that define how the station handles primary power alarms, including the alarm class to use and other alarm source information properties. Several settings reflect read-only status properties:
 - **Primary Power Present** — Boolean, displays `Yes` (true) if AC power is currently supplied to the controller.
 - **Battery** — container shows two values concatenated on a single line:
 - **State** — (with icon) is an enumerated descriptor, which is typically `Idle` if fully charged, else `Charging`, `Discharging`, or `Unknown`.
 - If this indicator displays `Charging`, it also displays the estimated remaining charge time until fully charged (`Charge Time Left`).
 - **Battery Good** — Boolean, displays `Yes` (true) if the last controller backup battery test was good.
 - **Battery Time of Last Test** - provides a timestamp (in `AbsTime` format) of the last battery test performed by the controller.

Step 3 Click **Save** to write the configuration to host platform.

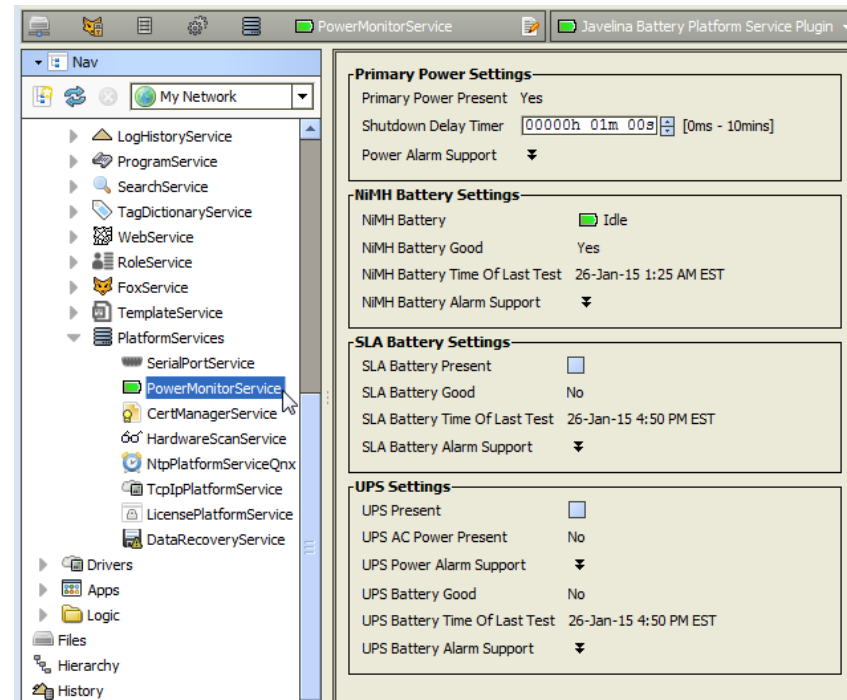
Configuring JACE-700

Prerequisites:

- The setup of the onboard tamper switch Contact Input (CI TMP) is at a different location.
- A station in the controller is running and open in Workbench.

Step 1 **Services > PlatformServices**, and double-click **PowerMonitorService**

The **Power Monitor Platform Service** view opens in the view pane.



Step 2 As needed, change configuration properties, which include:

- **Primary Power Settings**
 - **Shutdown Delay Timer**

Defines the period that the controller waits between detecting loss of AC power and performing a graceful shutdown (backs up database and powers board off).

NOTE: At shutdown the system also turns off 12V battery power wired to any external I/O modules. Depending on whether a sealed lead-acid (SLA) battery is connected, and also on the battery's capacity (as well as the loading factor of any attached remote I/O modules), the maximum recommended shutdown time can vary. Longer periods mean more time running on battery power. If no external SLA battery is present, a value from 30 seconds to 1 minute (the default) is recommended. If an external SLA battery is present, a time of one fourth or less than the total possible battery run time is conservative. Otherwise, in a scenario with successive multiple lengthy power failures, the SLA battery may become completely discharged.

- **Power Alarm Support**

- Expand this property to access additional properties that define how the station handles primary power alarms, including the alarm class to use and other alarm source information properties.
- **NIMH Battery Settings**
 - **Nimh Battery Alarm Support**
 - Expand this property to access additional properties that define how the station handles nimhBattery alarms, including the alarm class to use and other alarm source information properties. Such alarms apply to the onboard NiMH battery pack in the controller, which is always periodically tested.
- **SLA Battery Settings**
 - **Sla Battery Present**

Boolean (checkbox) specifies if an external SLA battery is connected. If set to `true` (checked), the controller supplies trickle charge voltage, and also periodically tests the battery. The default value is `false` for no SLA battery (checkbox cleared).
 - **Sla Battery Alarm Support**
 - Expand to this property to access additional properties that define how the station handles slaBattery alarms, including the alarm class and other alarm source information properties. If **Sla Battery Present** is set to `true` (checked), such alarms apply to the external 12V sealed lead-acid battery connected to (and trickle charged by) the controller.
- **UPS Settings**
 - **Ups Present**

