Troubleshooting Guide

Nymi Connected Worker Platform
v11.0
2025-01-25

Contents

Preface

Nymi™ provides periodic revisions to the Nymi Connected Worker Platform. Therefore, some functionality that is described in this document might not apply to all currently supported Nymi products. The *Connected Worker Platform Release Notes* provide the most up to date information.

Purpose

This document is part of the Connected Worker Platform (CWP) documentation suite.

This document provides information about how to troubleshoot issues and the error messages that you might experience with the NES Administrator Console, the Nymi Enterprise Server deployment, the Nymi Band, and the Nymi Band Application.

Audience

This guide provides information to NES Administrators. An NES Administrator is the person in the enterprise that manages the Connected Worker Platform for their workplace.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
11.0	January 25, 2025	Eleventh release of this document. Updates includes new enrollment error messages when using a centralized Nymi Agent.
10.0	December 15, 2024	Tenth release of this document. Updates include changes to support Nymi Band 4.0 troubleshooting.
9.0	August 20, 2024	Ninth release of this document. Updates include the re-introduction of pre-CWP1.18.0 NES logging content.

Version	Date	Revision history
8.0	July 30, 2024	Eighth release of this document. Updates include: • Addition of new topics for issues where Centralized Nymi Agent crashes. • New error message related to enrollment, re-enrollment, registration, and re-registration.
7.0	March 26, 2024	Seventh release of this document. Updates include: • New Invalid Credentials error that appears in the Nymi Band Application • New error message that appears when you log into the NES Administrator Console for NES deployments that use HTTP. • New enrollment-specific error messages. • Revision to the section that discusses how to replace L1 and L2 certificates. • New section for Nymi WebAPI troubleshooting.
6.0	November 22, 2023	Sixth release of this document to include content from knowledge base.
5.0	November 3, 2023	Fifth release of the document. Updates include change to Lock Control log files, and new content about how to troubleshoot a Nymi Band that does not charge or display a 6000D fault code.
4.0	September 29, 2023	Fourth version of this document. Updates include new errors for NES installation.

Version	Date	Revision history
3.0	September 6, 2023	Third version of this document. Updates include the addition of information about how to create a self-signed certificate.
1.0	May 16, 2022	First version of this document.
2.0	May 8, 2023	Second version of this document.

Related documentation

- **Nymi Connected Worker Platform—Overview Guide**

  This document provides overview information about the Connected Worker Platform (CWP) solution, such as component overview, deployment options, and supporting documentation information.
- **Nymi Connected Worker Platform—Deployment Guide**

  This document provides the steps that are required to deploy the Connected Worker Platform solution.

  Separate guides are provided for authentication on iOS and Windows device.
- **Nymi Connected Worker Platform—Administration Guide**

  This document provides information about how to use the NES Administrator Console to manage the Connected Worker Platform (CWP) system. This document describes how to set up, use and manage the Nymi Band™, and how to use the Nymi Band Application. This document also provides instructions on deploying the Nymi Band Application and Nymi Runtime components.
- **Nymi SDK Developer Guide—NymiAPI(Windows)**

  This document provides information about how to develop Nymi-enabled Applications by using the Nymi API(NAPI).
- **Nymi SDK Developer Guide—Webapi(Windows)**

  This document provides information about how to understand and develop Nymi-enabled Applications (NEA) on Windows by utilizing the functionality of the Nymi SDK, over a WebSocket connection that is managed by a web-based or other application.
- **Connected Worker Platform with Evidian Installation and Configuration Guide**

  The Nymi Connected Worker Platform with Evidian Guides provides information about installing the Evidian components and configuration options based on your deployment. Separate guides are provided for Wearable, RFID-only, and mixed Wearable and RFID-only deployments.
- **Nymi Connected Worker Platform with Evidian Troubleshooting Guide**

  This document provides overview information about how to troubleshoot issues that you might experience when using the Nymi solution with Evidian.

