SOFTWARE INSTALLATION

JACE-NXT Niagara[AX] Install & Startup Guide

Information and/or specifications published here are current as of the date of publication of this document. Tridium, Inc. reserves the right to change or modify specifications without prior notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia. Products or features contained herein are covered by one or more U.S. or foreign patents. 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. Complete confidentiality, trademark, copyright and patent notifications can be found at: http://www.tridium.com/galleries/SignUp/Confidentiality.pdf © 2010 Tridium, Inc.

JACE, Niagara Framework, Niagara AX Framework and the Sedona Framework are trademarks of Tridium, Inc.

This document covers the initial NiagaraAX software configuration for a JACE-NXT with NiagaraAX. Instructions assume that you are an engineer, technician, or service person who is performing control system installation. This document is also in Workbench help, via the "docJaceNxtStartup" module.

- AX-3.5 or later (NiagaraAX build 3.5.33 or higher) is required by a JACE-NXT.
- For physical mounting and wiring details for any JACE controller, please see its specific hardware installation document. Also, this document does not cover station configuration or NiagaraAX components. For details on these topics, refer to NiagaraAX online help and the NiagaraAX User Guide.

The following main sections are in this document:

- "Overview" on page 1-1
- "JACE-NXT Windows notes" on page 1-2
- "Preparation" on page 1-3
- "Connect to the JACE-NXT" on page 1-4
- "Run the Commissioning Wizard" on page 1-5
- "Additional JACE-NXT platform configuration" on page 1-17
- "JACE-NXT platform services" on page 1-20
  - "Hardware monitoring JACE-NXT configuration" on page 1-21
  - "Power monitoring JACE-NXT configuration" on page 1-22
- "Modem configuration" on page 1-25
- "Recovery tips" on page 1-25
- "JACE-NXT Windows XPE security" on page 1-26
- "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31
- "Document Change Log" on page 1-34

Overview

As shipped from the factory, a JACE-NXT with NiagaraAX has Windows XP Embedded pre-installed, but only the bare minimum of software to run the Niagara platform daemon (niagarad). It does *not contain* the Sun Java VM, Niagara runtime environment or software modules, lexicons, license, certificate, stations, and so on.

To install this software, you must use Workbench to open a platform connection to the JACE-NXT and install Niagara distribution files, software modules, license(s), and do other platform configuration. Some important related tasks include setting the JACE's:

- IP network address, and related IP networking parameters
- Platform daemon credentials (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. As described ahead, the most straightforward way is to use the **`Commissioning Wizard`**.

Note: *Starting in AX-3.5, the Commissioning Wizard is the* only way to install the needed core software *in a JACE. It is no longer possible to "inadvertently install" core software from the Software Manager, Station Copier, or Distribution File Installer (this could cause re-connection issues). Moreover, steps in the wizard were reordered, along with other changes.*

Note that most steps in the Commissioning Wizard remain 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 JACE. See the "Niagara platform" section in the Platform Guide.

However, always use the Commissioning Wizard to commission a new JACE, as well as to upgrade any JACE from one point release to the next—and make sure a license file is available for that release! Also, if commissioning a new CompactFlash based JACE-NXT, see *"Flash-based unit preparation" on page 1-4.*

JACE-NXT factory-shipped state

The following default settings are in effect for a factory-shipped JACE-NXT:

- IP address
- HTTP port for platform access
- Platform daemon credentials

Note: *As factory-shipped on any JACE-NXT, the default Windows Firewall settings may also require adjustment, depending on its intended Niagara configuration. These topics are briefly covered in this document. For related details, see the section* *"JACE-NXT Windows XPE security" on page 1-26.*

JACE-NXT factory IP address

When shipped, a new JACE-NXT controller with NiagaraAX has the following TCP/IP settings for its two Ethernet ports:

- Primary (*left*) port 1: `192.168.1.19`*n* (static IP) with subnet mask: `255.255.255.0` where the last numeral (*n*) matches the last numeral in the JACE's *serial number*
- Secondary (*right*) port 2: enabled for DHCP in the Windows OS.
  Note: *Typical usage of the secondary port is for isolating a "driver's" Ethernet traffic from the primary port. Or, only for occasional use by a directly-attached service notebook to access the unit.*

The primary factory-assigned IP address should also be listed on the packing slip that accompanied the JACE. You change these IP network settings during your startup commissioning of the JACE.

JACE-NXT factory HTTP port for platform access

When shipped, the JACE's platform daemon is configured to listen on HTTP port 3011. Often, this is left at default. However, if a *different* port is needed for a platform connection (perhaps for firewall reasons), you can change this during the commissioning of the JACE.

Note: *If changing from the default port (3011) for the platform daemon, you will also need to change the corresponding Windows Firewall exception (named "admin") on the JACE-NXT, in order to allow access. For related details, see* *"Change HTTP Port" on page 1-19.*

JACE-NXT factory platform daemon credentials

A JACE-NXT controller is shipped using "basic platform authentication," meaning by native Windows OS user accounts, with a default Windows administrator user with credentials:

Username: `tridium` Password: `niagara`

Note: *Password is case-sensitive, however, a Windows username is not.*

Initially, you use these default credentials to open (login) a platform connection to the JACE. Like the factory-assigned IP address, default credentials are intended to be *temporary*. During your startup configuration, you should change these credentials to be something unique, and *guard them closely*.

Note: *You can also add additional Windows users, assign/modify privileges, or change Niagara platform access to use "digest authentication" (a single non-Windows user, as for any QNX-based JACE).*

JACE-NXT Windows notes

Any JACE-NXT uses Windows XP Embedded (XPE), pre-installed as the operating system. No Windows CD is included. However, a Windows "Certificate of Authenticity" sticker is affixed near the model number label. When ordered with NiagaraAX, the OS is installed differently, depending on model:

- NXT-AX-FL model: 2GB CompactFlash. This flash drive has 3 partitions:
  - C: System (996MB) — has the Windows OS
  - D: Niagara (800MB) — with NiagaraAX release folder, subfolders for station database and graphic files
  - History (156MB) — for the station's NiagaraAX history space.

  Note: *A flash-based JACE-NXT uses an EWF overlay filter, which affects commissioning and maintenance. For details see* *"Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.*
- NXT-AX-HD model: 250GB hard drive, as an alternative to the CompactFlash-based model.

Windows XP Embedded on either JACE-NXT model supports a "local desktop environment," meaning the attachment of a (USB) keyboard, (USB) mouse, and (DVI-I capable) monitor.

Note: *Although a local console is supported, the usual method to apply Windows updates (and/or make changes in Windows security) is to access the JACE-NXT via a "**`Remote Desktop Connection`**", using Microsoft's "Remote Desktop" client software. This is usually installed on any PC with Windows XP or later.*

On any JACE-NXT, Windows XP Embedded requires periodic updates to ensure proper security. This can apply even to a new unit. See "JACE-NXT Windows XPE security" on page 1-26 for more details.

Preparation

At least two areas of preparation are required before proceeding:

- Provide power and connectivity
- Niagara and PC Requirements
- Flash-based unit preparation (applies only if a new CompactFlash-based JACE-NXT)

Provide power and connectivity

Invariably, you perform the initial Niagara software installation and startup of a JACE (as described in this document) *in your office*, before physically mounting it in place at a job site. Please refer to *JACE-NXT Mounting & Wiring Guide* for details on making (temporary) power wiring and Ethernet wiring connections.

The remainder of this document assumes that you have the JACE 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 JACE 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 NiagaraAX Workbench (AX-3.5 or later) installed with the "installation tool" option. That option copies distribution files needed for commissioning various models of JACE controllers. This PC is referred to as "your PC."

Note: *AX-3.5 or later (NiagaraAX build 3.5.33 or higher) is required for the JACE-NXT. Your PC must meet minimum hardware/operating system requirements for a Workbench workstation. This includes a working Ethernet adapter with TCP/IP support (browser capable). An Ethernet TCP/IP connection to the JACE is required to install Niagara software and establish other parameters.*

For this initial Ethernet connection, you can use either:

- An Ethernet patch cable connected directly between your PC and the JACE (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 JACE are physically connected to the same Ethernet hub or switch.

To prepare for new JACE-NXT commissioning

To prepare for new JACE-NXT commissioning, do the following steps:

Step 1 If not already installed, install the NiagaraAX software on your PC, including its permanent license.

Step 2 Typically, the license file for the JACE 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 JACE, and you wish to use it instead of the online license server (for some reason, for example your Workbench PC will not have Internet connectivity when you are commissioning the JACE), make the file available to Workbench first, as follows:*

- Copy the file to your `!licenses/inbox` folder, then restart Workbench. For more details, refer to the section "Local license inbox" in the Platform Guide.

Step 3 Attach one end of a standard category-5e Ethernet unshielded twisted pair (UTP) patch cable to the left RJ-45 Ethernet connector (**`Ethernet 1`**) on the JACE-NXT.

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 JACE.

Step 6 Record you PC's current IP settings, then re-assign your PC's IP address for its Ethernet LAN adapter (if necessary, refer to Windows online Help for information about configuring TCP/IP settings).

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

Set the IP address in the range: `192.168.1.11` to `192.168.1.181`

with a subnet mask of: `255.255.255.0`

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

Step 7 From your PC, start Workbench. The Nav tree should be visible in the side bar area (left pane). If not, from the menu bar, select **`Window > Side Bars > Nav`**.

Flash-based unit preparation

If a new CompactFlash-based JACE-NXT, it is recommended that you first *disable EWF* (enhanced write filter) for the "System" drive C partition, followed by a reboot, *before* starting commissioning. Do this with a Windows remote desktop connection to the unit, by selecting from the Windows Start menu:

`Start > AllPrograms > ewf > Commit changes to C drive and leave unprotected`

And then rebooting the unit before running the Commissioning Wizard. Following all commissioning, you must *then re-enable protection on drive* **`C`**. For related details, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31 and "EWF use case examples" on page 1-33.

Connect to the JACE-NXT

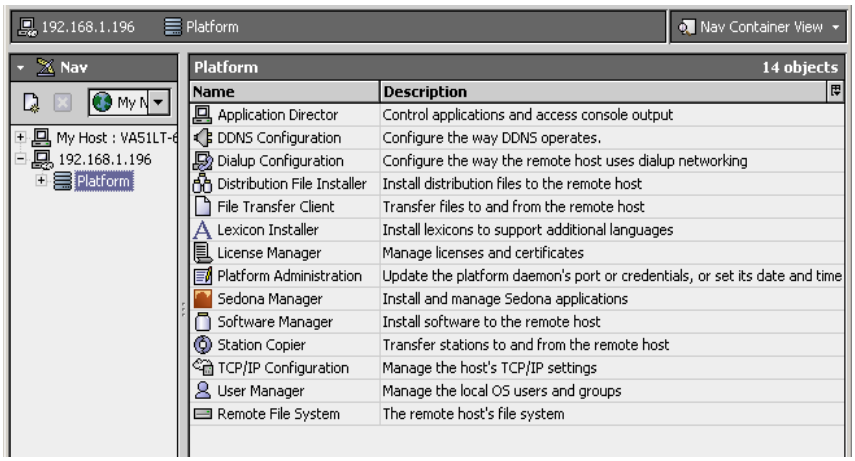
Once the JACE-NXT has powered up, connect to it with Workbench using "Open Platform." A platform connection to any JACE is required for *most host-level operations*. This includes installing NiagaraAX core software and modules, establishing network and TCP/IP settings, and other platform tasks.

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

- Open a platform connection
- Start the Commissioning Wizard

Open a platform connection

Figure 1 *Opened JACE-NXT platform*



To open a platform connection to a JACE-NXT

To open a platform connection from Workbench to the JACE-NXT, do the following:

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

The **`Open Platform`** dialog box appears.

Step 2 Complete the fields in the **`Open Platform`** dialog box as follows:

- Host — Leave at default **`IP`**, and type in the default IP address of the new JACE.
- Port — Leave at default 3011.
- Credentials (see "JACE-NXT factory platform daemon credentials" on page 1-2), which include:
  - Username — Type in default username: `tridium`
  - Password — Type in default password: `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 (Figure 1).

Note: *After you commission a JACE and it reboots, in future platform sessions you will need to 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 JACE's factory-assigned IP address, you will first need to reconfigure your PC to the appropriate TCP/IP settings (to communicate to the now-commissioned JACE).*

Run the Commissioning Wizard

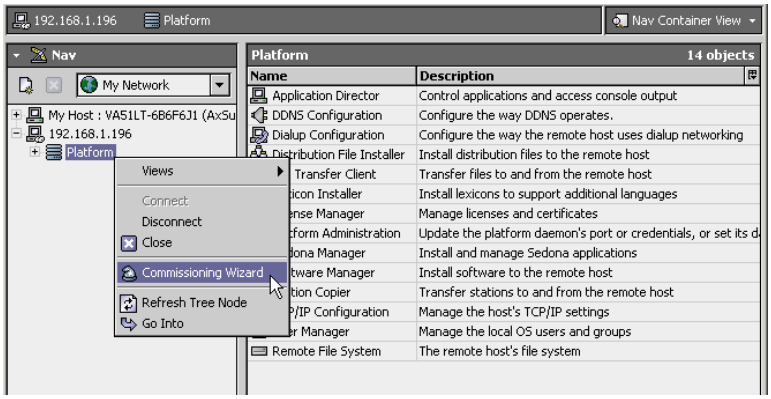
The following sections describe using the Commissioning Wizard for a new JACE-NXT:

- About the Commissioning Wizard
- Start the Commissioning Wizard
  - Set module content filter level
  - Install/upgrade core software
  - Station installation
  - Select modules
  - TCP/IP configuration
  - Platform daemon authentication
  - Install lexicons
  - Install license
  - Review and finish wizard

About the Commissioning Wizard

As shown in Figure 2, the Commissioning Wizard is a right-click option on any connected platform in the Nav tree. You can also launch the wizard from the Platform Adminstration view.