Boolean (checkbox) specifies if one or two normally-closed (N.C.) alarm contacts are wired to onboard Contact Inputs (CIs) labeled **PWR** and **BAT** on the controller. The default value is `false` (checkbox cleared) for no monitoring.
 - **Ups Power Alarm Support**
 - Expand this property to access the additional properties that define how the station handles upsPower alarms (based on “open” at the controller’s onboard CI **PWR** (UPS PWR)), including alarm class and other alarm source information properties.
 - **Ups Battery Alarm Support**
 - Expand this property to access additional properties that define how the station handles upsBattery alarms (based on an “open” at the controller’s onboard CI **PWR** (UPS BATT)), including alarm class and other alarm source information properties. Several settings reflect read-only status properties, as follows:
 - **Primary Power Present** — Boolean, displays `Yes` (true) if 15Vdc power is currently supplied to the controller.
 - **NiMH Battery** — is a container for NiMH battery values concatenated on a single line:
 - **State** — (with icon) is an enumerated descriptor, which is typically `Idle` if fully charged, else `Charging`, `Discharging`, or `Unknown`.
 - If this indicator displays `Charging`, it also displays the estimated remaining charge time until fully charged (`Charge Time Left`).
 - **NiMH Battery Good** — Boolean, displays `Yes` (true) if last controller NiMH battery test was good.

- **NiMH Battery Time of Last Test**, provides a timestamp (in AbsTime format) of the last NiMH battery test performed by the controller.
- **SLA Battery Good** — Boolean, displays *Yes* (true) if the last controller test of the external SLA battery was good.
- **SLA Battery Time of Last Test**, provides a timestamp (in AbsTime format) of the last NiMH battery test performed by the controller.
- **UPS AC Power Present** — Boolean, displays *Yes* (true) if the controller's onboard CI PWR (UPS PWR) is closed.
- **UPS Battery Good** — Boolean, displays *Yes* (true) if the controller's onboard CI BAT (UPS BATT) is closed.
- **UPS Battery Time of Last Test** - provides a timestamp (in AbsTime format) of the last poll of all onboard contact inputs on the controller.

Step 3 Click **Save** to write the configuration to the controller.

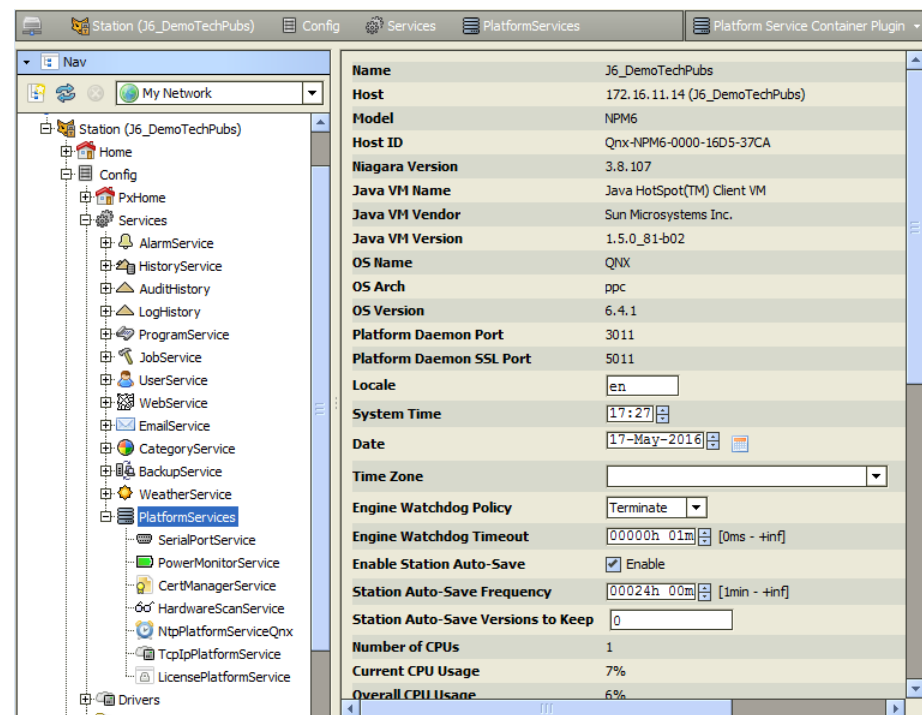
Managing PlatformServices properties

The properties in this topic apply in general to all controllers. Specific differences are noted.

Prerequisites: The controller is licensed with the **dataRecovery** feature. A station in the controller is running and open in Workbench.

Step 1 In the Nav tree, click **Services > PlatformServices**.

The **Platform Service** container view opens in the view pane.



Some properties are read-only status types, similar to many seen in the **Platform Administration** view. Other configuration properties are available. A group of three properties allows adjustment of the time, date, and time zone settings for the host controller (alternately accessible using a platform connection to the host). Access to these properties is useful if the installation requires all setup access using a browser only.

Step 2 Scroll down to the **Battery Present** property.

Hardware Revision	1.3	
Hardware Jumper Present	true	
Battery Present	<input checked="" type="radio"/> true <input type="radio"/> false	
Failure Reboot Limit	3 [1 - max]	
Failure Reboot Limit Period	000000h 10m [0ms - +inf]	
RAM Disk	Min Free	Size
	5 % [0 - 100]	32

By default, **Battery Present** is set to `true`. This is the proper setting for any controller, *unless*:

- The controller has SRAM and has *no backup battery* installed (NiMH and/or external 12V), and:
- The controller has the **DataRecoveryService** running and enabled (license includes a dataRecovery feature).