- **Nymi Connected Worker Platform—FIDO2 Deployment Guide**

  The Nymi Connected Worker Platform—FIDO2 Deployment Guide provides information about how to configure Connected Worker Platform and FIDO2 components to allow authenticated users to use the Nymi Band to perform authentication operations.
- **Connected Worker Platform with POMSnet Installation and Configuration Guide**

  The Nymi Connected Worker Platform—POMSnet Installation and Configuration Guides provides information about how to configure the Connected Worker Platform and POMSnet components to allow authenticated users to use the Nymi Band to perform authentication operations in POMSnet.
- **Nymi Band Regulatory Guide**

  This guide provides regulatory information for the Generation 3 (GEN3) Nymi Band.
- **Third-party Licenses**

  The Nymi Connected Worker Platform—Third Party Licenses Document contains information about open source applications that are used in Nymi product offerings.

How to get product help

If the Nymi software or hardware does not function as described in this document, you can submit a support ticket to Nymi, or email support@nymi.com

How to provide documentation feedback

Feedback helps Nymi to improve the accuracy, organization, and overall quality of the documentation suite. You can submit feedback by using support@nymi.com

Log Files

NES, the Nymi Band, and the Nymi Band Application write information to log files, which enables you to monitor and troubleshoot issues that you might encounter with the Connected Worker Platform components. Log files from the Nymi Band may also be required for troubleshooting issues with your Nymi Solution Consultant.

Enrollment Terminal Log Files

Use the Menu option in the Nymi Band Application to save or view the log files.

Saving Nymi Band Application log files

Perform the following actions to save a zip file of the log files.

About this task

Procedure

1. In the Nymi Band Application, from the navigation bar, select **`Logs > Save Log Files`**. The `Save Log Files Save As` window appears.
2. From the **`Folder`** list, select a folder to save the files.
3. In the **`File name`** field, type a name for the zip file.
4. Click **`Save`**.

Viewing Nymi Band Application log files

Perform the following actions to view the log files.

About this task

Procedure

1. In the Nymi Band Application, from the navigation bar, select **`Logs > Explore Logs`**.
   Windows Explorer opens and displays the content of the log files folder. The default path to the log files is *C:\users\username\AppData\Roaming\Nymi\NEM\Logs*.
2. Double-click the log file to open the contents in the default text editor. The Nymi Band Application logs information in two files:
   - *nem.log*—Contains information about the Nymi Band Application.
   - *nymi_api.log*—Contains information about the Nymi SDK.

Windows User Terminal Log Files

Nymi Runtime is installed on the user terminals in the environment. The Nymi Runtime includes the Nymi Bluetooth Endpoint and Nymi Agent services.

- The Nymi Bluetooth Endpoint log file (*nymi_bluetooth_endpoint.log*) is located in *C:\Nymi\Bluetooth_Endpoint\logs* folder.
- The Nymi Agent log file (*nymi_agent.log*) is located in the *C:\Nymi\NymiAgent* folder.

In some configurations, for example, in RDP and Citrix Environments, the configuration uses a centralized Nymi Agent. In this configuration, the *nymi_bluetooth_endpoint.log* is on the user terminal and the *nymi_agent.log* file is located on remote machine, on which the Nymi Agent is installed.

To enable debug mode for the Nymi Runtime services, create a system environment variable named `NYMI_DEBUG` with a non-zero value, and then restart the Nymi services.

Nymi Bluetooth Endpoint Status Indicator Logs

CWP 1.19.0 includes the Nymi Bluetooth Endpoint Status Indicator application that monitors the state of the Nymi Bluetooth Endpoint service.

The includes the following log files:

- *C:\Nymi\BluetoothEndpointSystemTrayIcon\logs*-Provides information about Nymi Bluetooth Endpoint Status Indicator application.
- *C:\Nymi\NymiBluetoothEndpointRestart\logs*-Provides information that is related to the use of the *Restart* option.

Enabling Nymi Bluetooth Endpoint Debug Mode

Put the Nymi Bluetooth Endpoint service in debug mode to provide detailed information while troubleshooting issues related to Nymi Band taps.