Figure 2 *Commissioning Wizard as right-click platform option*



Use this wizard when installing a *new JACE*, as it provides a "checklist" method to perform essential (and often "one time") platform tasks. Also use this wizard whenever you *upgrade* the core software in a JACE, at some future time. See "Upgrading a JACE" in the *Platform Guide*.

Note: *Starting in Workbench AX-3.5, significant changes were made in the platform Commissioning Wizard. For a summary of these changes, see the next section "Important Commissioning Wizard notes".*

Important Commissioning Wizard notes

- If you were familiar with the Commissioning Wizard in Workbench AX-3.4 and earlier, note these changes starting in AX-3.5:
  - Steps were reordered. For example, the license step "Request or install software licenses" is now *first*. This helps prevent the scenario of installing core software above the supported version in the JACE's license, where as a result the station cannot start. Now, the wizard cannot complete (and start execution) unless the license in the JACE is at the required version.
  - The wizard no longer performs core software (dist file) installation first, separately, where after the JACE reboots and remaining steps execute in a second sequence, ending in another reboot. Now, all wizard steps execute in a single sequence, meaning that the JACE reboots only *once*.
- Throughout the wizard's dialogs, use the buttons **`Back`** and **`Next`**, as needed, to retrace (or skip) steps. 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.

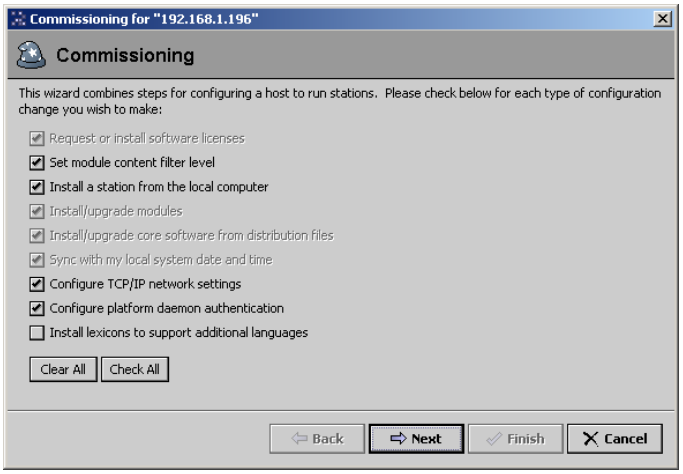
Start the Commissioning Wizard

To start the Commissioning Wizard

From Workbench with the JACE platform open, to start the Commissioning Wizard do the following:

Step 1 In the Nav tree, right-click on Platform and select **`Commissioning Wizard`**.
The dialog box **`Commissioning for "<IP address>"`** appears (Figure 3).

Figure 3 *Commissioning Wizard (default selections shown)*



By default, all steps are preselected except lexicon installation (for language support). Steps are executed in the order listed in the wizard.

Commissioning steps include:

- Request or install software licenses — Preselected for any new JACE.
- Set module content filter level — Recommended.
- Install a station from the local computer — Recommended.
- Install/upgrade modules — (always preselected, whenever wizard is run).
- Install/upgrade core software from distribution files — Preselected for any new JACE.
- Sync with my local system date and time — Preselected in most cases (new JACE for example).
- Configure TCP/IP network settings — Recommended.
- Configure platform daemon authentication method — Recommended.
- Install lexicons to support additional languages — Recommended for non-English language support.

Step 2 As needed, click to include or omit steps.

For a new JACE, you typically *accept all default selections*, plus if not already selected, add (check) "Sync with my local system date and time."

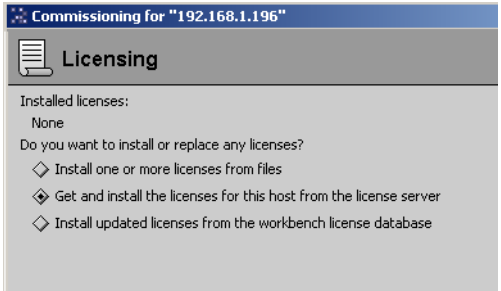
Step 3 Click the **`Next`** button to continue. With wizard selection defaults, this is "Install license".

Install license

To automatically install or update licenses

At the License step (Figure 4) in the Commissioning Wizard, you install one or more license files in a new JACE. You typically select the option to get and install licenses from the licensing server.

Figure 4 *License dialog (select method)*



Note: *At least one license file specific to any JACE is stored on the licensing server. Providing you have Internet connectivity, this is the recommended method to install or update a license. See "About the Licensing Server" on page 1-8 for more details.*

A minimum of one license file is always needed. Typically, other license files 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 "Get and Install the licenses for the host from the license server."

Step 2 Workbench silently searches the licensing server, locates the license(s), and the wizard advances to the next step. See "Set module content filter level" on page 1-8.

Note: *If the "license server" option shown above does not appear, Workbench has not detected Internet connectivity, and so cannot contact the licensing server. In this case, you can either:*

- If you already have a license for this JACE in your "local license database," select the *last* option shown in Figure 4, to install from your "workbench license database." Workbench locates the license, and the wizard advances to the next step. See "Set module content filter level" on page 1-8. This option will be missing if your local license database does not include a license for this JACE.
- If you have the JACE license file(s), use the next procedure "To install or update licenses from files". If necessary, you can also install license(s) later, either from your local license database or from license files.

To install or update licenses from files

Step 1 At the License step, select "Install one or more licenses from files".

Step 2 Click the **`Next`** button.

The "Choose license files to install" step appears (Figure 5).

Step 3 Click the **`Add`** button.

A "Select File" dialog appears (Figure 5). By default, the contents of your `licenses` subfolder is listed (showing your Workbench license). If you previously pointed Workbench to another location, license files in that location are listed instead.

- If you see the license you need, click it to *highlight* it. If other licenses are also needed, you can select multiples by holding down 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 *highlight* it.

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

Step 4 Click the **`OK`** button.

The "Choose license files to install" dialog appears (Figure 6) with the selected license(s).

Step 5 If necessary, click the **`Add`** button again (step 3) to add additional license files.

Step 6 When all needed licenses are listed in the "Choose license files" dialog, click the **`Next`** button to go to the last (review) dialog in the Commissioning Wizard.

Figure 5 *License dialog (choose files)*

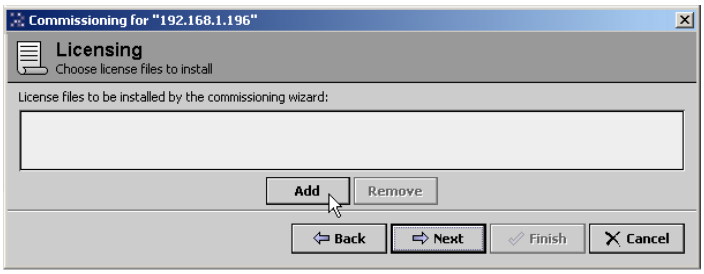


Figure 6 *Select Files dialog from Add in Licensing*

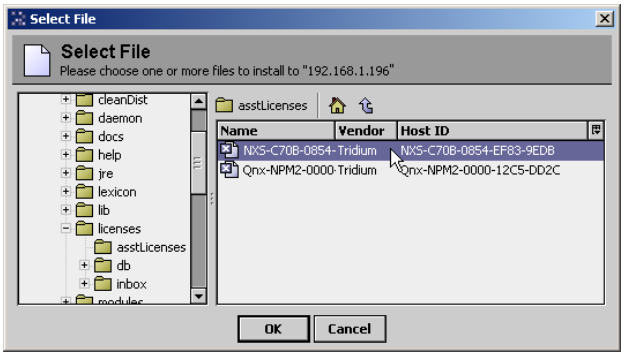
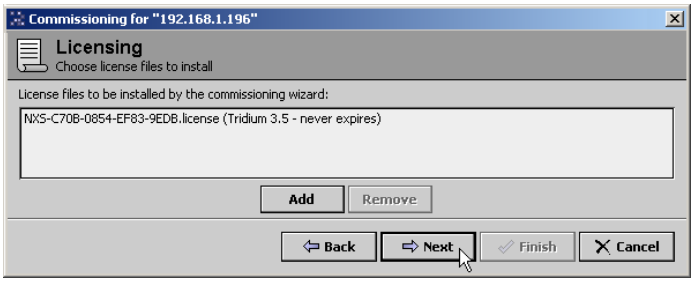


Figure 7 *License dialog with file selected*



About the Licensing Server

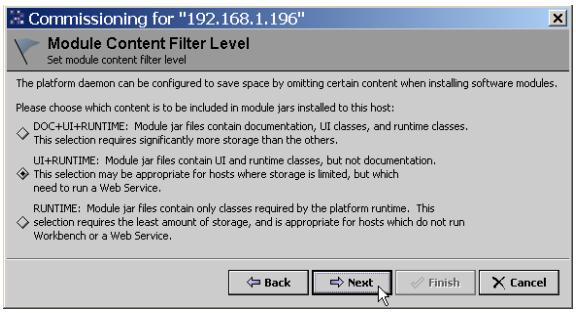
For license files validated against the Tridium certificate, installation can be automated from Workbench. All such purchased licenses (including JACE, Supervisor, or Workstation-only) are stored and available to Workbench through the licensing server.

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

Set module content filter level

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

Figure 8 *Module Content Filter Level*



To specify the module content filter level

At the Module Content Filter Level step (Figure 8) in the Commissioning Wizard, do the following:

Step 1 Click the desired level of content in Niagara modules to be installed in this JACE.

Module content level is *one* of the following:

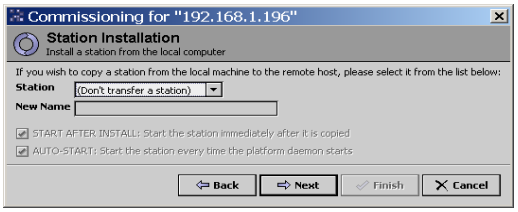
- DOC+UI+RUNTIME — Typically *not appropriate* for a JACE-NXT (unless a hard drive model).
- UI+RUNTIME — Appropriate for *most* JACE-NXT installations, to provide the Web Service.
- RUNTIME — Not typically chosen for any JACE-NXT, even if *not* running the Web Service.

Step 2 Click the **`Next`** button for the next step, which is typically "Station installation".

Station installation

If you have a specific station database ready to install in the JACE, you can specify it at this step in the wizard. Or, simply accept the default "(Don't transfer a station)" and click **`Next`**. (You can create a station later using the New Station Wizard, and install it using the platform's **`Station Copier`**.)

Figure 9 *Station Installation dialog (default)*



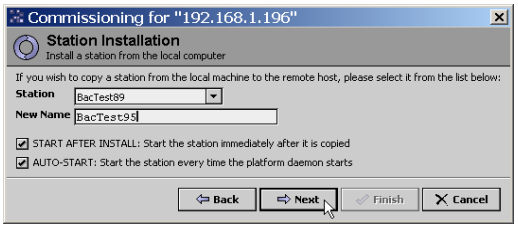
To specify a station database to install

At the Station Installation step (Figure 9) in the Commissioning Wizard, do the following:

Step 1 Click the Station drop-down control and click the name of a station database on your PC.

Listed are station subfolders under your PC's local Niagara stations folder.

Figure 10 *Station Installation dialog (station selected)*

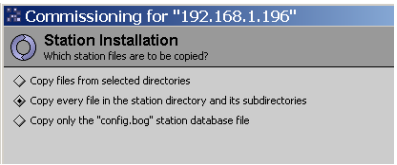


Step 2 If you select a station, the following additional selections are available (Figure 10):

- New Name — Either leave at same station name as local copy, or type in a new station name.
- START AFTER INSTALL — If enabled, the station starts after the commissioning completes.
- AUTO-START — If enabled, the station starts every time the JACE is rebooted.

Step 3 Click the **`Next`** button to continue.

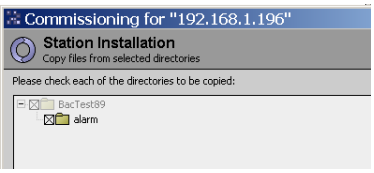
Figure 11 *Station Installation dialog (copy options)*



A dialog asks which station files to copy (Figure 11), where you can select *one* of the following:

- Copy files from selected directories — Allows you to specify which subfolders under that local station that are copied. It produces a "tree" selection dialog (Figure 12) upon **`Next`** button.