In this case only, set **Battery Present** to `false` and click **Save**. After the next reboot (required), this configuration property prevents battery bad nuisance alarms from occurring.

- Step 3 As needed, review other platform service configuration properties, which include the following:

NOTE: Leave these properties at their *default values*, unless otherwise directed by Systems Engineering.

- **Locale** — determines behavior that is specific to your geographical location, such as date and time formatting, and also which lexicon to use. The string you enter must use the form: language [“_” country [“_” variant]]

For example U.S. English is `en_US` and traditional Spanish would be `es_ES_Traditional`.

- **Engine Watchdog Policy** — defines the response taken by the platform daemon if it detects a station engine watchdog timeout. With the watchdog, the station periodically reports to the platform daemon its updated engine cycle count. The purpose of the watchdog is to detect and deal with a hung (stalled) station, and is automatically enabled when the station starts.

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 platform. If automatic start is enabled, the station restarts after the system reboots.
- **Engine Watchdog Timeout** — defaults to one (1) minute with a range of from 0 ms 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**.

- **Engine Station Auto-Save** — either enables (default) or disables the feature.

Allows for the automatic saving of a running station to the `config_backup<YYMMDD>_<HHMM>.bog` file at the frequency defined by the next property. Auto-saved backup files are kept under that station’s folder.

- **Station Auto-Save Frequency** — defaults to every 24 hours for any embedded controller with a range of from one (1) to many hours.
 - **Station Auto-Save Versions to Keep** — defaults to zero (0). Once the specified limit is reached, the oldest of the saved backups is replaced at the next manual save or auto-save backup. Significant flash space is saved by keeping this property set to 0 or perhaps 1.
 - **RAM Disk Size** — Specifies in MB the size of RAM disk used to store history and alarm files. where the default is 32 for JACE-3E, JACE-6 and JACE-6E series, or 48 for JACE-7 series.
-

For further details on these and other PlatformServices properties, refer to the *NiagaraAX Platform Guide*.

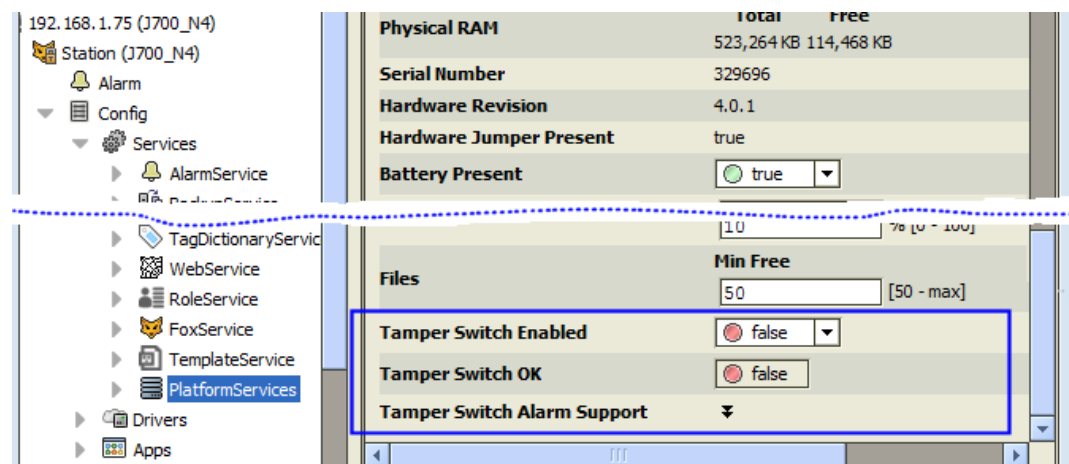
Step 4 To write any configuration change to the host controller, click **Save**.

Properties unique to the JACE-700

This controller includes properties for an onboard Contact Input (CI) intended for use with a nearby normally-closed (N.C.) tamper switch.

To see the three properties associated with this CI, In the Nav tree, click **Services > PlatformServices**, and scroll down to the bottom.

Figure 3. Tamper switch properties (for JACE-7 controller) at bottom of PlatformServices properties



The three properties related to this tamper switch CI are as follows:

- **Tamper Switch Enabled**
Default is `false`. If set to `true`, the onboard CI labeled **TMP** is polled once a second for a normally-closed (shorted) input. An open results in a `tamperSwitch` alarm from the default source `SystemService`.
- **Tamper Switch OK**
Read-only boolean that reflects tamper switch status as good (`true`) or bad (`false`). If the tamper switch is enabled, status is `true` while the **TMP** CI reads a closure (short), else `false` if the CI is open, which generates an alarm.
- **Tamper Switch Alarm Support**
- Expand this property to access additional properties to define how the station handles `tamperSwitch` alarms, including the alarm class and other alarm source information properties. Applies if **Tamper Switch Enabled** is `true`.