About this task

Perform the following steps on the user terminal.

Procedure

1. Run *regedit.exe*
2. Navigate to **HKLM > System > CurrentControlSet > Services**.
3. Right-click **NymiBluetoothEndpoint**, and the select **New > String value**
4. In the value field, type ***ImagePath***.
5. Edit the ***ImagePath*** key and in the **Value data** field, type ***C:\Nymi\Bluetooth_Endpoint\nbe.exe --service --log 5***, and then click **OK**.

6. Close `Registry Editor`
7. Restart the Nymi Bluetooth Endpoint service.

Nymi Application Log files

iOS devices that access web-based Nymi-enabled ApplicationNEAs require the Nymi Application, which includes the Nymi Bluetooth Endpoint component of Nymi Runtime. The option to log Nymi Bluetooth Endpoint messages is enabled by default.

To access the log file, open the Nymi Application and touch the **Logs** icon in the upper right corner, as shown in the following figure.

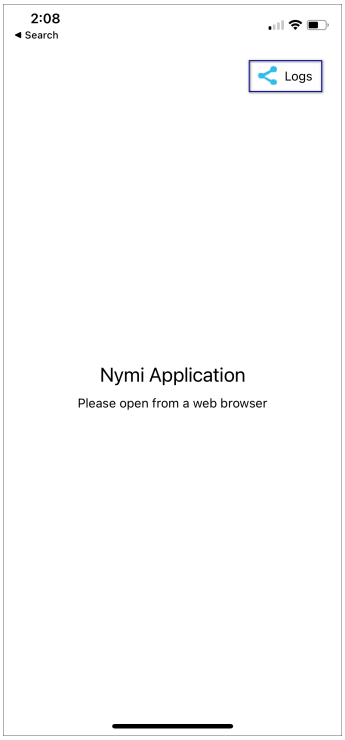


Figure 1: Nymi Application Logs

Note: If logging is disabled at the system level, the **Logs** icon does not appear.

On the file sharing options screen, select the method to share the file, for example, Air Drop or email.

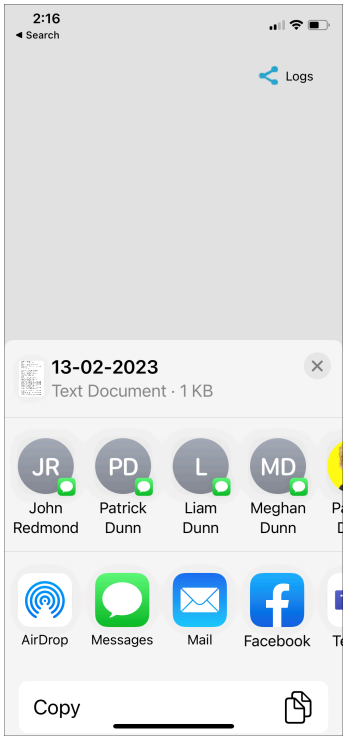


Figure 2: Nymi Application Send Options

To disable logging, navigate to **`Settings > Nymi`**, and then toggle **`Logs`** to the off position, as shown in the following figure.

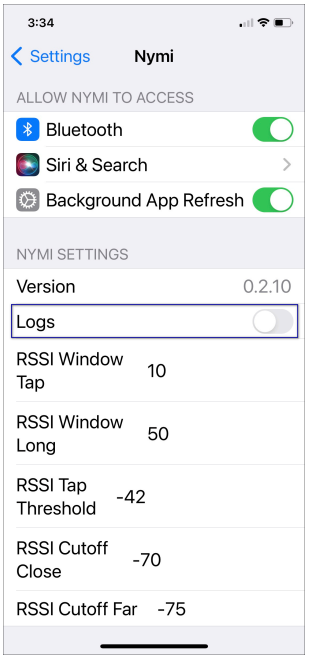


Figure 3: Disabling Nymi Application Logging

Nymi Lock Control Log Files

Nymi Lock Control creates log files for security and troubleshooting purposes.