Figure 12 *Station Installation dialog (select subfolders)*



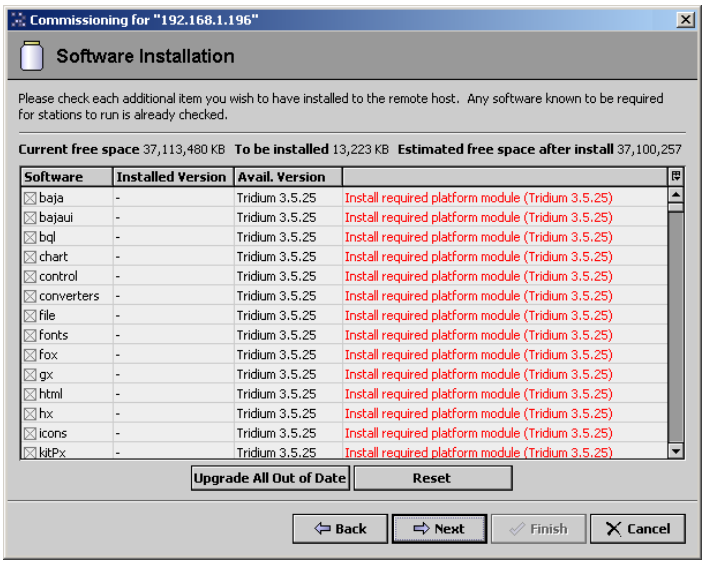
  - If you choose this, click folder controls to expand and contract as needed.
  - Selected folders appear with an "X" and unselected folders show an empty folder box.
- Copy every file in the station directory and its subdirectory — The default, most typically used.
- Copy only the "config.bog" station database file — Copies only the station configuration (components), and not any supporting folders/files like px files, html files, and so forth.

Step 4 Click the **`Next`** button for the next step, "Select modules".

Select modules

At the select modules step, a popup "Rebuilding software list" dialog briefly appears as the dependencies of the JACE are compared against the available software modules in your Workbench PC's "software database." During commissioning, you add to the software modules that are preselected for installation. Often, you do not make any changes, as the wizard preselects all necessary "core" modules, plus any additional modules needed by the station you previously selected (see "Station installation" on page 1-9).

Figure 13 *Module installation dialog (default)*



However, if you did not previously select a station to install, you may wish to select modules to support a station you have in mind. Or, you may know that the JACE will need a module in the future (say for a driver), and you wish to install it now.

Note: *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 will automatically prompt for confirmation to install any additional modules deemed necessary.*

To select modules

At the Module Installation step (Figure 13) in the Commissioning Wizard, do the following:

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.

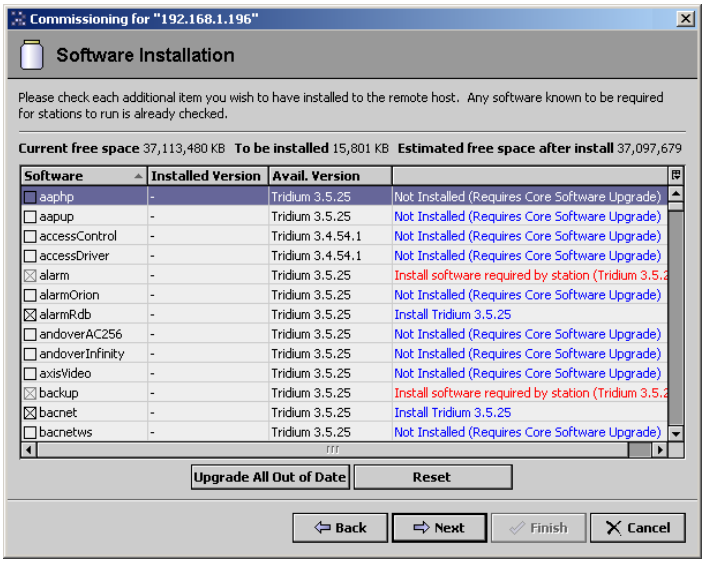
Note the following:

- Modules preselected from "core" need or station database reasons each have a *red text* descriptor, which may read as:
  - Install required platform module "Tridium *buildNumber*"
  - Install module required by station "Tridium *buildNumber*"

  By default, these modules are at the top of the list. You cannot deselect these modules.
- You can select *additional* modules to install by clicking selection boxes. The description for each is in *blue text*, and displays as either:
  - Not Installed (if not selected)
  - Install "Tridium *buildNumber*" (if selected)
- To resort 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.

Figure 14 shows the dialog after modules have been selected and the list resorted alphabetically.

Figure 14 *Module installation dialog (scrolling and selecting modules)*



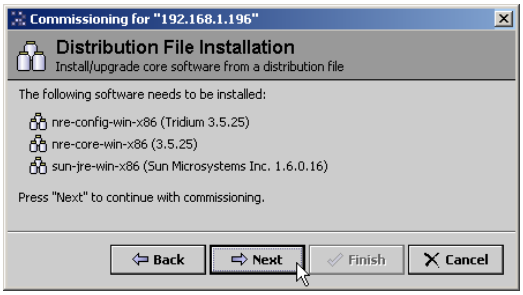
Step 2 Click the **`Next`** button to go to the next step. Typically, this is "Install/upgrade core software".

Install/upgrade core software

At the install/upgrade core software step, the dependencies of the JACE platform are compared against the distribution (dist) files available in your Workbench PC's "software database." The wizard determines what dist file(s) need to be selected for installation, and then informs you in a dialog (Figure 15).

Note: *For related details, see the section "About your software database" in the* Platform Guide.

Figure 15 *Distribution File Installation (beginning)*



To select the distribution files

To select the distribution files for installation, do the following:

Step 1 Click **Next** to select the distribution files.

The next commissioning step appears. Using wizard defaults, this is "TCP/IP configuration".

TCP/IP configuration

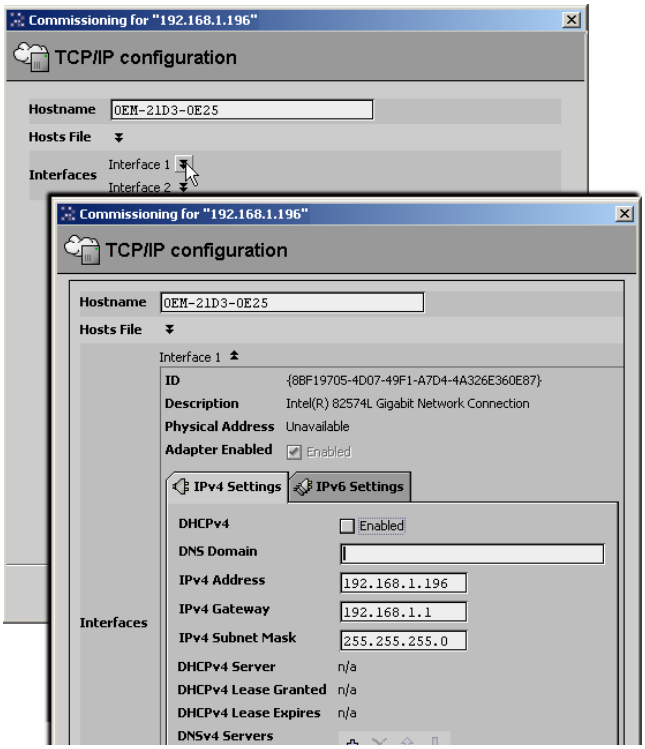
Note: *The following applies only to a CompactFlash (flash-based) JACE-NXT:*

- If a flash-based unit with EWF disabled for drive C (recommended for initial commissioning), new networks settings will become effective when the JACE-NXT is rebooted at the end of the Commissioning Wizard. Following all commissioning configuration, you should then re-enable the EWF overlay for drive C, and then reboot.
- If a flash-based unit with EWF already enabled for drive C, before making changes you should first choose to commit the EWF overlay for drive C. However, do not issue the reboot command from the EWF menu. Instead, the reboot performed by saving the TCP/IP configuration (from this platform view) will cause the new changes to be written to flash memory.

For related details, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.

In either case, note that simply turning off power to the JACE-NXT after making networking changes will not persist those changes to permanent flash memory.

Figure 16 *TCP/IP Configuration dialog*



Note: *IPv6-related properties on the* **IPv6 Settings** *tab of a JACE-NXT are* read-only *(this applies to any Win32 host). Adjustments, if necessary, must be made directly from the Windows OS interface, that is the Control Panel. For related details, see "TCP/IP configuration" in the NiagaraAX* Platform Guide.

To configure TCP/IP settings

Note: *The* **Undo Changes** *button resets all settings (both Interfaces) back to the original pre-wizard values.*

At the TCP/IP Configuration step (Figure 16) in the Commissioning Wizard, do the following:

Step 1 Click the "**Interface 1**" control to review its TCP/IP settings, which include the temporary factory-shipped IP address.

Step 2 Assign the JACE a unique IP address for the network you are installing it on. No other device on the network should use the same IP address. Include the appropriate subnet mask used by the LAN.

Alternatively, if the network supports DHCP, you can enable it (click DHCP Enabled). In this case, the IP Address and Subnet Mask fields become read only.

Note: *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 JACE may become unreachable over the network.

Step 3 Review, and if needed adjust other TCP/IP settings, which (in usual order of importance) include:

- IPv4 Gateway — The IP address for the device that forwards packets to other networks or subnets.
- DNS Domain Name — Enter the name of network domain, or if not applicable, leave blank.
- DNSv4 Servers — Click the ⊕ add button for a field to enter the IPv4 address of one or more DNS servers.
- Hostname — Default may be "localhost," or enter another name you want to use for this host.
- 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.
  1. To add a line, click at the end of the last line and press **`Enter`**.
  2. Type in the required data on the new line.
  3. To return to see all TCP/IP settings, click the control to contract the edit field when done.

Step 4 Click the **`Next`** button to go to the next step.

Note: *An "**`Interface 2`**" is also available, for configuring its (separate) TCP/IP settings. By default, this port is configured for DHCP. Although DHCP is supported in the TCP/IP configuration of both ports, typically static IP addresses are used, for stability.*

Intended usage of Interface 2 (Ethernet 2 on the JACE-NXT) is for:

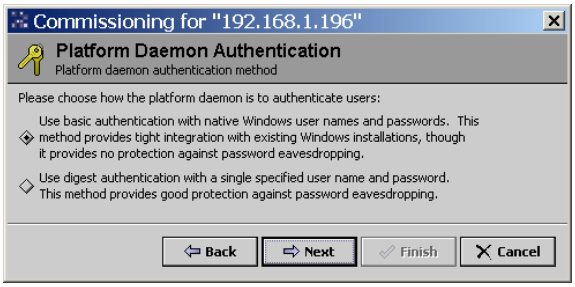
- Isolating a "driver's" Ethernet traffic from the primary (LAN1) interface, OR
- In some cases, LAN2 may be set up with a standard, fixed, IP address that is used only by a company's service technician, when on site. This allows access to the JACE without disconnecting it from the customer's network, and without connecting the technician's service PC to the customer's network (which might go against local IT security policies).

In general, it is recommended that you check with Systems Engineering before engineering a JACE-NXT solution dependent on the secondary (Ethernet 2) port, and otherwise leave it at default values.

Platform daemon authentication

At the platform daemon authentication step (Figure 17) in the wizard, you specify whether to use "basic" (Windows XP user) or "digest" authentication for platform login access to the JACE-NXT. The default is basic authentication. If you select digest instead, you can further specify the "one-only" user name and password. Always consider platform daemon access as the highest-level access to the JACE.

Figure 17 *Platform Daemon Authentication dialog (choose method)*



Caution *Regardless of chosen platform authentication method, it is strongly recommended that you change the default administrator-level Windows XP user password (user name=`Tridium`, password=`niagara`). You can do this after the wizard completes, via the platform's User Manager view. See "Additional JACE-NXT platform configuration" on page 1-17 for more details.*

Furthermore, when making credential changes, make careful note of your changes. If you lose or forget platform credentials, Tridium cannot provide you with an alternative means to access the unit. In this case, the JACE-NXT may need to be returned to Tridium for re-commissioning.

The following procedures apply to both authentication methods:

- To specify basic platform daemon authentication
- To specify digest platform daemon authentication

Note: *Following your initial commissioning of the JACE-NXT, you can always change the platform authentication method, using the Update Authentication option in the Platform Administration view.*

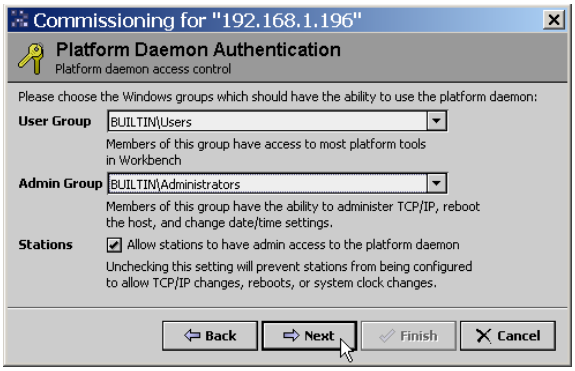
To specify basic platform daemon authentication

To specify *basic* platform daemon authentication, do the following:

Step 1 In the choose method dialog (Figure 17), leave the top ("Use basic") selection checked, and click **Next**.

A dialog for selecting Windows user groups appears, as shown in Figure 18.

