Technical Document

Niagara FIPS 140-2 Configuration Guide

June 7, 2023

niagara4

Niagara FIPS 140-2 Configuration Guide

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

Confidentiality

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

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

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

Trademark notice

Copyright and patent notice

Contents

About this guide

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

Product documentation

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

Document content

The Federal Information Processing Standard (FIPS) is a U.S. government security standard used to accredit cryptographic modules. These cryptographic modules undergo a thorough certification process to ensure that all cryptographic algorithms adhere to the government security guidelines.

One of the features in Niagara 4.6 and later is a FIPS 140-2 compliant mode for stations. When running in FIPS mode, stations use only cryptographic algorithms supplied by a FIPS-certified cryptographic module. This document describes how the software uses FIPS; how to get FIPS mode up and running; how to upgrade an existing NiagaraAX FIPS installation;, and some special considerations both when deploying FIPS, and when developing software to be used in a FIPS environment.

Document change log

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

June 7, 2023

Added "Host not licensed for FIPS mode" and "Cannot run the platform using Windows Supervisor in FIPS mode" topics to Troubleshooting chapter.

January 8, 2020

In the topic, "Supported FIPS 140-2 modes", replaced references to "applet" and "WebStart" with "Web Launcher".

July 19, 2018

In the Developer's notes chapter, added the topic "High CPU usage in mixed FIPS/non-FIPS environment".

Initial release: January 19, 2018

Related documentation

These documents provide additional information.

- *Niagara LDAP Guide* documents Kerberos authentication.
- *Niagara Station Security Guide* documents station security improvements.

Chapter 1 FIPS 140-2 requirements

Topics covered in this chapter

♦ Supported FIPS 140-2 modes
♦ In the Workbench : FIPS Mode vs. Non-FIPS Mode
♦ FIPS Options
♦ FIPS mode in a station

The Federal Information Processing Standard (FIPS) is a U.S. government standards regulation that governs how hardware and software use encryption and cryptographic services. To meet FIPS 140 accreditation, cryptographic modules undergo a thorough certification process by NIST (National Institute of Standards and Technology). This process ensures that all cryptographic algorithms adhere to government security guidelines. The current version of FIPS 140 is version 2, widely known as FIPS 140-2.

In order for a Niagara 4 installation to run in a FIPS 140-2 compliant mode, it must meet the following requirements:

- Its license must contain the “fips140-2” feature. This ensures that only FIPS-compliant cryptographic modules running in FIPS mode are used.
- Passwords must be at least 14 characters in length. This applies to most passwords, such as user passwords (platform and station), certificate passwords, the system passphrase, etc. Some passwords are excluded from this rule, such as passwords destined to be used with an external server, such as an email server.
- Certificates must use a key size of 2048 or 3062, and must be stored in a FIPS compliant key store.

For new Niagara installations, these requirements will be enforced where possible. When upgrading an existing installation to FIPS mode, some changes may need to be made manually. This is described in the section, “Upgrading a NiagaraAX FIPS 140-2 station”.

Supported FIPS 140-2 modes

This table shows which Niagara applications support FIPS 140-2.

Table 1 Supported FIPS 140-2 modes in Niagara

	Non FIPS	**FIPS Licensed/FIPS Enabled**	**FIPS Licensed/FIPS Disabled**
Workbench	Yes	Yes	Yes
Web Launcher	Yes	No	No
Station	Yes	Yes	No
Daemon	Yes	Yes	No
Platform	Yes	Yes	No

Workbench

A Workbench licensed for FIPS can run both in FIPS mode and non-FIPS mode. Running in non-FIPS mode allows Workbench to connect to non-FIPS stations (with potentially non-FIPS compliant passwords) and update the passwords to a FIPS-compliant length. Similarly, a non-FIPS Workbench can connect to a non-FIPS platform to update the user accounts and system passphrase as required.

IMPORTANT: A non-FIPS Workbench is required to connect to a clean JACE, since the default password is not FIPS compliant.

Web Launcher

FIPS mode is not supported for Web Launcher.

Station

The station runs in FIPS mode if it is licensed for FIPS. If it is not licensed for FIPS, it runs in non-FIPS mode.

Platform/Daemon

The platform runs in FIPS mode if it is licensed for FIPS. If it is not licensed for FIPS, it runs in non-FIPS mode.

In the Workbench : FIPS Mode vs. Non-FIPS Mode

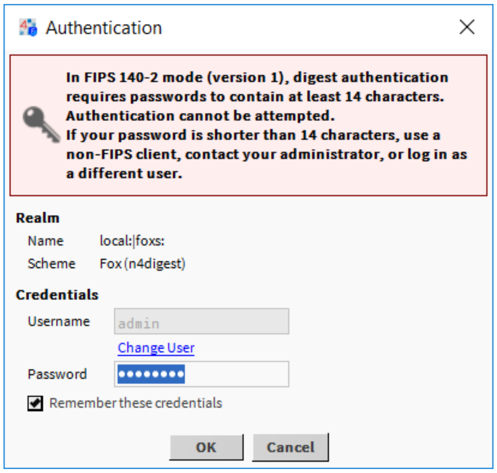
In some cases, it may be necessary to run Workbench in non-FIPS mode, even if Workbench is licensed for FIPS.

This may be necessary if:

- You are connecting to a non-FIPS station, with a non-FIPS compliant password.

  In this situation, the connection fails due to a non-FIPS strength password and the Authentication window displays a FIPS error message:

  Figure 1 Non-FIPS strength password invokes Authentication error message

  Authentication

  In FIPS 140-2 mode (version 1), digest authentication requires passwords to contain at least 14 characters. Authentication cannot be attempted.
  If your password is shorter than 14 characters, use a non-FIPS client, contact your administrator, or log in as a different user.