To enable debug mode for Nymi Lock Control , create a system environment variable named `NYMI_DEBUG` with a non-zero value, and then restart the Nymi services.

Security log

The *C:\Users\Public\AppData\Nymi\unlock\Log\credential-provider.log* file contains a record of the time and result of each authentication attempt on the user terminal.

Collecting log files and contacting support

To quickly create a zip file of the Nymi Lock Control log files that you can send to Nymi Support, perform the following steps:

1. Right-click the Nymi Lock Control icon on the system tray and select **`Contact Nymi Support`**.
2. On the `Include Logs?` window, click **`Yes`**.
3. On the `Nymi Support` page, log in with your Nymi Support account.
4. On the `Nymi Support` page, click `Submit a Request`, and then in the drop-down, select **`Technical Issue`**.
5. Fill in the appropriate details, and in the **`Attachments`** section, click **`Add file`**.

6. Navigate to the *C:\Users\[username]\AppData\Roaming\Nymi\unlock\ZipLog* folder, and then select the zip file.

(CWP 1.16.0 and earlier) NES Log Files

Nymi Enterprise Server(NES) has separate log files for each web service. When you encounter an issue, review the messages that appear in each log file.

(CWP 1.16.0 and earlier) NES web services log files

NES places the installation log file in the *C:\ProgramData\Nymi\NESg2.install\log* directory.

The NES log files are in the following locations, where `nes_service_name` is the Instance name selected during the NES installation:

- *C:\ProgramData\Nymi\NESg2.Admin\Default_Web_Site*`nes_service_ name`*\log*
- *C:\ProgramData\Nymi\NEnrollment\Default_Web_Site*`nes_service _name`*_ES\log*
- *C:\ProgramData\Nymi\AuthenticationService\Default_Web_Site*`nes_service_name`*_AS \log*

(CWP 1.16.0 and earlier) Enabling NES Verbose Logging

By default, Nymi Enterprise Server (NES) logs information level messages to the log files. When you encounter an issue, Nymi Support might request that you enable verbose mode for each web service, retry the operation, and then review the messages that appear in each log file. NES has a feature that writes previously encountered error messages to log files when you increase the logging level, so it is not necessary to leave NES in debug mode after troubleshooting completes. Logging levels include Critical, Error, Warning, Information, and Verbose.

About this task

To enable verbose logging mode, perform the following steps:

Procedure

1. Edit the *C:\inetpub\wwwroot*`nes_service_name`*\nes\web.config* file and in the <system.diagnostics> section, change the value for each add name parameter from **Information** to **Verbose**.

   For example:

```
<system.diagnostics>
    <switches>
      <add name=”Global” value=”Verbose” />
      <add name=”Authentication” value=”Verbose” />
```

```
    </switches>
<system.diagnostics>
```

2. Edit the *C:\inetpub\wwwroot\`nes_service_name`\nenrollment\web.config* file and in the <system.diagnostics> section, change the value for each add name parameter from **Information** to **Verbose**.

   For example:

```
<system.diagnostics>
   <switches>
      <add name=”Global” value=”Verbose” />
      <add name=”Authentication” value=”Verbose” />
      <add name=”CertificateEnrollment” value=”Verbose” />
    </switches>
<system.diagnostics>
```

3. Edit the *C:\inetpub\wwwroot\`nes_service_name`\authenticationservice\web.config* file and in the <system.diagnostics> section, change the value for each add name parameter from **Information** to **Verbose**.

   For example:

```
<system.diagnostics>
   <switches>
      <add name=”Global” value=”Verbose” />
      <add name=”Authentication” value=”Verbose” />
    </switches>
<system.diagnostics>
```

4. Restart the IIS.

(CWP 1.17.0 and later) NES Log Files

NES has separate log files for each web service. When you encounter an issue, review the messages that appear in each log file.

(CWP 1.17.0 and later) Changing NES Log Levels

By default, Nymi Enterprise Server (NES) logs all messages to the log files.