Figure 18 *Platform Daemon Authentication (Use basic)*



Note: *Typically, you accept all defaults in the initial commission, then after managing Windows users, return (if necessary) to re-assign user and admin platform access to the appropriate groups.*

Step 2 In the **User Group** field, select the Windows user group to have access to most platform tools (default selection is `BUILTIN\Users`).

Step 3 In the **Admin Group** field, select the Windows user group to have access to *all* platform tools, including the ability to modify TCP/IP settings, reboot the JACE, and change date and time (default selection is `BUILTIN\Administrators`).

Step 4 Click the **Next** button.

Step 5 Click the **Next** button for the next step. Unless installing lexicons, this is "Review and finish wizard".

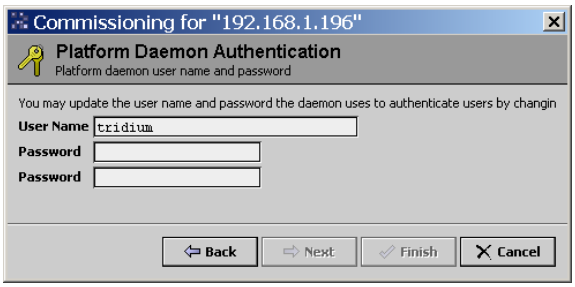
To specify digest platform daemon authentication

To specify *digest* platform daemon authentication, do the following:

Step 1 In the choose method dialog (Figure 17), check the *bottom* ("Use digest") option, then click **Next**.

A dialog for entering the digest credentials appears, as shown in Figure 19.

Figure 19 *Platform Daemon Authentication (Use digest)*



Note: *Digest user name and password entries are both case sensitive.*

Step 2 In the **User Name** field, type in the desired user name for platform login.

The digest platform user name in a JACE-NXT be any "non-empty" combination of characters, including alphanumeric (`a - z`, `A - Z`, `0 - 9`), spaces, and/or punctuation.

Step 3 In the **Password** fields, type in the desired password (it must *match* in both password fields).

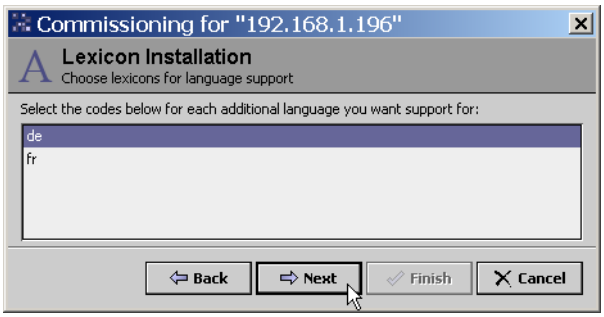
Entry characters display only in asterisks (*).

Password can be any desired length and mix of characters ("strong" passwords are supported).

Step 4 Click the **Next** button for the next step. Unless installing lexicons, this is "Review and finish wizard".

Install lexicons

Figure 20 *Lexicon Installation dialog*



At the Lexicon Installation step (Figure 20) in the Commissioning Wizard, you can install one or more lexicon files in a new JACE. Lexicons provide support for *non-English languages* in the JACE. Lexicons are identified by java locale *codes*, such as "fr" (French) or "de" (German).

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 related details, see the section "Notes on English (en) lexicon usage" in the NiagaraAX* User Guide.

In order to select lexicons, you must have installed them as part of the NiagaraAX Workbench installation on your PC. You will see only those lexicons you selected at install time, along with the "en" lexicon if added. Typically, after installing lexicons on your PC, you customize (edit) them using the Lexicon Editor in Workbench. Afterwards, you install them in JACEs, so that *each* JACE has the proper changes.

To install lexicons

To install lexicons, do the following:

Step 1 Click a language code to select (highlight) it.

If multiple lexicons are also needed, hold down the Ctrl key while you click.

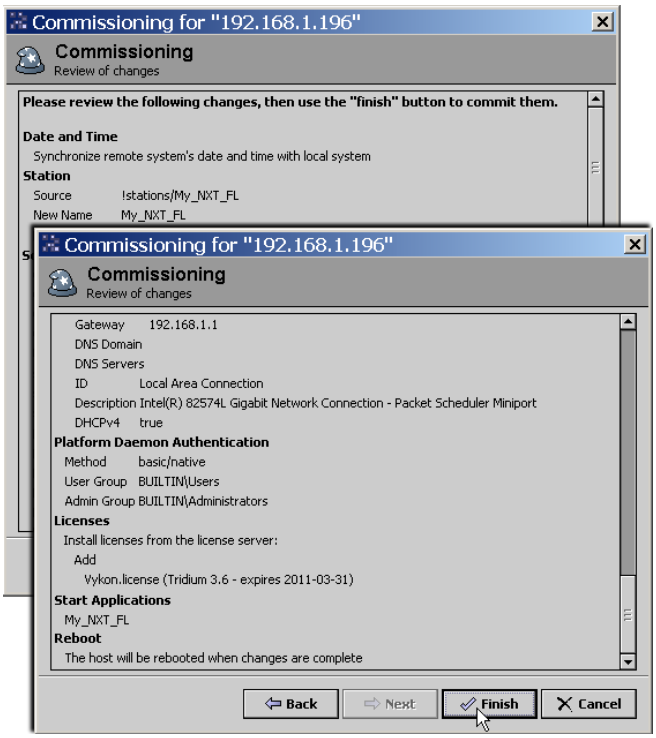
Step 2 When needed lexicons are selected, click the **`Next`** button to "Review and finish wizard".

Review and finish wizard

To review and finish the Commissioning Wizard

After the final selected step in the Commissioning Wizard, a “Review of changes” dialog appears, as shown in Figure 21. It lists a summary of all remaining actions to be performed by the wizard.

Figure 21 *Review Commissioning Wizard dialog*



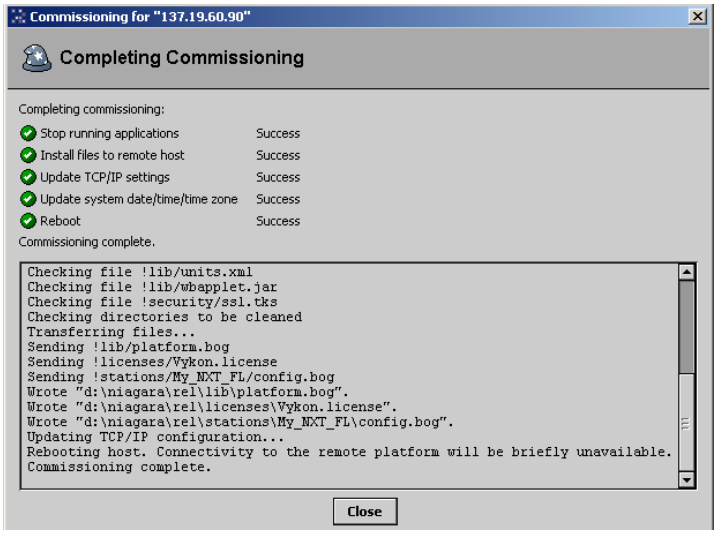
Before proceeding:

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

- If no change is needed, click the **`Finish`** button to initiate the rest of the Commissioning Wizard.
- If any change is needed, click the **`Back`** button until the step dialog appears, then make the change. Then, click the **`Next`** button until this review dialog appears again.

Step 2 While the wizard is working, progress updates are posted in a “Completing Commissioning” dialog. When completed, the wizard reboots the JACE, and a “Close” button is available (Figure 22).

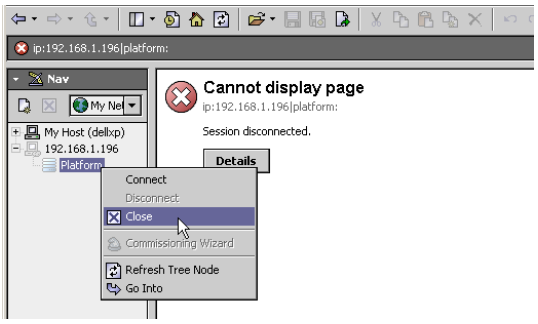
Figure 22 *Commissioning Wizard complete dialog*



Step 3 Click the **`Close`** button to exit the wizard.

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

Figure 23 *Closing now-invalid platform instance*



Step 4 Right-click and *close that platform* instance (Figure 23), as it is now invalid due to changed IP address.

Note: *Going forward, you must access the JACE by its new (assigned) IP address. Note that your Workbench keeps a history of TCP/IP changes made. See "IP changes history" on page 1-25. Also, remember to login using its new assigned platform credentials, see "Platform daemon authentication" on page 1-13.*

Note: *If you changed the IP address of your PC to commission the JACE, you also 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.*

Additional JACE-NXT platform configuration

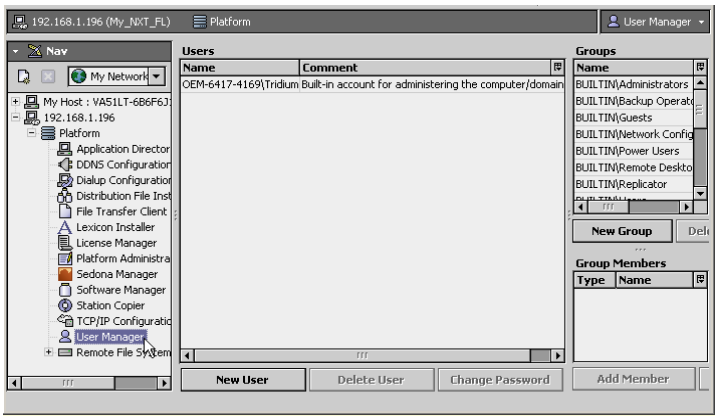
The Commissioning Wizard performs most, but not all, needed configuration for a new JACE-NXT platform. There are some items you should review (and in one case, always change) in a follow-up platform connection to the JACE, using two different platform views: the User Manager view and Platform Adminstration view.

JACE-NXT user management

After running the Commissioning Wizard to install and configure NiagaraAX in the JACE-NXT, you should open another platform connection and use the **`User Manager`** view to do the following:

- *Change the password* of the default administrator user (Tridium) from "`niagara`" to something else. Otherwise, the JACE is exposed to unauthorized access by anyone familiar with this well-known username/password convention. This applies to both general Windows host access, and (if using basic authentication) NiagaraAX platform access.
- Optionally, add other Windows users and/or groups, if needed.

Figure 24 *User Manager is one of several platform views*



For more details, see the "User Manager" section in the *Platform Guide*. For a procedure specific to a new JACE-NXT, see the next section "Change the default Windows password".

Change the default Windows password

To change the default Windows password

With your Workbench PC configured with its normal working IP address, and the JACE already commissioned using the Commissioning Wizard:

Step 1 Open a platform connection to the JACE-NXT.

Use the procedure "Open a platform connection" on page 1-4, *except* use the JACE IP address and platform credentials (username and password) that you configured when running the wizard.

Step 2 In the JACE platform's Nav Container View, double-click `User Manager`.

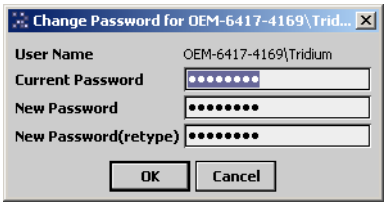
The **`User Manager`** view appears (Figure 24).

Step 3 In the **`Users`** pane, click the `Tridium` user to highlight it.

Step 4 Click the **`Change Password`** button (bottom of view).

A "Change Password" dialog appears, as shown in Figure 25.

Figure 25 *Change password dialog*



Step 5 In the **`Current Password`** field, type in the default password.

Typically, this is: `niagara`

Step 6 In the **`New Password`** fields, type in the desired password (it must *match* in both password fields).

Entry characters display only in asterisks (*).

Password can be any desired length and mix of characters ("strong" passwords are supported).

Note: *Remember this password—no one else can provide it back to you.*

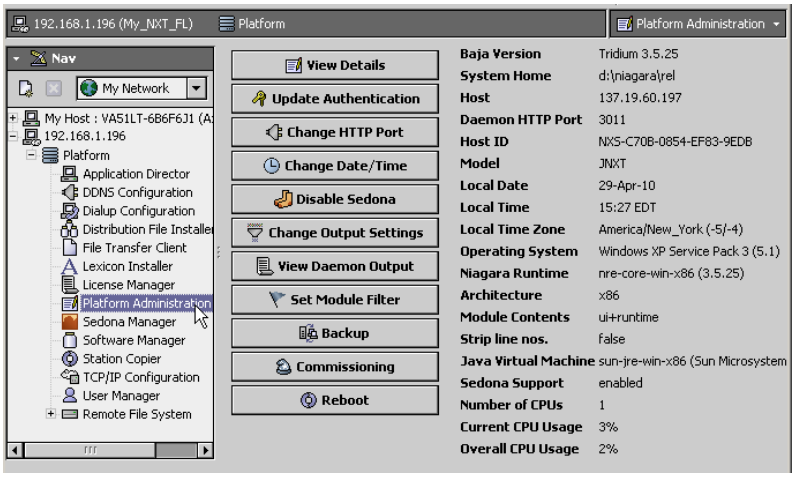
Step 7 Click **`OK`**.