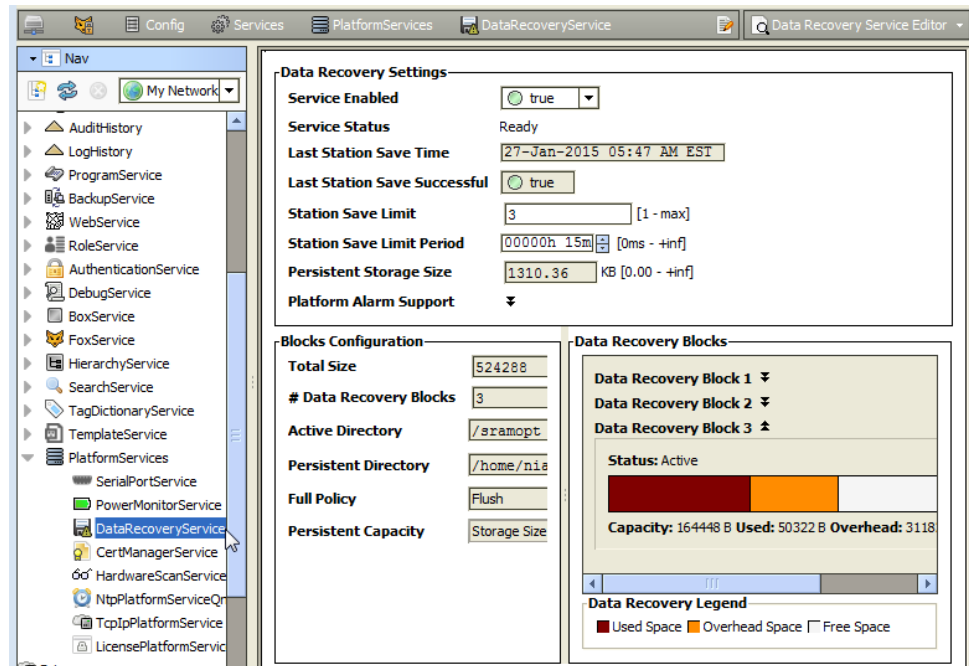
Enabling or disabling SRAM support

SRAM support is provided by the **DataRecoveryService**, a platform service that applies to SRAM-equipped controllers. This service has only a single configuration property: **Service Enabled**. The main use case for this property is for JACE-3E or NPM6E-based controller (JACE-6E, JACE-603, and JACE-645) *with an installed backup battery*, where you *do not* want it to use SRAM. This property setting is retained in any future controller upgrades.

Prerequisites: A station in the controller is running and open in Workbench.

- Step 1 In the Nav tree, click **Services > PlatformServices**, and double-click **DataRecoveryService**.

The **Data Recovery Service Editor** opens.



By default, the **Service Enabled** property is `true`. This is appropriate if the controller has no backup battery installed—for example, the JACE-3E and JACE-6E ship from the factory without a battery.

Step 2 Do one of the following:

- If the controller *has a backup battery* installed, you can optionally set this property to `false`, providing:
 - The **Battery Present** property in the station's **PlatformServices** container is set to `true`.
 - The backup battery is known to be good. If you disable SRAM support, it is recommended that you set the **PowerMonitorService**'s **Shutdown Delay** time to no higher than the default of one (1) minute.
- If a controller without a battery is powered from a battery-backed UPS, you could also choose to set **Service Enabled** to `false`.

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

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

You are prompted to reboot now to apply the changes.

Step 4 Click **Yes** to reboot with the change in the **DataRecoveryService** (disabled or enabled) made effective.

For more details, including scenarios where this configuration may be best, refer to the *Data Recovery Service Guide*.

Configuring controller serial port

Serial port configuration applies only to older platforms (JACE-403 and JACE-545), particularly if equipped with an onboard dialup modem module. More recent controller platforms have

pre-determined serial port configuration, including the "retrofit board" JACE-603 controllers. Dialup modem support was dropped in AX-3.7, such that port configuration for a controller running AX-3.7 should not include a "_modem" choice. An onboard modem module should be removed.

Prerequisites:

- A running station in the controller
- In Workbench, an open connection to that station

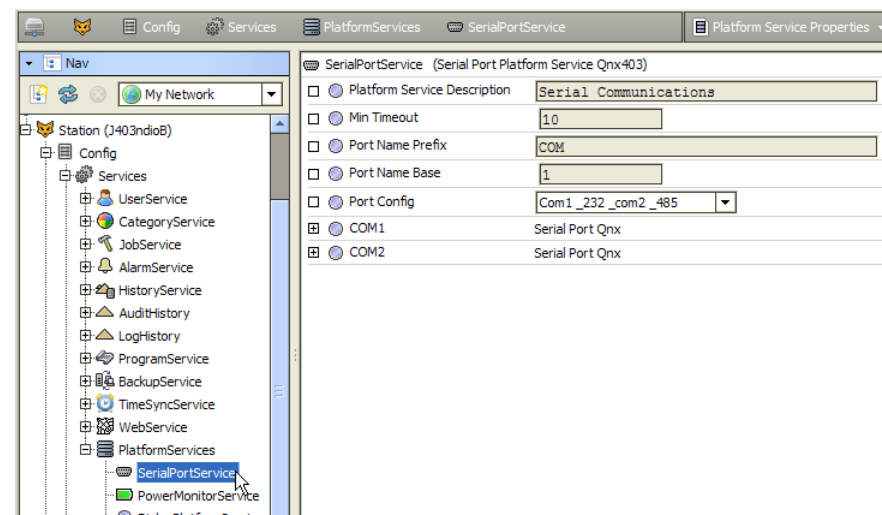
Perform the following steps:

- Step 1 In the Nav tree, expand the station and click **Services** > **PlatformServices** to reveal all contained services.
- Step 2 Double-click **SerialPortService**.
- Step 3 the **Port Config** property, click the drop-down list to select from a list of available choices.