About this task

NES supports the following log levels:

Level	Description	Message levels included in the log file
OFF	Turns off logging completely. NES does not log messages, regardless of their severity level.	n/a
ALL	NES logs all messages including low level debug messages, regardless of their severity level.	• DEBUG • INFO • WARN • ERROR • FATAL
DEBUG	NES logs messages at the DEBUG level and higher. DEBUG messages provide detailed information for debugging and troubleshooting purposes.	• DEBUG • INFO • WARN • ERROR • FATAL
INFO	NES logs messages at the INFO level and higher. INFO messages provide general information about the operation and progress of the application.	• INFO • WARN • ERROR • FATAL
WARN	NES logs messages at the WARN level and higher. WARN messages indicate potential issues or unusual conditions that might require attention.	• WARN • ERROR • FATAL
ERROR	NES logs messages at the ERROR level and higher. ERROR messages indicate errors or exceptions that occur during the execution of the application.	• ERROR • FATAL
FATAL	NES logs messages at the FATAL level only. FATAL messages represent critical errors that cause the application to terminate or become unusable.	• FATAL

Note: Nymi recommends that you leave the level at the default level *ALL*

To change the logging level, perform the following steps:

Procedure

1. Edit the *C:\inetpub\wwwroot\nes_service_name\nes\web.config* file and in the <log4net> section, change the value for each *level value* parameter from to the required level.

   For example, to change from the default value *ALL* to *DEBUG*:

```
<root>
   <level value="DEBUG" />
   <appender-ref ref="RollingLogFileAppender" />
</root>
<logger additivity="false" name="RollingLogFileAppender">
<level value="DEBUG" />
  <appender-ref ref="RollingLogFileAppender" />
</logger>
```

2. Edit the *C:\inetpub\wwwroot\nes_service_name\NEnrollment\web.config* file and in the <log4net> section, change the value for each *level value* parameter from **ALL** to **INFO**.

   For example, to change from the default value *ALL* to *INFO*:

```
<root>
<level value="INFO" />
   <appender-ref ref="RollingLogFileAppender" />
</root>
<logger additivity="false" name="RollingLogFileAppender">
   <level value="INFO" />
   <appender-ref ref="RollingLogFileAppender" />
</logger>
```

3. Edit the *C:\inetpub\wwwroot\nes_service_name\AuthenticationService\web.config* file and in the <log4net> section, change the value for each *level value* parameter from **Information** to **Verbose**.

   For example, to change from the default value *ALL* to *FATAL*:

```
<root>
   <level value="FATAL" />
   <appender-ref ref="RollingLogFileAppender" />
</root>
<logger additivity="false" name="RollingLogFileAppender">
      <level value="FATAL" />
    <appender-ref ref="RollingLogFileAppender" />
</logger>
```

4. Restart the IIS.

(CWP 1.17.0 and later) NES Log File Location

NES Installation Log File

NES places the installation log file in the *C:\ProgramData\Nymi\logs\NESInstaller* folder.

Log file names follow the format *NESGUIInstall_yymmdd*.

NES Application Log Files

The NES log files are in the following folders:

- NES Administrator Console logs: *C:\ProgramData\Nymi\logs\iis_instance_name\NesAdmin* folder.
- NES Authentication Service logs: *C:\ProgramData\Nymi\logs\iis_instance_name\AuthenticationService*
- NES Enrollment Service logs: *C:\ProgramData\Nymi\logs\iis_instance_name\EnrollmentService*

where *iis_instance_name* is the IIS instance name that was selected during the NES installation.

Log file names follow the format *iis_instance_name_nes_service_name_date*.log.*file_number*

where:

- *iis_instance_name* is the IIS instance name that was selected during the NES installation.
- *nes_service_name* is the one of the following NES service names:
  - Admin
  - AS
  - ES
- *date* is the creation date of the log file in the format *yymmdd*.
- *file_number* is optional. The maximum file size is 10MB. NES automatically renames the application log files by appending a number to the file name every 24 hours or when the file size reaches 10MB. The number appended to the file name depends on the existing log file names in the directory, and the number increases in increments of 1.