The new password becomes immediately effective. If the JACE-NXT is configured to use basic platform authentication, and you click on another platform view, you are challenged for platform login again.

JACE-NXT platform administration

The Platform Administration view is one of several views for any platform, listed under the platform in the Nav tree side bar (Figure 26).

Figure 26 *Platform Administration is one of several platform views*



Note: *As shown above, the "Model" of a JACE-NXT shows as "`JNXT`", however, its "Host ID" begins with "`NXS-`".*

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

- Set the date and time in the JACE.

Typically, this is needed only if you did *not* choose to "sync" with your local system date and time when running the Commissioning Wizard.

- Change the HTTP port used by the JACE for the Niagara platform daemon (platform server). The default port is 3011.
- View a simple text summary of the JACE's current software configuration, including its model number, OS level, JVM version, installed modules, lexicons, licenses, certificates, and so on.
- Use debug-level tools to change logging levels and view platform daemon output.
- Perform other platform tasks available using the Commissioning Wizard, such changing platform authentication (platform's username and password), and so on.

For more details, see the Platform Administration section in the *Platform Guide*. For a procedure specific to a new JACE-NXT, see the next section "Administer the JACE-NXT platform".

Administer the JACE-NXT platform

To perform platform administration

With your Workbench PC re-configured with its working IP address, and the JACE already commissioned using the Commissioning Wizard:

Step 1 Open a platform connection to the JACE, if not already opened.

Use the procedure "Open a platform connection" on page 1-4, *except* use the JACE IP address and platform credentials (username and password) that you configured when running the wizard, and if using basic authentication, the changed Windows password (see "Change the default Windows password" on page 1-18).

Step 2 In the JACE platform's Nav Container View, double-click `Platform Administration`.

The Platform Administration view appears (Figure 26).

Step 3 As needed, click the following buttons to review or make changes:

- **`View Details`** — For a platform summary that you can copy to the Windows clipboard.
- **`Update Authentication`** — For platform daemon authentication dialog to change platform login authentication method (as previously included as step in commissioning wizard).
- **`Change HTTP Port`** — For dialog to change the HTTP port for the JACE's platform daemon from port 3011 to some other port. See "Change HTTP Port" on page 1-19.
- **`Change Date / Time`** — For dialog to change the JACE's current date, time, and time zone (as previously included as step in commissioning wizard).
- **`Enable (Disable) Sedona`** — Toggles platform support for the Sedona Framework. Any change results in a reboot of the JACE. Note that at the time of this document, a JACE has little practical application for use with Sedona.
- **`Change Output Settings`** — Provides dialog to change the log level of different processes that can appear in the platform daemon output
- **`View Daemon Output`** — Provides window in which you can observe debug messages from platform daemon processes in real time. Also includes ability to pause or load.
- **`Set Module Filter`** — Provides dialog to change the module content level of the JACE (as previously included as step in commissioning wizard).
- **`Backup`** — Make a complete backup of all configuration on the connected host platform, including all station files as well as other Niagara configuration (typically unnecessary for any JACE just started up).
- **`Commissioning`** — Another way to re-launch the Commissioning Wizard, as previously used in the initial commissioning of the JACE.
- **`Reboot`** — Provides a method to reboot the JACE platform, which restarts all software including the OS and JVM, then the platform daemon, then (if so configured in the Application Director) the installed station. If you click this, a confirmation dialog appears.
  If you reboot, your platform connection is lost, and it is typically a couple of minutes until you can reconnect to this JACE. Note that a reboot is *not necessary* if you manually stopped the JACE-NXT station from the Application Director (Station Director)—unlike with a QNX-based JACE, you can **`Start`** it again without a reboot.

Change HTTP Port This step is optional, and the default port 3011 is typically used in many Niagara installations. However, for reasons of additional security or perhaps firewall issues, you may need to change the HTTP port used by the JACE's platform daemon.

Note: *If you change this port, you will be unable to reopen a platform connection without first accessing the* **`Windows Firewall`** *on the JACE-NXT, and making the corresponding change in the exception named "admin." See "Review the Windows XP Firewall" on page 1-28 for more details.*

To change HTTP port

From the Platform Administration view (Figure 26):

Step 1 Click the **Change HTTP Port** button.

A dialog appears showing the current HTTP port number highlighted (Figure 27).

Figure 27 *Change Platform Daemon HTTP Port dialog*

Step 2 Type in the new HTTP port number.

Step 3 Click **Ok**.

Your current platform connection is dropped, and the JACE platform appears ghosted in the Nav tree, showing the new HTTP port number (:*n*) in parenthesis by the platform icon.

Step 4 Access the JACE-NXT's firewall. See "To access the Windows Firewall in a JACE-NXT" on page 1-29.

On the **Exceptions** tab, edit the "admin" exception to allow access to the same TCP port.

Save and exit the firewall.

Step 5 Back in the Platform Administration view, double-click the ghosted JACE platform to get the platform login (Authentication) dialog, and enter the commissioned platform username and password. Click **OK**.

Step 6 From the platform's container view, double-click Platform Administrator to return to its view.

Note: *Before closing the host (removing it from Nav tree), carefully note the new (non-default) port number you entered. You must always specify that port number whenever reopening the JACE's platform. Note that you can also see this port number listed in a running station on that JACE, by going to the property sheet of its PlatformServices container.*

JACE-NXT platform services

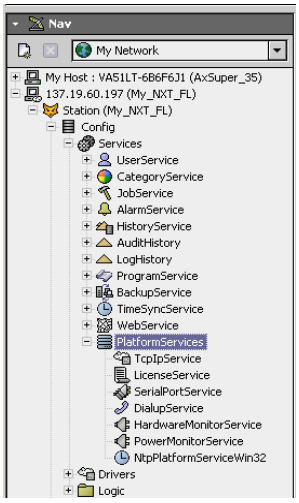
Some platform configuration is possible only by accessing *platform services* in a *station* running on that JACE. Although such configuration for a JACE-NXT may be optional, you may want to do it during the initial commissioning. The following sections explain further:

- About JACE-NXT Platform Services
- Hardware monitoring JACE-NXT configuration
- Power monitoring JACE-NXT configuration
- PlatformServices properties in a JACE-NXT

About JACE-NXT Platform Services

Under its Services container, every NiagaraAX station has a PlatformServices container (Figure 28).

Figure 28 *JACE-NXT station's PlatformServices*



PlatformServices is *different from all other components* in a station in the following ways:

- It acts as the station interface to specifics about the host platform (whether JACE or a PC).
- It is built *dynamically* at station *runtime*—you do not see PlatformServices in an offline station.
- 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!*

For any JACE-NXT, the platform service items of interest during commissioning are as follows:

- **`HardwareMonitorService`** — Holds three internal JACE-NXT environmental values: CPU temperature, board temperature, and RAM temperature. Each one has an adjustable alarm high limit, with a "default" value. See "Hardware monitoring JACE-NXT configuration" on page 1-21.
- **`PowerMonitorService`** — Provides monitoring of the SITOP UPS module connected via USB cable to the JACE-NXS, including alarms in the event of a power failure, battery test failure, or USB connectivity problem. See "Power monitoring JACE-NXT configuration" on page 1-22.

Also, you may review the parent container's PlatformService properties and optionally adjust, if needed.

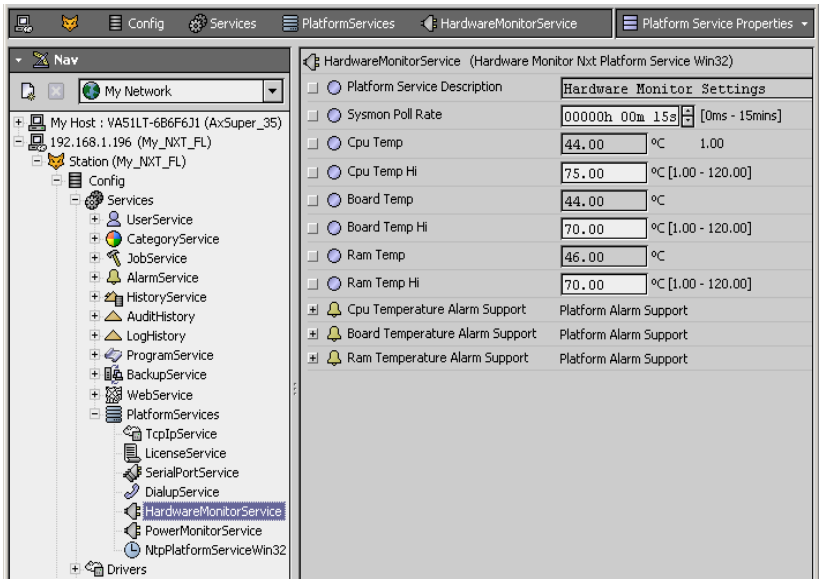
Note: *Unlike in a station running on a QNX-based JACE, the child* **`SerialPlatformService`** *contains read-only properties— serial port setup is done in the operating system, Windows XP.*

However, there is also a **`TcpIpService`** *and* **`LicenseService`***, providing station (Fox) access to dialogs used in platform views, for instance the TCP/IP Configuration dialog (as shown in Figure 16 on page 12). These platform services support installations where all configuration must be possible using only a browser connection (and not Workbench connected to the JACE's platform daemon).*

Hardware monitoring JACE-NXT configuration

The JACE-NXT provides "system monitoring" (sysmon) of *internal temperatures* of its CPU, main printed circuit board, and RAM module. These values can be indicators of the physical "health" of the device. Each temperature has a high alarm limit, used for offnormal alarming. Using Workbench, you can modify these limits and related parameters in a *running station* on the JACE, by accessing its **`HardwareMonitorService`** (under the station's PlatformServices container).

Figure 29 *Property sheet of HardwareMonitorService in JACE-NXT station*



To configure hardware system monitoring for the JACE-NXT

With a station in the JACE-NXT running, and that station opened in Workbench, do the following:

Step 1 In the Nav tree, click to expand the station's **`Services`**, **`PlatformServices`**, containers to reveal all contained services.

Step 2 Double-click the **`HardwareMonitorService`**.

Its property sheet displays in the view pane, as shown in Figure 29.

Each of the three temperatures are shown, using read-only status monitoring properties with a "float" datatype, as follows:

- Cpu Temp — Temperature of main board below the CPU.
- Board Temp — Temperature from sensor mounted elsewhere on the PC board. This provides a more general state of the environmental conditions inside the JACE-NXT.
- Ram Temp — Temperature from sensor mounted on main board near the RAM module.

If needed, you can link either of these properties into station database logic or Px graphics.

Note: *Special link considerations apply. For details, see the section "PlatformServices binding and link caveats" in the* Platform Guide*.*

Step 3 As needed, change configuration properties stored in the JACE-NXT platform, which include:

- **Sysmon Poll Rate**
  Defines the interval between system measurements. In normal operation, alarms are not generated or reset any faster than this. The default value is every 15 seconds.
- **CPU Temp Hi**
  High limit for CPU temperature, above which an alarm occurs. Default is 75°C, range is 1-120°C.
- **Board Temp Hi**
  High limit for PC board temperature, above which an alarm occurs. Default is 70°C, range is 1-120°C.
- **Ram Temp Hi**
  High limit for RAM temperature, above which an alarm occurs. Default is 70°C, range is 1-120°C.
- **CPU Temperature Alarm Support, Board Temperature Alarm Support, Ram Temperature Alarm Support**
  Each is a container for properties that define how the different "platSysmonNxt" alarms are handled in the station, including the alarm class to use and other "alarm source info" type parameters.

Step 4 Click **`Save`** to write the configuration to the JACE-NXTplatform.

Power monitoring JACE-NXT configuration

If the CompactFlash-based model (NXT-AX-FL) or any JACE-NXT model used with the NXT-UPS option (SITOP UPS and companion battery modules), a running station provides "platPower" monitoring of UPS-sourced power and battery values, including alarming capabilities. Using Workbench, access these values in a *running station* via its **`PowerMonitorService`** (under the station's PlatformServices container).

Note: *The only UPS supported by the* **`PowerMonitorService`** *is the Siemens SITOP UPS, as furnished with a NXT-AX-FL model, and connected via USB cable to the JACE-NXT. If the JACE-NXT is installed without this UPS, this platform service child has no application, and can be safely ignored.*

To configure power monitoring for the JACE-NXT

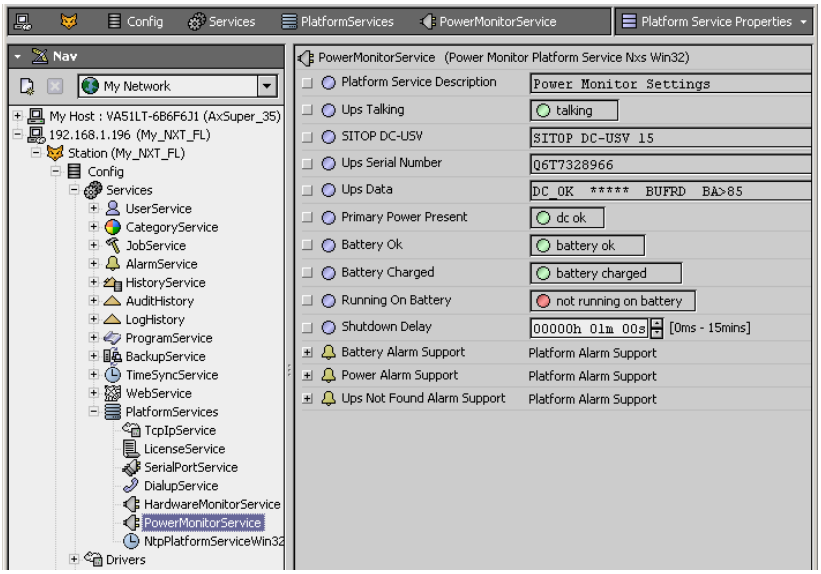
With a station in the JACE-NXT running, and that station opened in Workbench, do the following:

Step 1 In the Nav tree, click to expand the station's **`Services`**, **`PlatformServices`**, containers to reveal all contained services.