Options in this list vary depending on the particular controller model being commissioned.

For example, if a JACE-403 the following choices are available:

- Com1_232_Com2_485 – Default configuration for a JACE-403 (only valid choice in AX-3.7 or later)
- Com1_232_Com2_modem – if JACE-403 is equipped with onboard dialup modem.
- Com1_485_Com2_modem – if JACE-403 is equipped with onboard dialup modem.



NOTE: For any controller running AX-3.7 or later, do not select either of the "_modem" options.

- Step 4 Click **Save** to write the configuration to host platform.

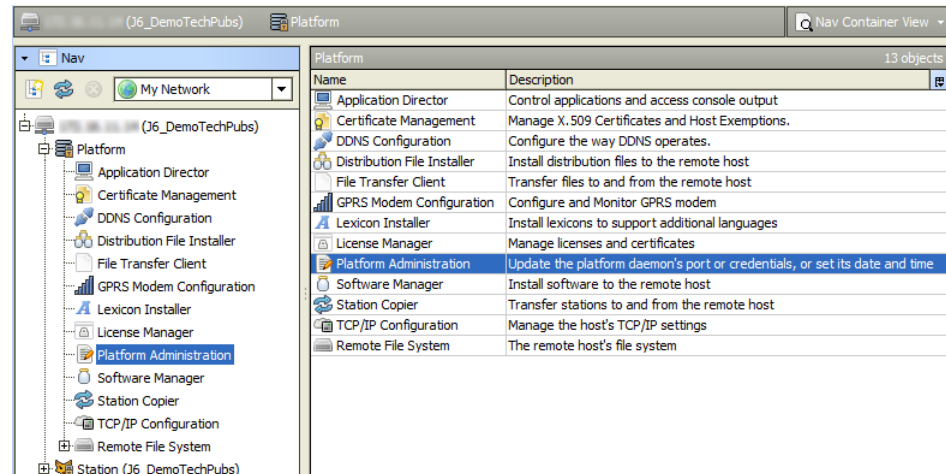
Performing platform administration

The Commissioning Wizard performs most, but sometimes not all, needed configuration for a new platform. There are several items you should review (and optionally change) in a follow-up platform connection to each host controller, using the **Platform Administration** view.

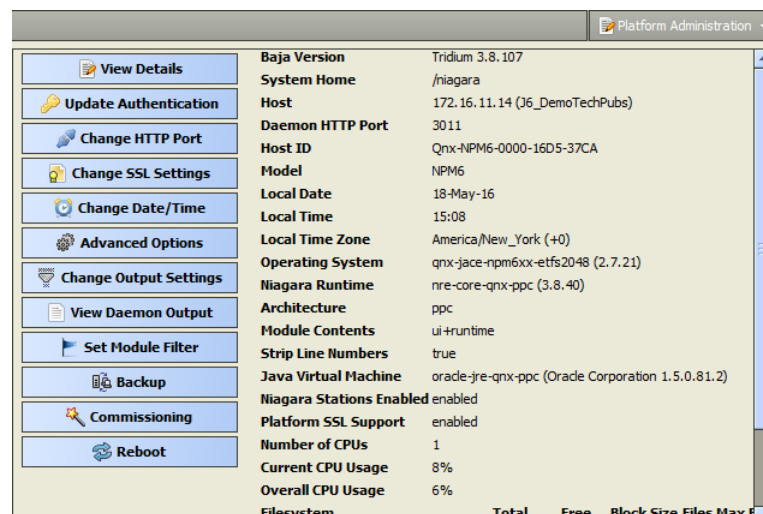
Prerequisites:

- The controller is already commissioned using the Commissioning Wizard.

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



Step 2 In the **Nav Container View**, double-click **Platform Administration**. The **Platform Administration** view opens.



This view is one of several views for any platform, listed under the platform in the Nav tree and in the platform's **Nav Container View**.

Step 3 Click any of the following to review or make changes:

- **View Details** — For a platform summary that you can copy to the Windows clipboard including its model number, OS level, JVM version, installed modules, lexicons, licenses, certificates, and so on.

- **Update Authentication** — For a platform daemon authentication window used to add, delete, or manage platform users (as previously available as step in the Commissioning Wizard).

NOTE: If using AX-3.8, see Platform credentials notes for AX-3.8.

- **Change HTTP Port** — For a window to change the HTTP port for the platform daemon (platform server) from port 3011 (the default) to some other port.
- **Change SSL Settings** — (Available only if the controller is licensed for SSL and has the necessary modules installed) For a window to specify platform SSL settings, including port to use, PKI certificate to authenticate by, and secure SSL protocol to use. The default port is 5011. Details are beyond the scope of this document. For complete information, refer to the *Station Security Guide*.
- **Change Date / Time** — For a window to change the current date, time, and time zone (as previously included as step in commissioning wizard). Typically, this is automatically handled by the Commissioning Wizard.
- **Advanced Options** — For a window that shows:
 - **FTP Enabled** — an enabled checkbox to temporarily enable FTP with the TCP/IP port number used .
 - **Telnet Enabled** — an enabled checkbox to temporarily enable Telnet with the TCP/IP port number used .
 - **Daemon Debug Enabled** — an enabled checkbox to temporarily enable the browser based daemon debugging tools.