  Realm

  Name local:|foxs:
  Scheme Fox (n4digest)

  Credentials

  Username admin
  Password ••••••••
  ☑ Remember these credentials

  To proceed, you need to connect using a non-FIPS client (i.e. a non-FIPS instance of Workbench or other non-FIPS station), or contact your administrator, or log in as a different user (one with a FIPS-compliant password.

- You are connecting to a factory JACE that is still using the default, non-FIPS compliant password.

  In this case, the **Change Platform Defaults Wizard** displays, which includes a step to indicate whether the remote platform will be licensed for FIPS. If so, the wizard enforces the FIPS strength password requirement.

There are two ways to start Workbench in non-FIPS mode when licensed for FIPS. Use either of the following methods as needed.

- When running in FIPS mode, select **File→Non-FIPS Restart**.

  This closes your current Workbench and restarts it in non-FIPS mode.

  Note that when Workbench is running in non-FIPS mode and licensed for FIPS, there is a corresponding **File→FIPS Restart** command. This method is useful when you only need to run in non-FIPS mode once.

- In **Tools→Options→FIPS Options**, set the **`Start Workbench In Non-FIPS Mode By Default`** to `true`.

This causes Workbench to run in non-FIPS mode every time you start it. You will need to restart Workbench for this to take effect. This method is useful when you need to run in non-FIPS mode most of the time.

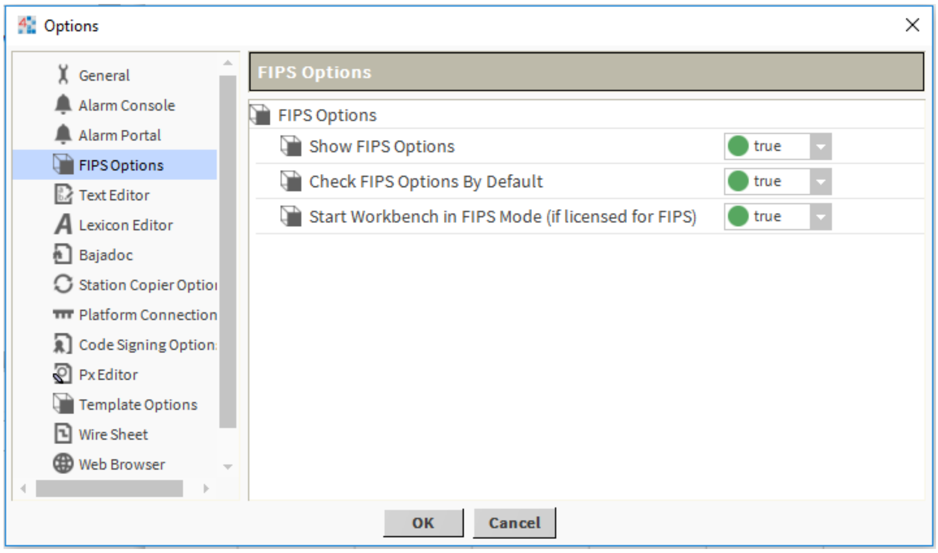
FIPS Options

In Niagara, Workbench may be used to commission remote controllers to run in FIPS mode, whether or not Workbench itself is running in FIPS mode.

In order to make FIPS options visible in various windows, go to **Tools→Options→FIPS Options**, and set **Show FIPS Options** to `true`.

If you would like the various FIPS options to be selected by default, set the **Check FIPS Options By Default** option to `true`.

Figure 2 FIPS Options



FIPS Options

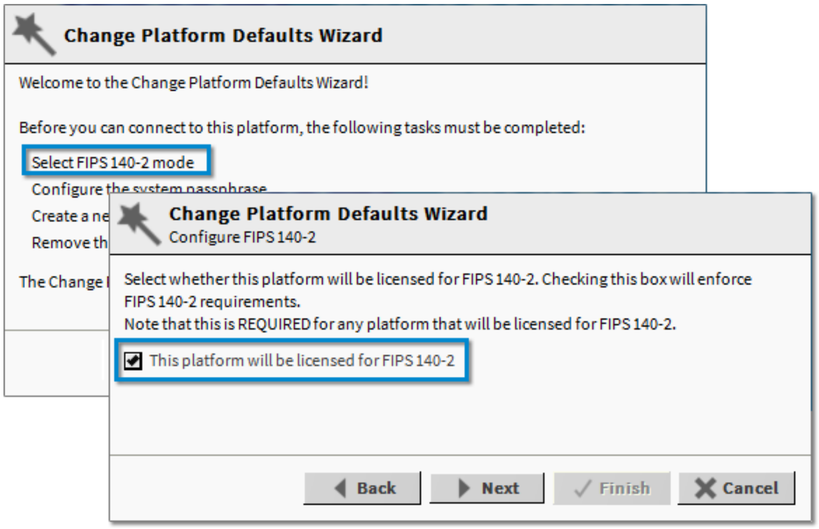
- Show FIPS Options: true
- Check FIPS Options By Default: true
- Start Workbench in FIPS Mode (if licensed for FIPS): true

Setting **Show FIPS Options** to `true` causes certain FIPS options to be visible during the following tasks:

- Changing the default platform credentials via the **Change Platform Defaults Wizard**

  If **`Show FIPS Options`** is set to `true`, the **Change Platform Defaults Wizard** adds a step: "Select FIPS 140-2 mode", as shown. This indicates that in a subsequent step the wizard displays a checkbox labeled, "This platform will be licensed for FIPS 140-2". Clicking this checkbox enforces FIPS password strength requirements. If not checked, the platform does not consider a password FIPS-compliant, even if it technically meets the requirements. Also, if both **FIPS Options** are set to `true`, by default this checkbox is visible and selected. In that situation, the wizard enforces FIPS password strength requirements by default.

Figure 3 Change Platform Defaults Wizard step to select FIPS mode



Change Platform Defaults Wizard

Welcome to the Change Platform Defaults Wizard!