Step 2 Double-click the **`PowerMonitorService`**.

Its property sheet displays in the view pane, as shown in Figure 30.

Figure 30 *Property sheet of PowerMonitorService in JACE-NXT*



Many slots are read-only status monitoring properties, using either a “boolean” or “string” datatype. If needed, you can link any of these (or other) properties into station database logic or Px graphics.

Note: *Special link considerations apply. For details, see the section “PlatformServices binding and link caveats” in the* Platform Guide.

These read-only monitoring properties include:

- **Ups Talking**
  Boolean with values of either “`talking`” or “`no comm`”, it indicates that the service was able to establish communications with the SITOP UPS through the USB cable. If the UPS is disconnected, a “Ups Not Found Alarm” is generated (see **`Ups Not Found Alarm Support`** container to configure).
- **Ups Model**
  Text string that indicates model number read from UPS, which should read “`SITOP DC-USV 15`” if Ups Talking property is “`talking`.”
- **Ups Serial Number**
  Text string that indicates the serial number read from the UPS.
- **Ups Data**
  Text string displaying the latest raw data string received from the UPS—typically, used only to diagnose problems.
- **Primary Power Present**
  Boolean that indicates if DC power is present at the input to the UPS (“`dc ok`”). An alarm is generated upon a transition to “`dc low`”. See **`Power Alarm Support`** to configure for this alarm.
- **Battery Ok**
  Boolean that indicates how the last battery test performed by the UPS was evaluated (“`battery ok`” or “`battery failed`”). An alarm is generated upon transition to “`battery failed`”. See **`Battery Alarm Support`** to configure for this alarm.
- **Battery Charged**
  Boolean that indicates the charged state of the UPS battery pack, where either “`battery charged`” if a charge >85%, or “`battery not charged`” if <85%. No alarms are generated.
- **Running On Battery**
  Boolean that indicates whether the UPS is supplying power from the DC power supply (“`not running on battery`”) or from the battery pack (“`running on battery`”). No alarms are generated.

Step 3 As needed, change configuration properties stored in the JACE-NXT platform, which include:

- **Shutdown Delay**
  Defines the period that the JACE-NXT waits after detecting loss of primary power (Primary Power Present is “`dc low`”) before initiating a graceful shutdown. If primary power is restored before this shutdown expires, no shutdown is performed. The default value is 1 minute, with a possible range of 1 to 15 minutes.
- **Battery Alarm Support**

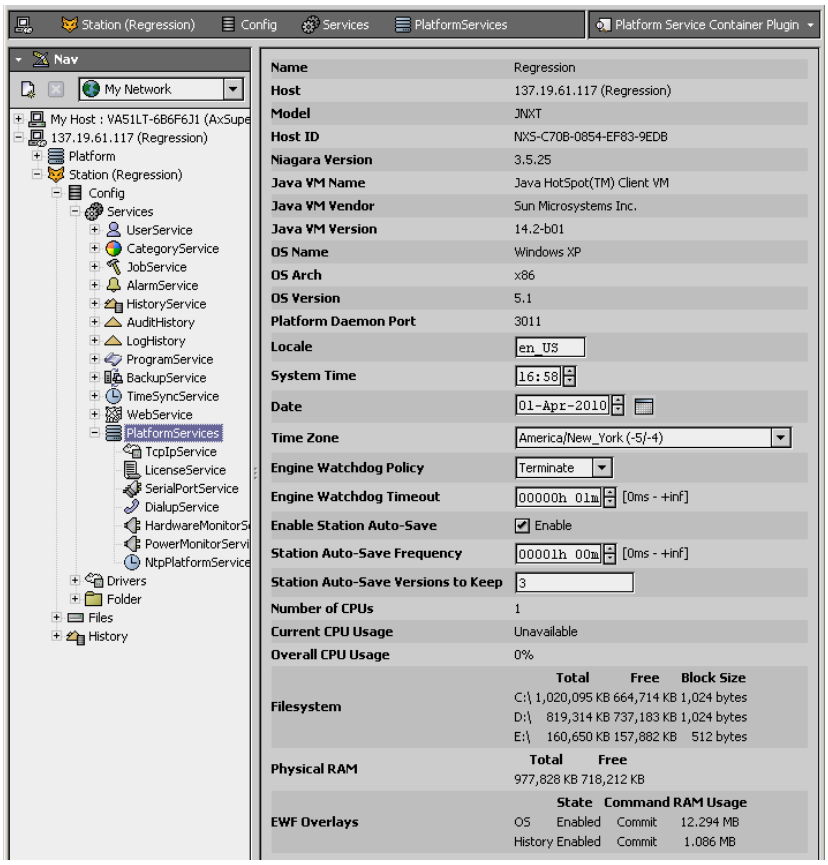
A container for properties that define how platPower "battery alarms" are handled in the station, including the alarm class used, and other "alarm source info" type parameters.

- **Power Alarm Support**
  A container for properties that define how platPower "primary power alarms" are handled in the station, including the alarm class used, and other "alarm source info" type parameters.
- **Ups Not Found Alarm Support**
  A container for properties that define how platPower "UPS not found alarms" are handled in the station, including the alarm class used, and other "alarm source info" type parameters.

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

PlatformServices properties in a JACE-NXT

Figure 31 *PlatformServices property sheet in JACE-NXT*



To review PlatformServices properties for the JACE-NXT

With a station in the JACE-NXT running, and that station opened in Workbench, do the following:

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

Its property sheet displays in the view pane, as shown in Figure 31.

Many are read-only status types, similar to what is available in the Platform Adminstration view. Other configuration properties are available. A group of 3 config properties allow adjustment of the time, date, and time zone settings for the host JACE (alternately accessible using a platform connection to the JACE). Access to these properties is useful if the installation requires all setup access using a browser only.

Step 2 As needed, review other platform service configuration properties, which include the following:

Note: *It is strongly recommended that you leave the following properties at default values, unless otherwise directed by Tridium Systems Engineering.*

- **Locale** — Determines locale-specific behavior such as date and time formatting, and also which lexicons are used. A string entered must use the form: `language` ["_" `country` ["_" `variant`]] For example U.S. English is "`en_US`" and traditional Spanish would be "`es_ES_Traditional`". For details, see Sun documentation at http://java.sun.com/j2se/1.4.2/docs/api/java/util/Locale.html.

- **`Engine Watchdog Policy`** — Defines 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 watchdog purpose is to detect and restart a "hung" or "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.
  - Terminate — (Default) Kills the VM process. If "restart on failure" is enabled for the station (typical), the station is restarted.
  - Reboot — Automatically reboots the host JACE platform. If "auto-start" is enabled for the station, the station is restarted after the system reboots.
- **`Engine Watchdog Timeout`** — Default is 1 minute, and range is from 0 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 Enable (default) or Disable.
  Allows for "auto save" of running station to "`config_backup_<YYMMDD>_<HHMM>.bog`" file at the frequency defined in next property. Auto-saved backup files are kept under that station's folder.
- **`Station Auto-Save Frequency`** — Default is every (1) hour for the JACE, the range is from 1 to many hours.
- **`Station Auto-Save Backups to Keep`** — Default is 3. Oldest of kept backups is replaced upon next manual save or auto-save backup, once the specified limit is reached.
  Note: *The remaining properties are read-only status properties, and provide statistics on platform resources including CPU, RAM, and file storage. However, the following property is unique (and appears) only if the CompactFlash-based JACE-NXT model.*
- **`EWF Overlays`** — Should contain two entries representing the RAM overlays of partitions on the JACE-NXT's CompactFlash card, named "`OS`" and "`History`". For each, the listed "State" should *typically* be "Enabled". The listed "Command" should typically be "`No_Cmd`" for "`OS`", and "`Commit`" for "`History`". However, during commissioning or configuration other values may be present.
  For related details, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.

Step 3 Click **`Save`** to write any configuration change to host platform.

Modem configuration

Unlike some other JACEs, the JACE-NXT cannot be equipped with an integral dialup modem. Contact technical support if an external modem is desired.

Recovery tips

During JACE commissioning, it is possible to run into problems. For instance, you may mis-type an IP address when entering it, and as a result be unable to regain access. In this scenario, you should know about the IP changes history kept by Workbench.

IP changes history

Your Workbench PC records "before and after" TCP/IP settings made from Niagara platform connections in an `ipchanges.bog` file. If necessary, you can review changes from Workbench using the following procedure.

To review TCP/IP changes made from your Workbench PC

From your PC with Workbench started, do the following:

Step 1 In the Nav tree, expand "`My Host`" and then "`My File System`."

Step 2 Expand "`Sys Home`" and then "`users`."

Step 3 Expand your user folder, then expand "`ipchanges.bog`."

Child folders are "date-named" using the following convention:

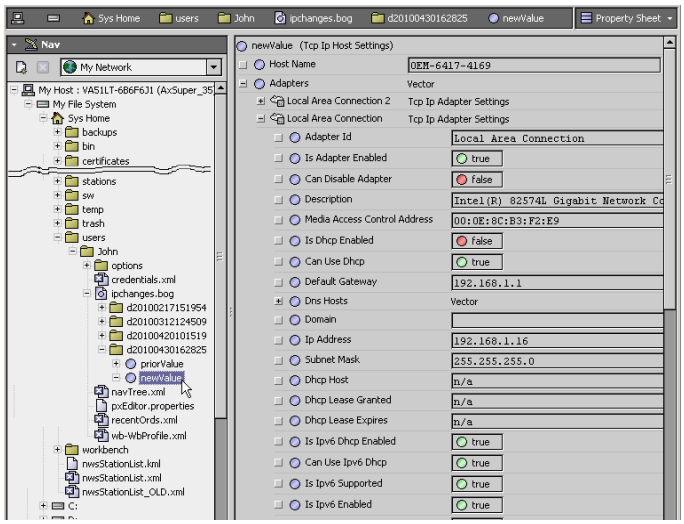
`d<yyyymmddhhmmss>` for example, "`d20100413141522`" for 2010 Apr 13 2:15pm

Step 4 Expand any folder of interest. Underneath each folder are two objects:

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

Step 5 Double-click a priorValue or newValue to see settings in the "Tcp Ip Host Editor" (see Figure 32).

Figure 32 *Accessing ipchanges.bog in Workbench*



Note: *If you have a platform connection open (to any host), you can also review the history of IP changes made from your Workbench's TCP/IP Configuration view.*

Click the **`Audit`** *button at the bottom of the view.*

This shows your `ipChanges.bog` *folder and all child change entries. Expand a change folder to see a decoded* "modTime" *value, for example, "13-Oct-2009 02:15 PM" (vs "d20091013141522").*

Double-click a "priorValue" or "newValue" in the view to see the settings in the "Tcp Ip Host Editor."

JACE-NXT Windows XPE security

Currently, any JACE-NXT ships with the SP3 (service pack 3) version of Windows XP Embedded (XPE). As shipped, Windows XPE on the controller may need to be updated with the latest security patches. In addition, a feature of Windows XPE is the **`Windows Firewall`**, which is factory-configured to permit network access to only selected TCP/IP ports used in NiagaraAX.

This section provides a brief overview about updating Windows XPE and reviewing Windows Firewall settings.

- Update Windows XPE on JACE-NXT
- Review the Windows XP Firewall

Update Windows XPE on JACE-NXT

Tridium prepares special Windows XP Embedded *security update* files on an ongoing basis for you to download and copy to the `C:` drive of the JACE-NXT. You can then logon as the Windows administrator on the unit and execute the update(s). The update process uses a "Device Update Agent" (DUA).

Note: *Support has also been added for applying Microsoft QFE (Quick Fix Engineering) updates. These will become available when Niagara-Central support for supplying these updates becomes available. In the future, updates may be provided in the form of QFEs , DUA packages, or a combination of both. More information on QFEs is likely to be covered in a future document update.*

Caution *Typically, installation of Microsoft OS updates and/or security patches ends with a system reboot. Although this does not matter for a new JACE-NXT (without a working station), please keep this in mind whenever installing future Windows XP updates.*

- If a CompactFlash-based unit, *before* installing updates, be sure to *disable* EWF (leave unprotected) for the drive C partition first, rebooting afterwards. For details, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.
- Also *before* updates, use the NiagaraAX backup feature to backup the JACE-NXT to your PC.
- In addition, make sure any controlled equipment is in a safe, manual mode of operation.