CAUTION: Enabling any of the advanced options poses security risks. We strongly recommend you *keep access disabled*, unless otherwise directed by Systems Engineering. Upon completion of any use, such access should be disabled once again.

- **Change Output Settings** — Provides a window to change the log level of different processes that can appear in the platform daemon output.
- **View Daemon Output** — Provides a window to view platform daemon output in real time, and change logging levels. It includes the ability to pause and load.
- **Set Module Filter** — Provides a window to change the module content level of the JACE (a previously included as step in commissioning wizard).
- **Backup** — Makes a complete backup of all configuration on the connected host platform, including all station files, plus other configuration information (typically unnecessary for any controller that is just started up).
- **Commissioning** — Another way to re-launch the Commissioning Wizard, as previously used in the initial commissioning of the controller.
- **Reboot** — Reboots the controller, which restarts all software including the OS and JVM, the platform daemon, then if so configured in the Application Director (Station Director), the installed station. If you click this, a confirmation window opens.

If you reboot, your platform connection is lost, and it takes, typically, a few minutes until you can reconnect to the controller.

For more details, see the “Platform Administration” section in the *NiagaraAX Platform Guide*.

Modem configuration

In AX-3.7, dialup modem support ended (no longer any “Dialup Configuration” platform view).

However if the controller is equipped with a GPRS modem, you can use the controller’s **GPRS Modem Configuration** view to configure its settings. Details are beyond the scope of this document. See “GPRS Modem Configuration” in the *Platform Guide*, and for further details the Engineering Notes document *GPRS Modem Option*.

CHAPTER 5 RECOVERY TIPS

TOPICS COVERED IN THIS CHAPTER

Reviewing TCP/IP changes

System shell

About serial shell mode

During JACE 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. In this scenario, the following information can facilitate troubleshooting.

Reviewing TCP/IP changes

Workbench records before and after TCP/IP setting changes made from a platform connections in an `ipchanges.bog` file on your PC. If necessary, you can review these changes.

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

Child folders are named using the date and following this convention:

<yyyymmddhhmmss> for example, "d20170113153640 for 2017 Jan 13 3:36pm

Step 2 To expand any folder of interest, right-click and select **Views > > Property Sheet**).

The included decoded **modTime** value opens, for example, 13-Jan-2015 03:36 PM EST (vs "d20150113153640").

Underneath each folder are two objects:

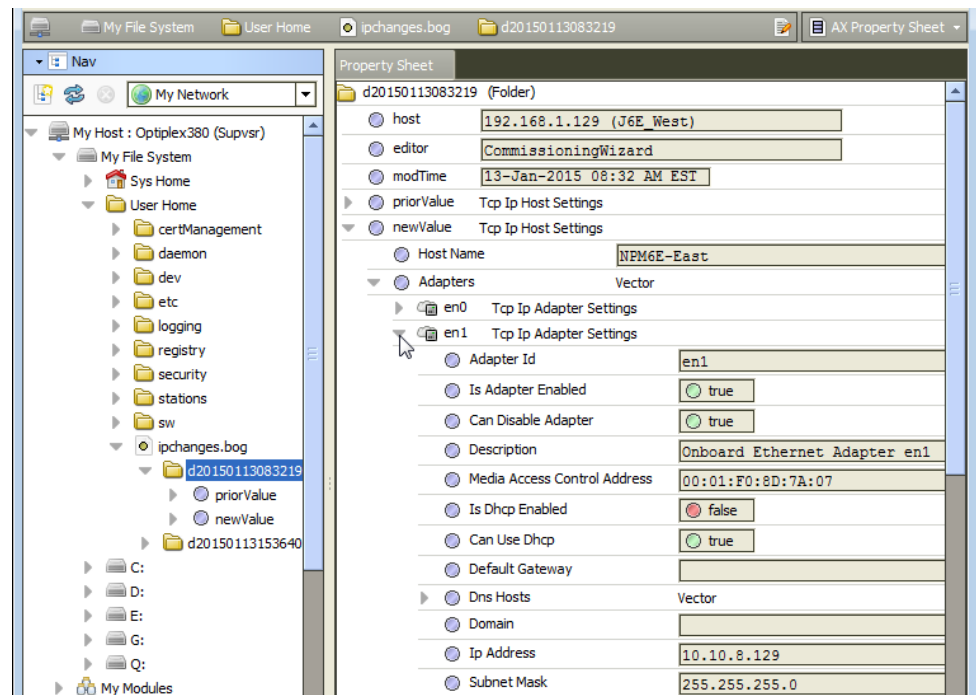
- **priorValue** — TCP/IP settings that existed before this change.
- **newValue** — TCP/IP settings that exist *after* this change.

Step 3 In the property sheet, expand a **priorValue** or **newValue** to see settings.

If you have a platform connection open (to any host), you can also review this same history of IP changes made from Workbench to remote platforms.

Step 4 To view the same `ipCHanges.bog` folder and all child change entry folders in a property sheet view, at the bottom of the **TCP/IP Configuration** view, click the **Audit** button.

The folder opens.