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

Select FIPS 140-2 mode
Configure the system passphrase
Create a ne
Remove th

The Change

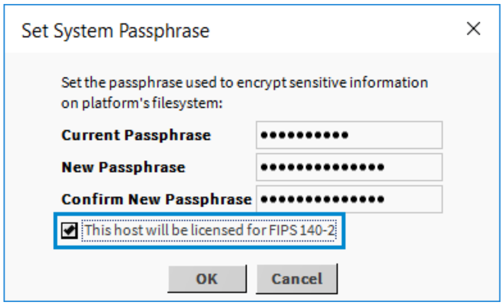
Change Platform Defaults Wizard
Configure FIPS 140-2

Select whether this platform will be licensed for FIPS 140-2. Checking this box will enforce FIPS 140-2 requirements.
Note that this is REQUIRED for any platform that will be licensed for FIPS 140-2.

☑ This platform will be licensed for FIPS 140-2

- Changing the system passphrase via the **System Passphrase** command in **Platform Administration**

Figure 4 FIPS Option in Set System Passphrase window



Set System Passphrase

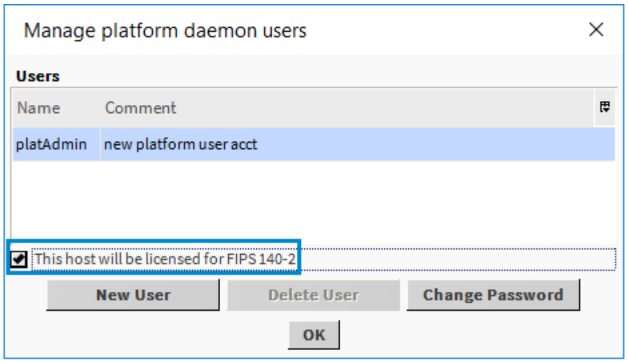
Set the passphrase used to encrypt sensitive information on platform's filesystem:

Current Passphrase ••••••••••
New Passphrase ••••••••••••••
Confirm New Passphrase ••••••••••••••

☑ This host will be licensed for FIPS 140-2

- Changing the platform user passwords via the **User Accounts** command in **Platform Administration**

Figure 5 FIPS Option in Manage platform daemon users



Manage platform daemon users

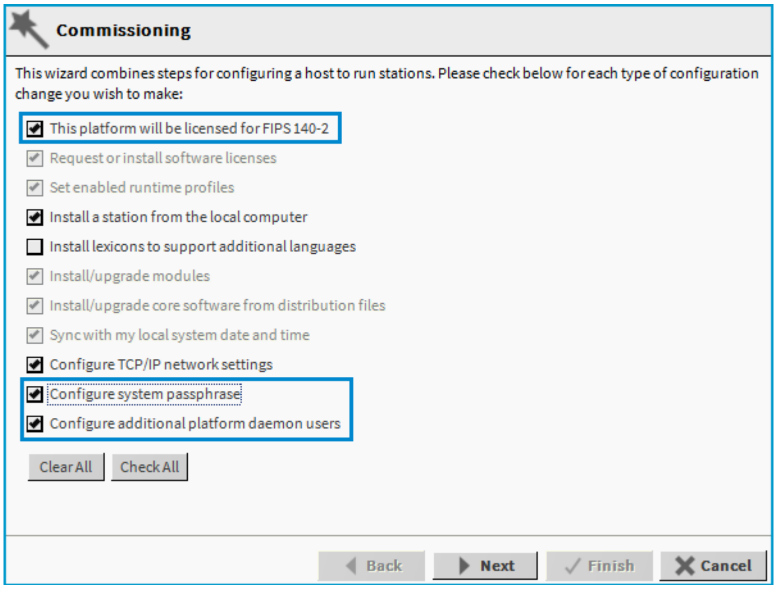
Users

Name	Comment
platAdmin	new platform user acct

☑ This host will be licensed for FIPS 140-2

- Setting the system passphrase and platform user passwords during **Commissioning**

Figure 6 FIPS Option in Commissioning



Commissioning

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

- ☑ This platform will be licensed for FIPS 140-2
- ☑ Request or install software licenses
- ☑ Set enabled runtime profiles
- ☑ Install a station from the local computer
- □ Install lexicons to support additional languages
- ☑ Install/upgrade modules
- ☑ Install/upgrade core software from distribution files
- ☑ Sync with my local system date and time
- ☑ Configure TCP/IP network settings
- ☑ Configure system passphrase
- ☑ Configure additional platform daemon users

NOTE: To install a FIPS license to a particular host, the **FIPS Options** described above must be set to `true`.

FIPS Compliant Passwords in Workbench

Workbench running in FIPS mode enforces strong passwords for operations, such as exporting certificates, setting passwords on certificates, and logging in to stations.

FIPS-compliant passwords must be at least 14 characters in length. This applies to most passwords, such as user passwords (platform and station), certificate passwords, the system passphrase, etc. Some passwords are excluded from this rule, such as passwords destined to be used with an external server, such as an email server.

FIPS mode in a station

FIPS 140-2 running in a station (Supervisor or remote controller station) uses the JCA (Java Cryptography Architecture), which allows the software to request cryptographic algorithms without relying directly on a specific security provider. Instead, requests for specific algorithms go through an ordered list of installed providers, selecting the first provider with an implementation for the algorithm. You may install additional security providers as needed, as well as remove unneeded providers.

The JCA processes all requests for cryptographic algorithms. Stations running without FIPS 140-2 provide all the Sun (Oracle) built-in providers as well as the standard BouncyCastle provider. The software selects cryptographic algorithms from any of these providers.

FIPS mode removes most Sun cryptographic providers and services. Instead, it uses the FIPS-certified BouncyCastle modules. Since all cryptographic algorithm requests through the JCA are restricted to installed providers, only FIPS-compliant algorithms are used.