The following subsections provide more details:

- About Windows security updates for the JACE-NXT
- Check JACE-NXT Windows XPE update level (listUpdates)

- Apply an NxtXpeUpdate to a JACE-NXT
- Notes on NxtXpeUpdates

About Windows security updates for the JACE-NXT

Windows XP Embedded updates and security patches for Win32 based JACEs are released by Tridium as self-extracting executable files. When copied to (and executed on) the target JACE, files are extracted to appropriate directories on that host. This includes files for security patches as released by Microsoft, as well as a special "`update.dup`" device program file, which works with the DUA service running on the JACE-NXT (as well as the previous JACE-NXS controller).

Tridium-prepared update files are numbered sequentially, and must be applied one at a time, in numerical order.

For a JACE-NXT, the file naming convention used for updates is:

`NxtXpeUpdate_SPn_y.exe`

where *n* is XP Service Pack level (3, for example) and *y* is update sequence number.

For example: `NxtXpeUpdate_SP3_12` can be applied to any JACE-NXT already running the earlier (`NxtXpeUpdate_SP3_11`) update. See the next section, "Check JACE-NXT Windows XPE update level (listUpdates)" and also "Apply an NxtXpeUpdate to a JACE-NXT" for a typical installation procedure.

Note: *The previous JACE-NXS controller uses* different *update files:* `NxsXpeUpdate_SPn_y.exe`

About the Windows Device Update Agent (DUA) The Device Update Agent (DUA) is a service which runs in the background of Windows XP Embedded. This service starts whenever the JACE-NXTboots, and remains running. The tasks performed by the DUA service on a JACE-NXT are simple:

1. On a regular poll cycle, it checks for the existence of any "`.dup`" file in the `C:\dua` directory. Note that a "`.dup`" file is a "device update program," and is actually a compiled version of a script file with instructions to move/copy/rename/delete files, add/remove/modify registry keys, reboot, and so on.
2. If this special file exists, it executes it. If it does not exist, it does nothing but wait until the next poll cycle.

Note: *The* `update.dup` *file, along with all the necessary Microsoft patch files, are automatically copied under the target* `C:\dua` *directory when you execute a self-expanding* `NxtXpeUpdate.exe` *file. See the section "Apply an NxtXpeUpdate to a JACE-NXT" for the installation procedure.*

Check JACE-NXT Windows XPE update level (listUpdates)

Use a **`Remote Desktop Connection`** to the JACE-NXT (or local console) to check its original Windows XP Embedded image level, current update level, *next update* required, as well as its update history.

To check Windows XP Embedded update level

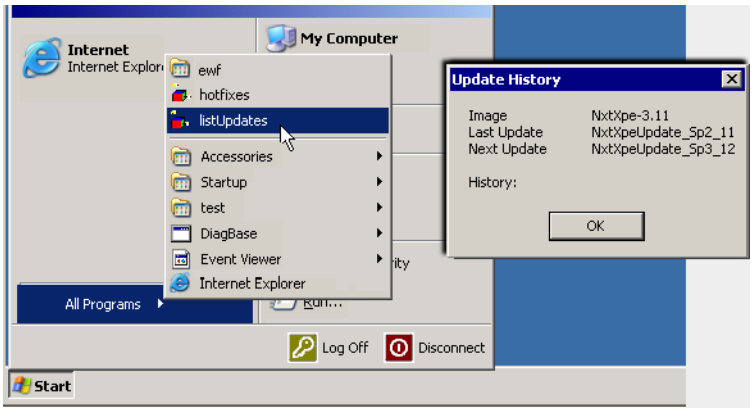
Step 1 Logon as an administrator to Windows XP running on the JACE-NXT, using either a **`Remote Desktop Connection`**, or a local console.

Step 2 From the **`Start`** menu, click **`All Programs > listUpdates`**.

As shown in Figure 33, a popup **`Update History`** dialog lists all currently applied security updates.

Step 3 After carefully noting the "*Next Update*" to be applied, click **`OK`** to close the dialog.

Figure 33 *Checking Windows XPE update level*



You can check for available JACE-NXT Windows security updates on the Tridium portal (Niagara Central) or secure website. If the "Next Update" is not yet available, no action is necessary. If more than one update is needed, download them all, and apply them in numerical sequence. See the next section, "Apply an NxtXpeUpdate to a JACE-NXT".

Apply an NxtXpeUpdate to a JACE-NXT

After checking the JACE-NXT's update level (see "Check JACE-NXT Windows XPE update level (listUpdates)" on page 1-27), you should compare its "Next Level" needed to what security updates are available for download for the JACE-NXT, on the Niagara Central portal. If a needed update (or updates) are available, use the following procedure to install each one.

Note: *If a CompactFlash-based JACE-NXT, before applying any update you should disable EWF on drive C (leave unprotected). For related details, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.*

To apply an NxtXpeUpdate to a JACE-NXT

Step 1 Download the `NxtXpeUpdate_SPn_y.exe` file from the Niagara Central portal to your PC.

Step 2 With your PC on a LAN with the JACE-NXT, transfer the downloaded update file to it. Typically, you use a NiagaraAX platform connection and the File Transfer Client. The target destination is not critical—for example, you can copy the `NxtXpeUpdate_SPn_y.exe` file to the `C:\` (root) of the JACE-NXT.

Note: *If desired, simply copy the downloaded NxtXpeUpdate file to the root of USB flash drive. Then insert the drive into the JACE-NXT, where it will appear on a new logical drive.*

Step 3 If not already started, open a **`Remote Desktop Connection`** to the JACE-NXT, logging on with a Windows administrator-level account.

Step 4 Open Windows Explorer on the JACE-NXT, then navigate to the location of the copied update `.exe` file.

The location of the file will depend on the file transfer method chosen.

Caution *Within 1 minute of completing the next step, the update script file will execute, and will typically result in a reboot of the JACE-NXT. Make sure it is safe to reboot before performing this action!*

Step 5 Double-click the NxtXpeUpdate `.exe` file to launch the WinZip self extractor, and select **`Unzip`**.

Note: *Leave the target "`Unzip to folder`" at "`C:\dua`" to ensure proper extraction. Do not change "`Unzip to folder`".*

Click **`OK`** when the WinZip Self-Extractor finishes, and close the WinZip dialog.

Step 6 The JACE-NXT will execute the security update on the next DUA poll cycle, which by default occurs once per minute. When completed, the JACE-NXT will reboot.

Any connections to the JACE-NXT (Remote Desktop Connection, NiagaraAX Workbench, browser connections, etc.) will be lost.

Step 7 After sufficient time for the reboot, open another **`Remote Desktop Connection`** to the JACE-NXT. Verify the update successfully applied. See "Check JACE-NXT Windows XPE update level (listUpdates)" on page 1-27.

Notes on NxtXpeUpdates

Additional notes about applying Windows XP Embedded security updates to a JACE-NXT are as follows:

- Each NxtXpeUpdate.`exe` file should also have a companion "readme.txt" file, which contains a list of all contained Microsoft hotfixes, as well as a list of prerequisites for installing the update.
- Note that you can see the list of already-applied Microsoft hotfixes in a JACE-NXT. With a Remote Desktop Connection established, from the **`Start`** menu, click **`All Programs > hotfixes`**.

Review the Windows XP Firewall

As shipped from the factory, a JACE-NXT has its Windows Firewall configured to block incoming network connections, save for a few program and service "exceptions." Typically, each exception corresponds to one or more TCP/IP *ports*.

The following sections provide more details:

- Review current Windows Firewall settings
- Windows Firewall (port) defaults
- Using optionalLockdown.bat

Review current Windows Firewall settings

Depending on the drivers and features to be used on the station running on the JACE-NXT, you may need to make adjustments or additions to Windows Firewall exceptions. For example, if you changed the platform daemon port in the Platform Adminstration view (see "Change HTTP Port" on page 1-19), you will need to make the same change to the firewall exception named "admin." Or, if you intend to use the drivers for either Modbus TCP or SNMP, you will need to make additions in order for those drivers to work.

Note: *The JACE-NXT has a batch file that you can edit and run to simplify making certain firewall changes. See "Using optionalLockdown.bat" on page 1-30.*

Access the Windows Firewall in the JACE-NXT using the following procedure:

To access the Windows Firewall in a JACE-NXT

Step 1 Logon as administrator to Windows XP running on the JACE-NXT, using either a **`Remote Desktop Connection`** or via a local console.

Step 2 Click **`Start > Control Panel`** to open the **`Windows Control Panel`**.

Step 3 Double-click the **`Windows Firewall`** applet to launch the Windows Firewall application.

It opens displaying the **`General`** tab, showing the firewall **`On (recommended)`**.

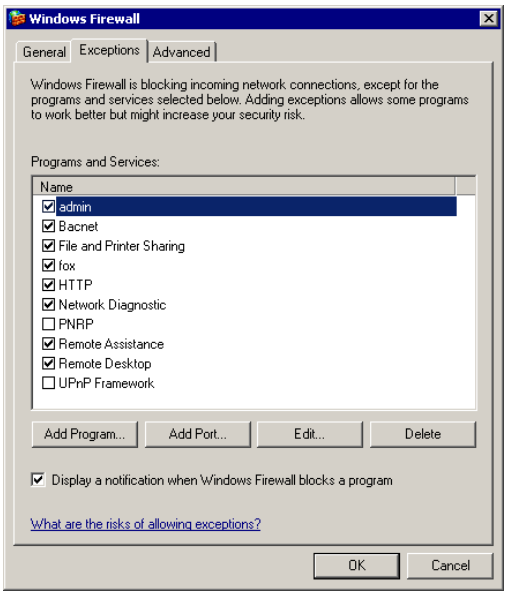
Step 4 Click the **`Exceptions`** tab, as shown in Figure 34. This is where you view or edit most settings.

See Table 1-1 for a listing of default Windows Firewall exceptions for a new JACE-NXT.

Step 5 To see the configuration for any exception, click to highlight it, then click the **`Edit`** button.

Step 6 If you make changes to any exception, click **`OK`** to save and exit the dialog.

Figure 34 *Windows Firewall exceptions (defaults) in a JACE-NXT*



For related details, see the next two sections, Windows Firewall (port) defaults and "Using optional-Lockdown.bat" on page 1-30.

Windows Firewall (port) defaults

Table 1-1 summarizes the factory-shipped Windows Firewall exceptions for a new JACE-NXT.

Table 1-1 *Windows Firewall exceptions in a factory-shipped JACE-NXT*

Exception Name	TCP port	UDP port	Protocol/Program	Description (Scope is "any source" unless noted)
admintool	3011	—	TCP, HTTP	Niagara platform connection
Bacnet	—	47808	UDP	BACnet/IP (conventional port)
File and Printer Sharing	139, 445	137, 138	NetBIOS, SMB	Windows file and printer sharing ***Note:*** *Scope for each port is local subnet only.*
fox	1911	—	Fox over TCP	Niagara Fox Service (Workbench, station-to-station)
HTTP	80	—	HTTP	HTTP, Hx access to a station
Network Diagnostic	—	—	system32\sessmgr.exe	Microsoft Remote Desktop Help Session Manager
Niagara Tunnel	9973	—	Niagara Tunnel Service	Default port for TunnelService (LonTunnel and/or SerialTunnel)
Remote Assistance	—	—	Network Diagnostic\xpnetdiag.exe	Network Diagnostics for Windows XP
Remote Desktop	3389	—	Terminal Server	Remote access using Remote Desktop Connection client
UPnP Framework (disabled)	2869	1900	SSDP	Universal plug-and-play framework, i.e. addition of PNP devices connected through Ethernet port

In addition, ICMP protocol "ping" requests are enabled, from all computers (on the Windows Firewall's **`Advanced`** tab, this is under **`ICMP Settings`**, "**`allow incoming echo request`**").

Note: *By default, both FTP and Telnet are disabled on a JACE-NXT, as each of these typically poses a significant security risk. However, if needed, you can enable these using optionalLockdown.bat.*

Alternatively, you can also add and edit firewall exceptions directly using the Windows Firewall dialog of the Windows Control Panel, as shown in Figure 34 on page 29.

Using optionalLockdown.bat

The JACE-NXT's system drive (C:) has a directory named "`lockdown`." It contains two files as shipped from the factory:

- **lockdown.bat**
  A batch file that can be run (after removing all firewall exceptions) to return the system to default firewall settings, matching all "as shipped" firewall exceptions. Usage is expected to be infrequent.
- **optionalLockdown.bat**
  A batch file which you can first edit and then execute to implement additional firewall exceptions, if needed. See the next section, "To use the optionalLockdown.bat file on a JACE-NXT".

Note: *Updates to JACE-NXT lockdown batch files may occur. Check the Niagara Central portal for details.*

To use the optionalLockdown.bat file on a JACE-NXT

Step 1 Logon as administrator to Windows XP running on the JACE-NXT, using either a **`Remote Desktop Connection`**, or a local console.

Step 2 Open a command prompt window.
To do this, click **`Start > Run...`** , type "`cmd`", then click **`OK`**.

Step 3 In the command window, navigate to the `C:\lockdown` directory.
To do this, type "`cd C:\lockdown`", then press Enter. The prompt should now be: `C:\lockdown>`

Step 4 Edit the file by typing "`notepad optionalLockdown.bat`" and pressing Enter.
The `optionalLockdown.bat` file opens in **`Notepad`** for editing. This batch file has several pre-edited command lines which have been commented out with the "`rem`" (remark) syntax.