- Step 5 To see a decoded **modTime** value, expand a change folder , f
For example, 13-Jan-2015 03:36 PM EST (vs "d20150113153640").
- Step 6 To see the settings, expand a **priorValue** or **newValue** in the view.

System shell

Any QNX-based controller has a system shell that provides low-level access to a few basic platform settings. Using a special power-up mode, you can make a *serial connection* to the system shell via the onboard RS-232 port. The system shell is also available via SSH (provided that SSH is enabled in the controller).

Typical usage is for troubleshooting. However, in the case of IP address mis-configuration, you can use the *serial* system shell to regain access to the unit.

Also, depending on your preference, you may use the *serial shell* to set a controller's 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 (using Ethernet/IP) and perform all other software installation and platform configuration functions 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.

About system shell menu

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

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

CAUTION: Be careful when changing items from the system shell, in particular platform account (logon credentials) and network settings. If you change platform logon credentials and then lose or forget them, you can restore the factory default platform credentials—however, you will need to make a serial shell connection, reboot the controller, and then be careful to press a key at the appropriate time during boot up sequence.

Following, is an example of the main controller system shell menu.

Figure 4. JACE system shell menu (serial shell or Telnet access)

NPM6E System Shell

```

hostid: Qnx-NPM6E-0000-175F-91F7
serial number: 576465
build version: 4.0.23.2
build
date: built on 2015-01-16 19:31:47
system time: Tue Jan 27 19:22:45
UTC 2015
niagara daemon port: 3011
en0: inet 192.168.1.36
netmask 0xffffffff broadcast 192.168.1.255

inet6 fe80::201:f0ff:fe91:97a2%en0 prefixlen 64 scopeid 0x2
en1: <disabled>

```

1. Update System Time
2. Update Network Settings
3. Ping Host
4. Enable/Disable SSH/SFTP
5. Update Platform Account
6. Reboot

L. Logout

Enter choice:

To select a menu option, type the associated number (1 to 6) 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.

Update Network Settings

Use this menu option to access most of the same IP networking options as are available in the Commissioning Wizard step **TCP/IP configuration**. When selected, you are prompted for each setting sequentially, starting with hostname.

Update Network Settings example in a controller system shell

```
JACE Network Configuration Utility

Enter new value, '.' to clear the field or '<cr>' to keep existing value.

Hostname <localhost> : J8_East
Domain <> : myDomain.net
Primary DNS Server <> : 8.8.8.8
Secondary DNS Server <> : 8.8.4.4
Route <192.168.1.1> :
Primary IPv6 DNS Server <> :
Secondary IPv6 DNS Server <> :
IPv6 Route <> :

NET1 Ethernet interface (en0)
  IP address (clear to use DHCP) <> : 192.168.1.36
  Subnet mask <255.255.255.0> :
  Enable IPv6 addressing on this adapter? (Y/n) :
  IPv6 address (clear to use stateless autoconfiguration) <> :

Enable NET2 (en1) interface? (y/N) : Y
NET2 Ethernet interface
  IP address (clear to use DHCP) <> : 172.15.16.36
  Subnet mask <255.255.255.0> :
  Enable IPv6 addressing on this adapter? (Y/n) :
  IPv6 address (only 1 adapter may use IPv6 Autoconfiguration) <> :

**** IPv6 Autoconfiguration NOT supported on NET2 interface.
IPv6 on NET2 will be disabled.
```

```
Confirm new configuration

Hostname      : J8_East
Domain       : myDomain.net
Default Gateway : 192.168.1.1
Primary DNS   : 8.8.8.8
Secondary DNS : 8.8.4.4
Default IPv6 Gateway :
Primary IPv6 DNS :
Secondary IPv6 DNS :

NET1 settings:

IP Address      : 192.168.1.36
Subnet Mask     : 255.255.255.0
IPv6 Addressing assigned via Autoconfiguration

NET2 settings:

IP Address      : 172.15.16.36
Subnet Mask     : 255.255.255.0
IPv6 Addressing assigned via Autoconfiguration

Save these settings? (Y/n) :
```

NOTE: After you save the network settings, they do not become active until you reboot the controller. You can do this when you return to the main system shell menu, by selecting Reboot, menu option 6.

Update System Time

If the commissioning process has not been completed yet, it is often important to set the current date and time (YYYYMMDDHHMM.ss). For example: 201510231536 for 23-Oct-2015 at 3:36pm UTC or 11:36 EDT.

About serial shell mode

Any controller circuit board has a small 4-pin jumper connector, commonly called the mode jumper. To put the controller in serial shell mode, you put a two-pin jumper on certain

connector pins, and cycle power to the unit. Upon system boot, this makes the system shell available at the controller's primary RS-232 (COM1) port using pre-defined serial parameters of: 115200, 8, N, 1.

Using a serial terminal program such as PuTTY, you can then log on with platform credentials and access the system shell menu. After changing platform IP address parameters, a reboot command from the menu is necessary, and you remove (or reposition) the mode jumper. The controller reboots using the changed IP address parameters, and its COM1 port and otherwise operates as normally configured.

NOTE: If using COM1 for any other application, be sure to *move the 2-pin jumper* from the serial-shell position to the normal position before rebooting from the serial system shell.