NOTE: To upgrade legacy (pre-AX-3.8) stations, and because of certain required Java core functions, a small number of non-FIPS approved algorithms are still available. Although these algorithms are accessible through JCA calls, their use is not allowed in a FIPS 140-2 environment. They are allowed only during the process of upgrading legacy systems.

Chapter 2 Licensing and installation for FIPS 140-2 stations

Topics covered in this chapter

The main requirement for FIPS 140-2 in Niagara 4 is to have a FIPS license. However, in order to install a FIPS license, certain steps must be followed. The installation procedures for a supervisor and for a JACE are slightly different, and detailed in the following sections.

NOTE: The version of FIPS 140-2 that you install must be compatible with the version of Niagara installed on your Supervisor PC and remote controller(s).

FIPS 140-2 consists of:

- the module, `docFips140.jar`
- two folders for the algorithm providers: `fips` and `meta-inf`. These folders contain configuration information.

NOTE: If your application runs in a web browser, you must install the JCE (Java Cryptography Extension) local and export policy files in the JAVA home folder.

Making FIPS available to Workbench

This procedure prepares Workbench to install FIPS 140-2 on a remote host as well as to install it on the PC localhost.

Prerequisites:

- You have a license (one for each host) and
- You have downloaded the FIPS 140-2 distribution ZIP file from the Niagara Community to your Supervisor PC.

Step 1 Acquire and install a license with the "**`fips140-2`**" feature.

NOTE: FIPS-compliant passwords are required to be at least 14 characters in length. In Niagara 4.6 and later, when Workbench is started in FIPS mode and detects a non-compliant passphrase, it prompts you to change your passphrase to be FIPS-compliant. To ensure your FIPS mode supervisor is functioning properly, you should:

- Set the system passphrase to a 14 character or longer passphrase. This can be done via a platform connection to the supervisor and using the **System Passphrase** command in **Platform Administration**.
- Set the Supervisor's platform user's password to a 14–character or longer password.

NOTE: When running in FIPS mode, you will be able to run only FIPS stations.

Step 2 Restart Workbench.

The FIPS 140-2 certified providers will now be used on your local platform and supervisor.

Installing the software on a remote host

This section describes the steps required to install FIPS 140-2 on a JACE controller.

Prerequisites:

- You have already set the Workbench option, `Show FIPS Options`, to “true” (under **Tools→Options→FIPS Options**).

NOTE: Step 1 must be done in non-FIPS mode otherwise you will not be able connect to the remote host with the factory default credentials.

Step 1 Connect to a clean remote host. Before completing the connection you are required to change the default credentials via the **Change Defaults Wizard**.

Note that this change is required for security reasons and is invoked anytime factory default credentials are detected.

Step 2 On the first pane in the **Change Defaults Wizard**, ensure that the **FIPS 140-2 option** is selected.

NOTE: If you do not see this option, make sure that the `Show FIPS Options` property under **Tools→Options→FIPS Options** is set to "true". This will ensure that the system passphrase and user password that you enter are FIPS-compliant.

Step 3 In **Platform Administration** view, click **Commissioning** to commission the controller, and click the FIPS 140-2 option.

Step 4 On the **License** step, select a license for this host that contains the "fips140-2" feature.

Step 5 Optionally, on the **Install a station** step, select a station to install.

NOTE: A station may be installed during commissioning or after.

The requirement to install a FIPS license ensures that the system passphrase and user passwords were entered with the FIPS option set. If the FIPS 140-2 option was not set in the **Change Defaults Wizard**, the system passphrase and user passwords can be edited at a later time via the **Platform Administration** view, with the FIPS 140-2 option set there.

Also, if you try to commission a JACE whose passwords were not set in FIPS mode with a FIPS license, you will be given the opportunity to set them during the commissioning process.

Installing the software on a Supervisor PC (localhost)

This procedure explains how to install the license and FIPS 140-2 distribution on a Supervisor PC (local host).

Prerequisites:

- The license file is updated with the fips140–2 feature is available

NOTE: In FIPS mode passwords are required to be at least 14 characters in length. Although not enforced on the Supervisor, failure to use FIPS compliant passwords so may result in unexpected behavior or broken functionality. For more details, see “Making FIPS available to Workbench”.

Step 1 To update the Supervisor PC’s license, copy the license file from the extracted license folder (for example, `Win-B350-4C3A-8FFC-EAA9`) to the system home`!licenses` folder.

Upgrading NiagaraAX FIPS 140–2 stations

Niagara 4’s FIPS implementation differs from that of a legacy NiagaraAX, and has additional requirements. In order to upgrade a legacy FIPS station to a Niagara 4 FIPS station, it is not enough to simply migrate the station to Niagara 4.

To properly upgrade a legacy FIPS 140–2 station, the following steps are required.

AX to N4 Migration

The first step towards migrating a NiagaraAX FIPS station to a Niagara 4 FIPS station is the same as to migrate any NiagaraAX station.

This process is documented in the Niagara AX to N4 Migration Guide.

Updating User Passwords

In Niagara 4 FIPS stations, all user passwords must be at least 14 characters in length. This is a change from NiagaraAX, where passwords must be 10 characters or longer. As a result, passwords should be changed before installing the FIPS license. There are two ways to accomplish this.

Manually change all passwords before migration

This method is suitable for stations with a small number of users, who can all be contacted to change their passwords before migration.

NOTE: Although an administrator could set other users' passwords and inform them of their new passwords, this is NOT recommended. Only the user should know their own password, and passwords should never be shared via email.

Change administrator passwords, then set force change option on all other passwords

This method is suitable for stations with a large number of users, where it is not feasible to get each user to change their password before the migration.

In Niagara, each password-based user has a **`Force Reset At Next Login`** property. If this is set to true, they will be forced to change their password the next time they log in. When they log in, they will be forced to change their password to a FIPS-compliant one.

Before installing the FIPS license, certain administrator users may choose to manually upgrade their passwords, and then set the **`Force Reset At Next Login`** property to "true" for all other users.