Nymi Support Tool

The Nymi Support Tool enables you to collect log information and generate a zip file that Nymi can review for troubleshooting purposes. The following logs and information is collected: NES Installation log files, Windows event logs, NES log files and NES instance configuration files.

About this task

Follow these steps to generate a log zip file.

Procedure

1. On NES server, double-click *..\`nes_installation_folder`\NesSystemInfo\NymiSupportTool.exe*.
   The `User Account Control` dialog box appears.

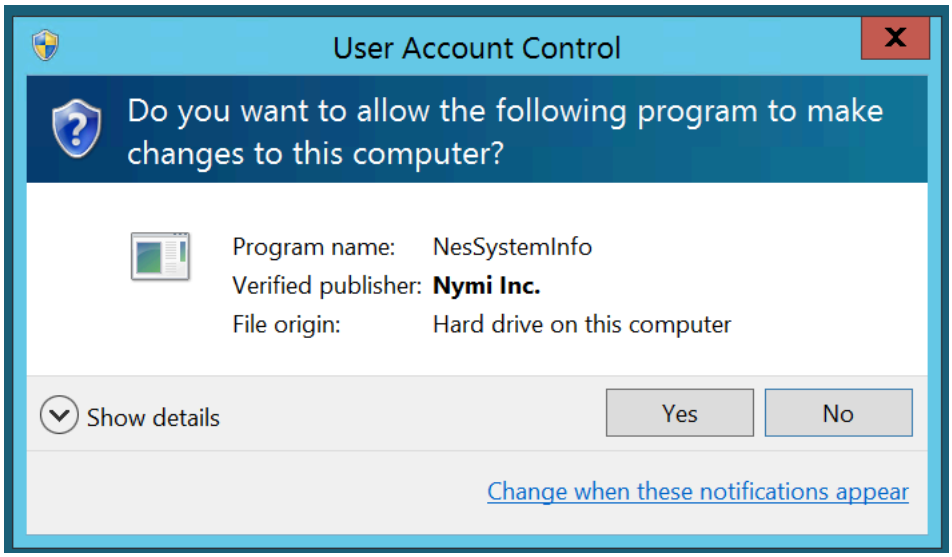


Figure 4: The User Account Control

2. On the `User access control` window, click **Yes** to start the script.
3. On the **Save As** window, click **Save** to accept the default zip file name and location. By default the name of the zip file is the server hostname and the default directory is the *Documents* folder for the user running the command.