Step 5 In the Notepad window, cursor down to the line in the file which contains the appropriate firewall command line, and remove the leading "`rem`" from that line.

Note: *Review all the firewall command lines to be sure only the ones which apply to this specific installation are uncommented. All lines without the leading "`rem`" are valid command lines, and will result in a new exception being added to the Windows Firewall.*

Step 6 **`Save`** the file, and exit Notepad.

Step 7 Run the `optionalLockdown.bat` batch file.

To do this, in the command window, type `optionalLockdown` and press Enter.

Commands in the batch file appear in the command window as they run, and any changes become immediately effective.

Step 8 Close the command window and review the Windows Firewall settings. See "To access the Windows Firewall in a JACE-NXT" on page 1-29.

Note: *If a CompactFlash-based unit with EWF enabled for drive C (typical), you will need to commit any changes from the EWF overlay (RAM) to flash. This requires EWF commands, including an orderly reboot. For related details, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.*

Notes on EWF (Enhanced Write Filter) in Windows XPE

Note: *A hard drive-based JACE-NXT does not use EWF, by default. However, you can manually configure such a unit to use EWF on drive partition C. For related details, please contact Systems Engineering.*

The Windows XPE operating system installed on CompactFlash based JACE-NXT models makes use of an "Enhanced Write Filter" (EWF) to protect the flash from excessive write transactions. This prevents premature failure of the flash memory. The EWF redirects file writes/modifies/deletes to an "overlay" located in RAM. Upon an orderly reboot, these overlay changes can then first be "committed" to persistent flash storage, or in cases where thought to be undesirable, be discarded.

By default, EWF is enabled only on two partitions of a flash-based JACE-NXT (C: System, and E: History), as the third Niagara (D:) partition does not need EWF overlay protection. Typically, Niagara writes occur only upon a station save, or if installing module jar files. These are low frequency writes as compared to various Windows file writes to the System (C:) drive or writes to the Niagara History (E:) partition.

Explicit EWF commands are used on these two partitions to either *commit* overlay changes to flash or to *discard* them. Any flash-based JACE-NXT provides related Start menu commands, see Figure 35.

Note: *EWF operation in a flash-based JACE-NXT* differs *from EWF operation in the predecessor JACE-NXS controller, which always committed changes to flash drive partitions upon an orderly reboot. Thus, the EWF commands shown in Figure 35 are new to the JACE-NXT.*

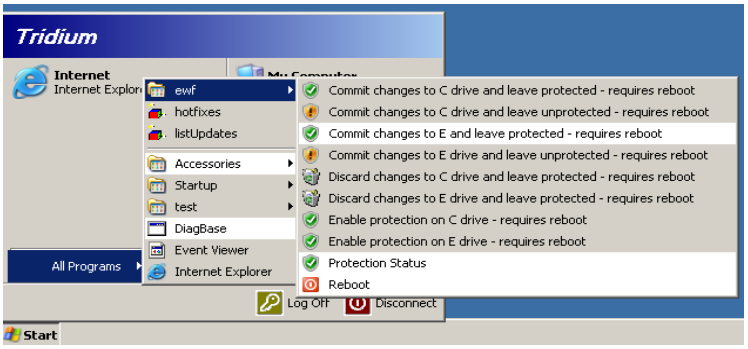
You typically access these commands using a remote desktop connection to the JACE-NXT. They are also available when you have a local console attached to the unit. For more details, see the following sections:

- EWF commands explained
- EWF use case examples

EWF commands explained

Note: *Commands in the Windows* **`Start > All Programs > ewf`** *menu of a flash-based JACE-NXT are also available as "`ewfmgr`" commands in a console window, but shortcuts were added to the menu as a convenience for the most commonly used commands.*

Figure 35 *EWF commands in Windows Start menu on a Flash-based JACE-NXT*



EWF commands in the Windows Start menu are described as follows:

- **Commit changes to C drive and leave protected - requires reboot**
  Executes the command `ewfmgr c: -commit`
  Use case:
  - When EWF (protection) is currently enabled on drive `C`, *and*
    - you have made changes to networking or other Windows configuration, even through Niagara tools (platform, PlatformServices, etc.), and you wish to persist the changes to flash.

One example use case here is after adjusting the Windows firewall.

After executing this command, you must use the Reboot command. Changes are persisted only upon shutdown.

- **Commit changes to C drive and leave unprotected - requires reboot**
  Executes the command `ewfmgr c: -commitAndDisable`
  Use cases:
  - *Before* applying Windows security updates (NxtXpeUpdate file or files), where you also invoke the Reboot command. The, after applying all security updates, re-enable EWF (protection) on drive C and Reboot again.
  - When EWF (protection) is currently enabled on drive C, *and*
    - you have made changes to networking or other Windows configuration, even through Niagara tools (platform, PlatformServices, etc.) *and*
    - you have *additional changes* you wish to make on drive C. Examples may include changes to Windows users or user groups, or changes to the Windows firewall.

    An example use case here is before the initial run of the Commissioning Wizard to commission a new JACE-NXT. You may still need to configure Windows users or user groups and/or adjust the Window firewall.

  After executing this command, you must use the Reboot command. Changes are persisted only upon shutdown.
  CAUTION: *Following the reboot, and after completing other additional changes, remember to re-enable EWF (protection) on drive C and then reboot again!*
- **Commit changes to E drive and leave protected - requires reboot**
  Executes the command `ewfmgr e: -commit`
  Note: *Drive E is used by the Niagara station to store histories and logs. During normal operation, it is best to have executed this command, and then leave it without rebooting.*

  Then, in the event the controller is rebooted, all of the history data accumulated in the overlay will be committed to flash storage. Thus, this should be the "normal" mode of operation for this partition.
- **Commit changes to E drive and leave unprotected - requires reboot**
  Executes the command `ewfmgr e: -commitAndDisable`
  CAUTION: *Drive E is used by the Niagara station to store histories and logs. You would normally not leave EWF disabled on this partition, unless directed to do so by technical support. Otherwise, excessive writes could damage the flash memory over time.*
- **Discard changes to C drive and leave protected - requires reboot**
  Executes the command `ewfmgr c: -nocmd`
  Use case:
  When EWF (protection) is currently enabled on drive C, *and* any of the below:
  - You have made changes to system configuration that you do not wish to keep.

    or
  - The system volume (drive C) has been corrupted and/or compromise, perhaps by a virus.

  After executing this command, you must use the Reboot command to discard the overlay data.
  Note: *Any system config changes made since the last boot* will be lost*, so if you have changed user names or passwords, IP config, etc., be aware of this. The same result occurs if you have local access to a JACE-NXT with protection enabled for drive C, by simply turning the unit off and then back on.*
- **Discard changes to E drive and leave protected - requires reboot**
  Executes the command `ewfmgr e: -nocmd`
  After executing this command, you must use the Reboot command to discard the overlay data.
  Note: *You would not normally exicute this command an reboot, unless directed to do so by technical support. Use may be necessary if there was obvious corruption to Niagara histories. Again, you get the same result if you have local access to a JACE-NXT with EWF enabled for drive E, by simply turning the unit off and then back on.*
- **Enable protection on C drive - requires reboot**
  Executes the command `ewfmgr c: -enable`
  Use this command to re-enable the EWF protection for the drive C System partition in flash memory. After executing this command, you must use the Reboot command for it to become effective.
- **Enable protection on E drive - requires reboot**
  Executes the command `ewfmgr e: -enable`
  Use this command to re-enable the EWF protection for the drive E Histories partition in flash memory. After executing this command, you must use the Reboot command for it to become effective.

- **Protection Status**
  Executes the command `ewfmgr -all`
  Leaving a command prompt window open to view the results, which include the current EWF state and next (boot) EWF command for both the `E` and `C` drive partitions.
  Note: *In normal operation, for a stable, already-commissioned (deployed) JACE-NXT, a summary of the EWF status command should be similar to below:*
  - Device Name: [E], State: ENABLED, Boot Command: COMMIT
  - Device Name: [C], State: ENABLED, Boot Command: NO_CMD
- **Reboot**
  Executes the command `Shutdown -r -t 10`
  Which reboots the JACE-NXT controller in 10 seconds.

EWF use case examples

A few use case variations of EWF for a flash-based JACE-NXT are described as follows:

- New JACE-NXT controller (initial commissioning)
- Windows security updates
- Minor Windows tweaks to a deployed unit
- Possible virus infection or corruption of the C (system) drive

New JACE-NXT controller (initial commissioning)

Before commissioning, disable EWF on drive `C`. This ensures that platform changes that affect Windows, such as TCP/IP changes or Windows user or user group changes, are written to persistent flash memory. Then after all commissioning, re-enable EWF on drive `C`. The specific sequence is summarized below:

1. Using a remote desktop client connection, invoke the *second* command to *Commit changes to C drive and leave unprotected*.
2. Invoke the *Reboot* command.
3. Using NiagaraAX Workbench, run the Commissioning Wizard. This typically ends with a system reboot.
4. Using NiagaraAX Workbench, reconnect and perform any subsequent Platform Administration and/or PlatformServices configuration tasks.
5. Using a remote desktop client connection, invoke the first command to *Commit changes to C drive and leave protected*.
6. Invoke the *Reboot* command.

For related details see "About the Commissioning Wizard" on page 1-5. For background details on EWF, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.

Windows security updates

Before applying Windows security updates (distributed as `NxtXpeUpdate` files), you must disable EWF on drive C. Then after applying the update(s), re-enable EWF on drive `C`. The specific sequence is summarized below:

1. Using a remote desktop client connection, invoke the *second* command to *Commit changes to C drive and leave unprotected*.
2. Invoke the *Reboot* command.
3. Apply security updates. If you have more than one update, apply them in the proper sequence. Note that a reboot should occur between update packages.
4. Invoke the first command to *Commit changes to C drive and leave protected*.
5. Invoke the *Reboot* command.

For related details see "About Windows security updates for the JACE-NXT" on page 1-27. For background details on EWF, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.

Minor Windows tweaks to a deployed unit

An already-commissioned flash-based JACE-NXT may require a minor platform or Windows change that should be persisted in CompactFlash. An example could be a firewall exception change, or a network settings change (say, `hosts` file change) performed from a Niagara platform connection.

In this case, the unit is likely operating with EWF enabled for both the drive `C` and drive `E` partitions. The specific EWF sequence is summarized below:

1. First use a remote desktop client connection, and invoke the command to *Commit changes to C drive and leave unprotected*, but do not explicitly invoke the reboot command from the EWF menu.

2. Perform the configuration change, using the save mechanism available.
   - If the platform change automatically ends in a reboot, such as from the platform's TCP/IP Configuration view, go to step 3.
   - If a reboot does not automatically occur (such as after running `optionalLockdown.bat`), issue a *Reboot* command from the EWF menu.
3. Re-establish a remote desktop connection and invoke the command to *Enable protection on C drive - requires reboot*.
4. Invoke the *Reboot* command.

For more EWF details, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31.

Possible virus infection or corruption of the C (system) drive

In this scenario, a flash-based JACE-NXT is considered to have a corrupted C drive, perhaps from a virus. The unit is likely operating with EWF enabled for both the drive `C` and drive `E` partitions. The specific EWF sequence is summarized below:

1. First use a remote desktop client connection, and invoke the command to *Discard changes to C drive and leave protected*.
2. Invoke the *Reboot* command.

For more EWF details, see "Notes on EWF (Enhanced Write Filter) in Windows XPE" on page 1-31. Also see the next section, "A few notes about virus protection".

A few notes about virus protection

The JACE-NXT runs the Windows XPE (XP Embedded) operating system, which differs from Windows XP installed on a normal PC workstation. Because of this, installing various third-party virus protection software on a JACE-NXT may prove problematic, especially with maintaining updates. Additionally, virus protection software has been known to reduce system performance.

Normal operation of NiagaraAX on the JACE-NXT does *not* result in file downloads or visitation of websites that might result in virus or malware infections, unlike with a PC workstation. Therefore, you can reduce or eliminate the exposure of these problems by observing these items:

- Only use a remote desktop connection (and/or local console) to the JACE-NXT to perform Windows configuration changes or apply Windows updates, as described in this document.
- Do *not* use a remote desktop connection (and/or local console) to the JACE-NXT as a "convenience" host to browse the Internet, for example using its Internet Explorer, accessing webmail, and so on.
- If using a USB flash drive to exchange files between the JACE-NXT and other computers, *before* inserting the USB drive in the JACE, scan it with anti-virus software running on your PC workstation.

Document Change Log

Updates (changes/additions) to this *JACE-NXT Niagara^{AX} Install and Startup Guide* document are listed below.

- Publication: December 6, 2010
  Initial document, similar to the previous NiagaraAX startup document for the JACE-NXS controller. However, this document reflects changes to the Commissioning Wizard starting in AX-3.5, and also has updated screen captures and PlatformService details specific to the JACE-NXT controller. In addition, a new "Notes on EWF (Enhanced Write Filter) in Windows XPE" was added, and is referenced in several areas of the document. This reflects changed behavior in EWF since the implementation on a JACE-NXS controller.