NOTE: All user accounts corresponding to devices should be manually changed. If the accounts will only be used from non-FIPS platforms, they will continue to function, but the shorter passwords are not FIPS compliant.

NOTE: Users corresponding to remote accounts (e.g. LDAP users) should not be manually changed nor forced to reset their password. Niagara does not support changing password on LDAP servers.

CAUTION: A user using a FIPS Workbench will not be able to log in to the station until their password has been changed. They can, however, log in from the browser or from a non-FIPS Workbench.

CAUTION: For device users meant for station-to-station connections, changing the password will break connectivity until the password is updated in the client station's NiagaraNetwork entry.

Exporting certificates

In Niagara 4 FIPS mode, certificates are stored in a FIPS-compliant key store format. These certificates are kept separate from certificates used in non-FIPS mode for performance reasons. In order to be sure that all TLS connections continue to work as expected when running in FIPS mode, the certificates must be exported from non-FIPS mode and imported to FIPS mode. These steps should be followed to export certificates.

Step 1 Open the station's **PlatformServices→CertManagerService**.

Step 2 On the **User Key Store** tab, select any certificate used by the station (e.g. the certificate used by the FoxService as its "foxs cert") and click **Export**.

It is recommended to encrypt the private key; if encrypting the key, a FIPS-compliant password (14 characters or longer) must be selected.

Step 3 In the **Certificate Export** window, click each of these checkboxes: **Export the private key** and **Encrypt exported private key**, and enter a FIPS-compliant password (14 characters or more) in the **Password** and **Confirm Password** fields.

Step 4 On the **User Trust Store** tab, for all certificates, click **Export**.

After the certificates have been exported, they can be re-imported to the station via the **PlatformServices→CertManagerService** once it is restarted and running in FIPS mode. You can also import via a platform connection on the host on which the station will run and double-click **Certificate Management**. This method can be done before the station is installed and running.

NOTE: If using a non-default certificate for the platform, fox or http TLS connections, be aware that these services will not be able to start up properly the first time the station or platform starts up, because the required certificates will not be available. To ensure connectivity, you can configure your station to use the default "tridium" certificate for the duration of the migration, or enable non-TLS connections.

NOTE: FIPS mode only supports certificates with key sizes of 2048 and 3072. Certificates using other key size may not import or function correctly.

FIPS mode station startup messages

Upon station startup, station output (visible in the host platform's **Application Director** view) indicates FIPS status with one of the following messages.

FIPS mode successfully loaded

WB, station and platform all have this log message when FIPS mode is loaded, if the "**security.initializer**" log is set to FINE.

```
MESSAGE [13:21:23 30-Oct-18 EDT][sys.registry] Loaded [669ms]
MESSAGE [13:21:59 30-Oct-18 EDT][sys]
FIPS mode successfully loaded.
```

FIPS mode is licensed but disabled

This message appears on Workbench only, it indicates that the host platform is licensed for FIPS 140-2but was not started in FIPS mode.

```
MESSAGE [13:21:23 30-Oct-18 EDT][sys.registry] Loaded [669ms]
MESSAGE [13:21:59 30-Oct-18 EDT][sys]
*******************************************************
*******************************************************
********* FIPS MODE IS LICENSED BUT DISABLED! *********
*******************************************************
*******************************************************
```

You also get a popup dialog in Workbench if it is licensed but FIPS mode is disabled.

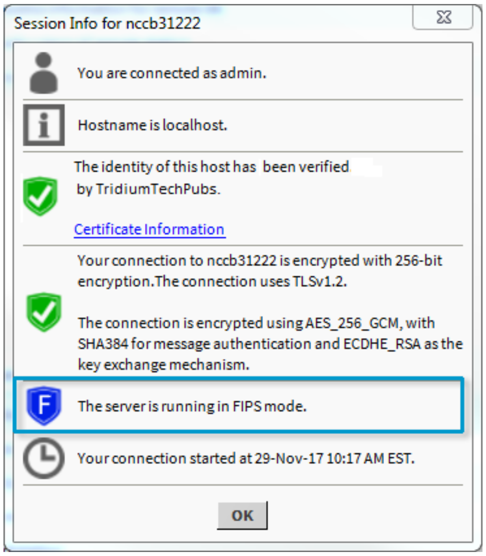
Visible FIPS mode indicators

When using Workbench or when connecting to a FIPS station or platform there are visible indicators if operating in FIPS mode.

FIPS mode indicators include the presence of either this blue shield (F) added as a badge on certain icons, or the text "FIPS Mode", or some combination of the two. For example:

- When using Workbench the application window Title Bar shows both the FIPS badge on the application icon (4F) and the text: "(FIPS Mode)".

- When connecting to a FIPS station or platform the FIPS badge is added on the fox/platform icon ( ) indicating that it is a FIPS station/platform.
- When connected to a station or platform, the **Session Info** view includes a **FIPS Mode** section which shows that it is running in FIPS Mode. You access this view by right-clicking on the station/platform icon and selecting **Session Info**:



Session Info for nccb31222

You are connected as admin.

Hostname is localhost.

The identity of this host has been verified by TridiumTechPubs.

Certificate Information

Your connection to nccb31222 is encrypted with 256-bit encryption.The connection uses TLSv1.2.

The connection is encrypted using AES_256_GCM, with SHA384 for message authentication and ECDHE_RSA as the key exchange mechanism.

The server is running in FIPS mode.

Your connection started at 29-Nov-17 10:17 AM EST.

NOTE: If the station/platform is not in FIPS mode, there will be nothing FIPS related in the **Session Info** window.