Apart from physical access to the controller, you need the following items:

- A working RS-232 port on your PC
Usually this is a DB-9 connector with a specific Windows ComN assignment (say Com1 or Com2). However, newer notebook PCs may require a USB-to-RS-232 adapter, installed with a Windows driver.
 - Terminal emulation software, such as PuTTY (free open source application)
 - A serial cable to connect between your PC's serial ComN port to the controller's RS-232 port, plus any adapter, if necessary.
 - The JACE-3E and JACE-6E use a DB-9 connector.
Use a standard DB-9 to DB-9 null modem cable.
 - For controllers with RS-232 ports that use RJ-45 connectors, such as JACE-603 or JACE-645, the following parts, listed by Tridium part number, apply:
 - 10148 — Adapter, RJ-45 to DB-9, null modem type
 - 10181 — Silver satin RJ-45 patch cable, 10 ft. (connects adapter to RJ-45 type RS-232 port)
- Patch cables are also available in lengths 4 ft. (10180) and 25 ft. (10182)

NOTE: If sourcing your own RJ-45 to DB-9 adapter, refer to the *Mounting and Wiring Guide* of the appropriate controller for the pinouts used on the RS-232 port.

- A 2-pin jumper block for the controller's serial shell jumper pins—in most cases this should already be installed on the normal position pins.

Connecting to a serial system shell

The following procedure provides steps to use serial system shell. Examples are given based on the PuTTY program.

Prerequisites:

You have physical access to the controller and all needed items (cable, etc.).

CAUTION: In serial shell mode, normal COM1 port usage is overridden!

Perform the following steps:

- Step 1 Connect the necessary serial cable and adapter between the controller's RS-232 port and the RS-232 COM 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 > PuTTY**.
- Step 3 In the tree in the **PuTTY Configuration** window, expand **Connection** and click **Serial**.
- Step 4 Set the **Serial line to connect to** for your PC's RS232 COM port to use.
For example, COM1.
- Step 5 Set the **Configure the serial line** fields as follows:
- Speed (baud): 115200
 - Data bits: 8
 - Stop bits: 1
 - Parity: None
 - Flow control: None
- Step 6 In the tree of the **PuTTY Configuration** window, click **Session** and click to select the **Connection type** as **Serial**.

NOTE: (Optional) You can save this configuration to reuse (load) it in the future for PuTTY to controller serial sessions. To do this, type in a connection name in the **Saved Sessions** field (for example, JACE-S), and click **Save**. When you start PuTTY again to serially connect to the controller, select this name and click **Load**.

- Step 7 At the bottom of the **PuTTY Configuration** window, click **Open**.
- Step 8 On the controller, locate the 4-pin serial-shell connector and put a two-pin jumper on the appropriate pins. See the label on the controller to locate the mode or serial-shell connector pins.
- Step 9 With your terminal (PuTTY) session active, remove power from the controller, let it cycle down, then reapply power. After a few seconds, text should appear in your terminal software window similar to:

Press any key to stop auto-boot...

Do not press any key, wait for the login prompt.

NOTE: If you did press a key to stop auto-boot, select option 1 (Boot from on-board nand flash).

- Step 10 At the logon prompt, enter a platform user name, and at the password prompt, the platform password.
If the logon is successful, a prompt appears as:
- \$
- Step 11 At the \$ prompt, type: `syssh`
\$ `syssh`
The system shell-menu appears.
- Step 12 When finished making platform changes from the serial system shell, do the following:
- On the controller, move the two-pin jumper block back to the normal position.
 - From the system shell menu, select the **Reboot** option.

Type **y** at the `Are you sure you want to reboot [y/n]` prompt, and press **Enter**.

Shutdown-related text appears in the terminal (PuTTY) window, and the connection is dropped.

- Step 13 Click the **Close** control (upper right corner) in the terminal session (PuTTY) window. Click **OK** in the **PuTTY Exit Confirmation** popup window.

INDEX

B

battery alarm configuration.....31–32, 34

C

commissioning.....1
commissioning notes1
Commissioning Wizard.....11
configuring serial port.....41
connectivity.....5
contact input39
controller
 configuring power management31–32, 34
 connecting to.....6
 prepare to commission.....5
controllers.....iii
converting a controller8
core software
 install/upgrade.....20
credentials
 platform daemon3

H

http port3

I

IP address.....3

L

lexicons.....17
license
 install on PC or remote host13
 request from server13

M

models covered in this guideiii
modem configuration.....44
modules
 install/upgrade.....18

N

network settings47
 configure21
non-portable password.....8

O

overview.....1

P

PC requirements5
plat makeportable command.....8
platform administration42
platform connection
 opening6
platform credentials notes.....1
platform daemon credentials.....3
platform services29–30
platform user
 creating23
PlatformService properties.....36
power5
 monitoring.....30
power management
 configuring JACE-7 series controller34
 configuring with backup battery, no
 SRAM.....31
 configuring with SRAM32
profiles
 runtime15
PuTTY.....50

R

runtime profiles.....15

S

serial port
 configuring.....41
serial shell mode.....50
serial system shell50
shutdown delay31–32, 34
SRAM
 enabling and disabling39
station
 install from local computer.....15
system shell46
system shell menu46

T

tamper switch39
TCP/IP
 configure21
 reviewing changes45

U

upgrading stationsAX-3.8U1
to.....8

W

wizard
review changes..... 24