Verifying FIPS mode using Platform Services

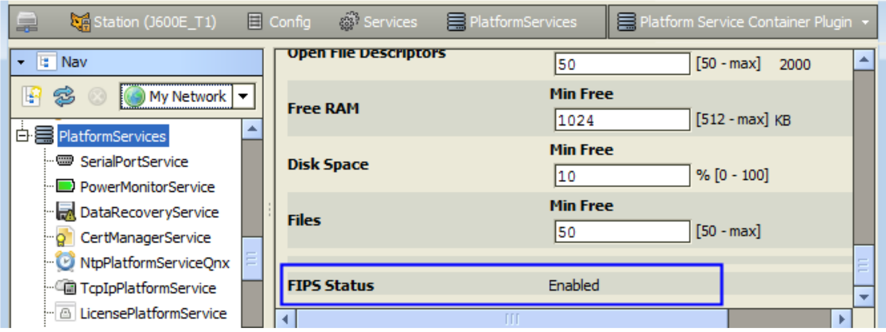
Because a station running in FIPS mode demonstrates few behavioral differences from a station not running in FIPS mode, you have several ways to check the FIPS 140-2 status of a station at any time. These are in addition to the station startup messages.

Step 1 To verify that the platform is licensed for FIPS 140-2, open the **Platform→License Manager**, select the license, click **View**, and look for a line similar to the following example in the license file:

```
<feature name="fips140-2" expiration="2025-12-31" lib="none"/>
```

Step 2 To verify that the FIPS 140-2 providers and software module are available, double-click **PlatformServices** (in the station).

The **Platform Services** view opens.



Open File Descriptors 50 [50 - max] 2000

Free RAM Min Free 1024 [512 - max] KB

Disk Space Min Free 10 % [0 - 100]

Files Min Free 50 [50 - max]

FIPS Status Enabled

Step 3 Locate the `FIPS Status` read-only property.

This property is present on hosts licensed for FIPS 140-2 and/or for which the FIPS 140-2 distribution has been installed. The property can have these values:

Value	Description
Enabled	Indicates that the station is running in FIPS mode.
Disabled (Licensed/JAR Not Installed)	Indicates that the host platform is correctly licensed, but the FIPS distribution cannot be found. The station is not running in FIPS mode.
Disabled (JAR Installed/Not Licensed)	Indicates that the FIPS distribution was correctly installed, but the host platform is not licensed for FIPS. The station is not running in FIPS mode.

Verifying FIPS mode using Spy

Provided that the **platCrypto** module is installed in the host, the station's Spy page includes a cryptographic info link that you can view.

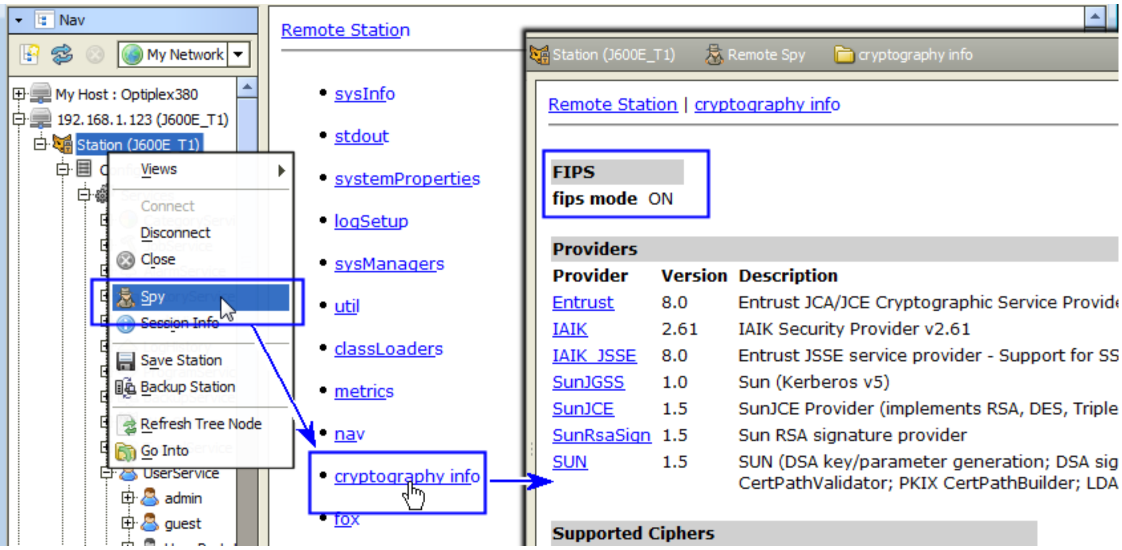
Prerequisites:

- The **platCrypto** module is installed

Step 1 Right-click the station node in the Nav tree and click **Spy**.

Step 2 Click the `cryptography info` link.

The **cryptography info** window opens.



FIPS
fips mode ON

Providers

Provider	Version	Description
Entrust	8.0	Entrust JCA/JCE Cryptographic Service Provid
IAIK	2.61	IAIK Security Provider v2.61
IAIK_JSSE	8.0	Entrust JSSE service provider - Support for SS
SunJGSS	1.0	Sun (Kerberos v5)
SunJCE	1.5	SunJCE Provider (implements RSA, DES, Triple
SunRsaSign	1.5	Sun RSA signature provider
SUN	1.5	SUN (DSA key/parameter generation; DSA sig CertPathValidator; PKIX CertPathBuilder; LDA

Supported Ciphers

- `fips mode ON` indicates that the station is in FIPS mode.
- `fips mode OFF` indicates otherwise. In addition, a station running in FIPS mode lists the Entrust, IAIK and IAIK_JSSE providers.

Chapter 3 FIPS mode

Topics covered in this chapter

♦ Web authentication and FIPS mode
♦ Kerberos authentication (in LDAP) and FIPS mode

When a host platform is licensed for FIPS 140-2 and has the FIPS 140-2 distribution installed, any station started on that platform runs in FIPS mode without any additional steps needed.

The following topics cover FIPS mode-related changes in Web and Kerberos authentication.

Web authentication and FIPS mode

When using the `DigestAuthenticationScheme` authentication scheme in a station's WebService, Javascript libraries supply client-side cryptography rather than the JCA security providers—whether the station is running in FIPS mode or not.

These Javascript libraries are FIPS compliant, but not FIPS certified.

Kerberos authentication (in LDAP) and FIPS mode

Kerberos authentication running with FIPS 140-2 is subject to additional requirements.

When this document was originally prepared, LDAP with Kerberos authentication running with FIPS 140-2 was untested. Since then, a station running in FIPS mode can only use FIPS-compliant algorithms, the LDAP and Kerberos servers were also required to support the FIPS 140-2 algorithms. The lack of FIPS-compliant support was a known problem for all versions of Windows Active Directory, which supported only DES and RC4 (neither of which are FIPS-compliant algorithms).

Kerberos authentication working together with FIPS 140-2 is not possible without meeting these requirements:

- The LDAP and Kerberos servers must support either 3DES or AES. Systems that include Hotspot QNX-based controller platforms (JACE-3E, JACE-6, JACE-7 series controllers), are limited to only 3DES.
- NiagaraAX hosts must support Kerberos. Only AX-3.8 Hotspot JVM platforms meet this standard. J9 JVM platforms (such as the JACE-2/4/5 series) do not support Kerberos authentication.
- It may be necessary to enable the use of stronger encryption on the Kerberos server. This is something the Kerberos administrator at your site would need to implement.

To ensure that only FIPS 140-2 algorithms are used when doing Kerberos authentication, configure Workbench to request only certain specific FIPS 140-2 encryption types. You do this by editing the `krb5.conf` file, described in the *Niagara LDAP Guide*. To restrict which encryption types are allowed by a client, add the following lines to the `[libdefaults]` section of this file:

```
[libdefaults]
default_tkt_enctypes = aes256-cts aes128-cts des3-cbc-sha1
default_tgs_enctypes = aes256-cts aes128-cts des3-cbc-sha1
permitted_enctypes = aes256-cts aes128-cts des3-cbc-sha1
```

These entries restrict the ciphers used to AES-128, AES-256 or 3DES.

Chapter 4 Troubleshooting

Topics covered in this chapter

♦ Non-FIPS-compliant algorithms
♦ Cannot connect to platform after commissioning to FIPS mode
♦ Cannot copy station in FIPS mode
♦ High CPU usage in mixed FIPS/non-FIPS environment
♦ Cannot run the platform using Windows Supervisor in FIPS mode
♦ Host not licensed for FIPS mode

These notes and troubleshooting tips are intended for advanced Niagara developers only.

When developing code intended for use in a FIPS 140-2 environment (a station running in FIPS mode), make sure that you use only FIPS-compliant cryptographic algorithms.

JCA (Java Cryptography Architecture) simplifies writing code for FIPS 140-2 environments. Using JCA you can add or remove security providers as needed. Different providers may implement different cryptographic algorithms, or they may provide different implementations of the same algorithm. Programs request specific algorithms through the JCA. For example, this line of code calls an AES-256 cipher:

```
Cipher cipher = Cipher.getInstance("AES256");
```

Although, to request a cipher from a specific provider you could use:

```
Cipher cipher = Cipher.getInstance("AES256", "BCFIPS");
```

You should avoid this type of call because FIPS mode and non-FIPS mode-compliant algorithms use different providers. Requesting a specific provider results in code that only works in one environment.

The JCA arranges security providers in a given order. When a program requests an algorithm, the JCA goes through the ordered list of providers and returns the first implementation it finds. In Niagara, the FIPS 140-2providers are always first in the list, which ensures, when possible, that the JCA always selects a FIPS-compliant algorithm.

In addition, with some exceptions, FIPS mode removes non-FIPS algorithms from the security providers list. This ensures that requests, which inadvertently introduce a non-FIPS algorithm, generate an exception.

Non-FIPS-compliant algorithms

Although FIPS mode removes most non-FIPS compliant algorithms from the JCA security providers list, a small subset of non-FIPS algorithms remain. In some cases, this is for compatibility with older systems (for example, to decrypt old BOG files). In other cases, Java needs specific non-FIPS-compliant algorithms, for example to load and verify security providers.

These algorithms remain available, but should be used only to upgrade an older system that uses non-FIPS algorithms.

Ciphers

- Blowfish

Message Digests

- MD5

Signatures

- MD5withRSA

For example, you can decrypt using the Blowfish cipher, but you cannot encrypt with it.

Cannot connect to platform after commissioning to FIPS mode

During the commissioning process, if a FIPS licensed is installed, a new default "tridium" certificate will be generated for TLS connections. If a certificate exemption was already approved for this host, a dialog should pop up indicating that the certificate for this host has changed, requiring the user to approve the new certificate before proceeding with the connection. In some cases, this dialog will fail to appear, and the connection cannot be made.

Two possible solutions are available.

- Go to Workbench **Tools→Certificate Manager**, and go to the **Allowed Hosts** tab. Find an entry corresponding to the JACE you are connecting to (be sure to select the entry with the correct port), and delete it.

  NOTE: Do not worry about deleting entries from this store. The only consequence of deleting the wrong certificate in Workbench is that you may need to accept the exemption again the next time you connect.
- Close the platform connection in the Nav tree, reconnect using **File→Open→Open Platform**, and approve the certificate exemption when it pops up.

Cannot copy station in FIPS mode

In some cases, after commissioning a JACE to FIPS mode, a station will fail to copy over using the platform Station Copier tool. If this occurs, doing the following may resolve the issue .

- Ensure the JACE's system passphrase is 14 characters or longer.
- Ensure the system passphrase of the host running Workbench is 14 characters or longer.
- If using a FIPS Workbench, try using a non-FIPS Workbench or vice-versa.

High CPU usage in mixed FIPS/non-FIPS environment

When using Workbench in FIPS mode and you connect to the platform of a non-FIPS JACE and open the **Platform Administration** view, the CPU usage may become very high (90-100%) while the window is open. This causes a slowdown for a number of other operations, including provisioning.

In Niagara 4.6 and later, there is a solution to the described situation. There is an added platform TLS Settings option that allows you to turn off the **Extended Master Secret** requirement on a server. If you are running in a mixed FIPS/non-FIPS environment and are experiencing a slow platform connection, perform the following steps:

1. On the JACE that is experiencing the high CPU usage, open **Platform Administration→Change TLS Settings→Use Extended Master Secret** and set this to `false`.

   NOTE: Beginning with Niagara 4.11, Extended Master Secret is supported in FIPS Mode. Niagara 4.11 introduced a new **Transport Layer Security** protocol TLS 1.3, and Niagara Framework is updated to use Bouncycastle as the TLS Provider. Before Niagara 4.11, FIPS mode did not support **Extended Master Secret**.
2. When prompted to restart the JACE, click **OK**. This is necessary for the setting change to take effect.

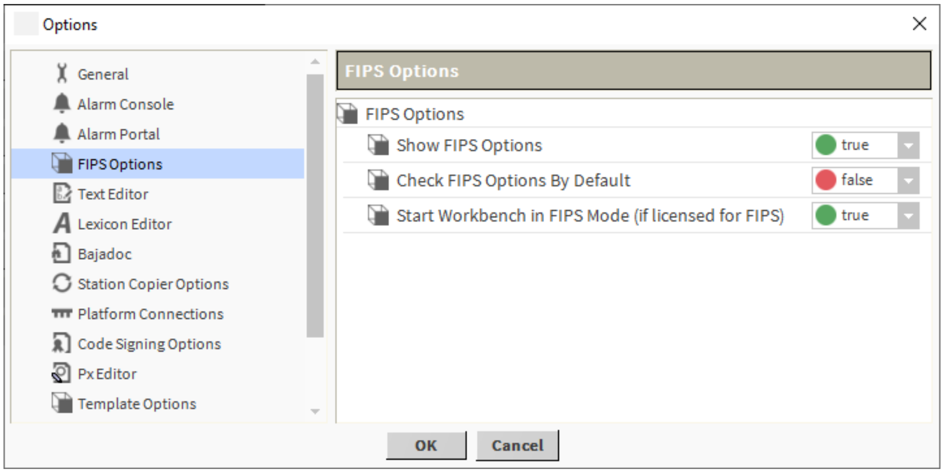
Once this is set to "false" and the platform is restarted, the JACE CPU usage does not change significantly when connecting to the **Platform Administration** view from a FIPS-mode Workbench.

Cannot run the platform using Windows Supervisor in FIPS mode

On the **Platform Administration** page, FIPS_140-2 will be listed under other components when a Windows Supervisor operates the platform in FIPS mode. If it's not there, it's running in non-FIPS mode. This will occur if a licence is required or the System Passphrase does not adhere to FIPS standards. Niagara cannot enforce Windows User passwords (or Linux Supervisor User passwords) to comply with FIPS.

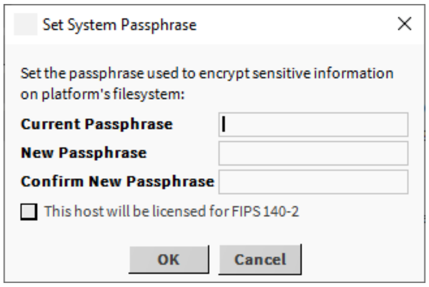
To ensure that the **System Passphrase** is FIPS compliant:

1. Go to Workbench, **Tools→Options→FIPS Options** and ensure that **`Show FIPS Options`** is `true`.



Show FIPS Options	● true
Check FIPS Options By Default	● false
Start Workbench in FIPS Mode (if licensed for FIPS)	● true

2. Login to the platform, on the **Platform Administration** page click **System Passphrase** button. To modify the system passphrase, select **This host will be licenced for FIPS-140-2** and then change the system passphrase.



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

Current Passphrase

New Passphrase

Confirm New Passphrase

□ This host will be licensed for FIPS 140-2

System Passphrase Not Updated

After providing appropriate values for the System Passphrase, a new window **System Passphrase Not Updated**, opens with the message `Error creating registry key (Error = 5).`

Two possible solutions are available:

- The Workbench must be started as Administrator to make the necessary registry key changes.
- Go to Workbench, **Tools→Options→FIPS Options** and ensure that **`Show FIPS Options`** is `true`. Login to the platform, on the **Platform Administration** page click **System Passphrase** button. To modify the system passphrase, select **This host will be licenced for FIPS-140-2** and then change the system passphrase and restart the Workbench.

Host not licensed for FIPS mode

The integrator plans to licence the host without a FIPS licence, configure and operate the Station with that licence, and then add a FIPS licence later.

The software prevents installing a FIPS license or updating a non-FIPS license to a FIPS one if the platform is not ready to run FIPS. The FIPS checkboxes ensure that the FIPS minimum requirements are met when setting the passwords. User passwords are hashed, so we can't know if they are compliant once established. `Host Is Not Ready For FIPS Mode` window appears.

Possible solution is as follows:

1. Go to Workbench, **Tools→Options→FIPS Options** and ensure that **`Show FIPS Options`** is `true`.

2. Login to the platform, on the **Platform Administration** page click **System Passphrase** button. To modify the system passphrase, select **This host will be licenced for FIPS-140-2** and then change the system passphrase.
3. Click **User Accounts** and select the **This host will be licensed for FIPS-140-2** check box. Change the password for each platform user.

   NOTE: Refer Updating User Passwords to ensure station configuration is compliant for running in FIPS Mode. Modify the password strength on the **Authentication Schemes** to ensure the station enforces FIPS-compliant passwords on all station users.
4. Navigate to **License Manager** and delete the existing license.
5. Import the license for FIPS and restart the station.

Index