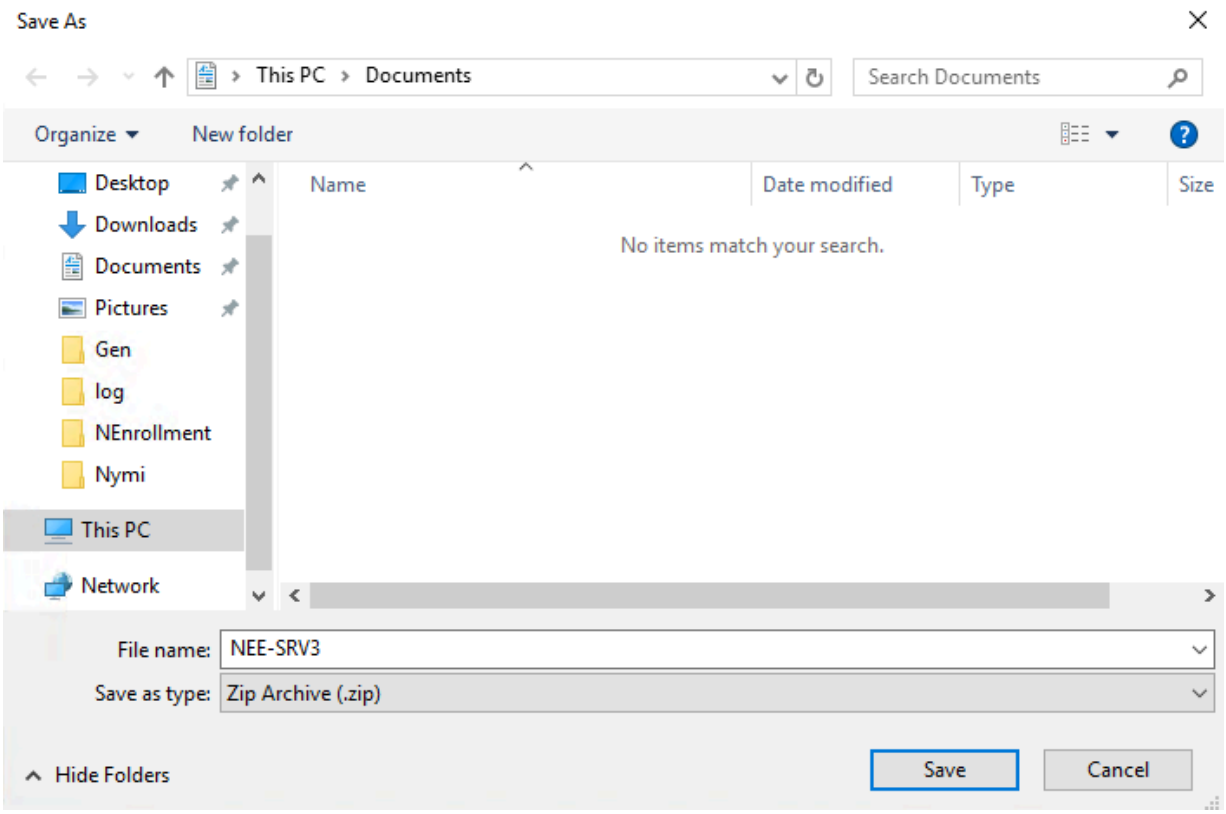


Figure 5: Saving Nymi Support Tool zip

Results

The zip file contains the following files and directory structure:

- *InstallLogs\NESg2.Installer* - Folder that contains the logs files that were created during the NES installation.
- *inetsrv\Config* - Folder that contains the *applicationHost.config*, which contains IIS configuration information.
- *NesInstances\`nes_instance_name`* - Folder that contains the IIS *web.config* files for the NES Authentication Service, Enrollment Service and Directory Service, and *info.txt* file that contains path and version information for each service..
- *EventLogs* - Folder that contains the Windows Event log files on the NES server.
- *SysInfo.txt* - File that contains information about the configuration of the NES server.
- *SupportTool.log* - Log file that contains the output of the *NymiSupportTool.exe* command.

Firmware Log Files

The Nymi Solution Consultant may request logs from the Nymi Band to troubleshoot issues.

To retrieve log files from the Nymi Band, first plug the Bluetooth Adapter supplied by Nymi into the workstation and put the Nymi Band on charge.

Nymi Band Firmware Log Retrieval

About this task

To retrieve logs from the Nymi Band, perform the following steps:

Procedure

1. Place the Nymi Band on charge while connected to a user terminal, and then move the Nymi Band and the charger close to the BLE radio antenna on the terminal (BLED112 adapter). This ensure that the retrieval tool retrieves logs files from the correct Nymi Band.
2. Download and extract the firmware package into a directory of your choice on a Windows computer. For example, *C:\Nymi_firmware*.
3. If the Windows machine has the Nymi Band Application installed on it, stop the Nymi Bluetooth Endpoint service.
4. Navigate to the *C:\nymi_firmware\build\exe.win32-2.7* directory.
5. Run the nsp_logs_download.exe. A command prompt window opens with the status of the log file download. When the download completes, the command window closes and the firmware log file is saved to the folder that contains the nsp_logs_download.exe file.

   Note: The log files from the Nymi Band are encrypted. Provide the log file to your Nymi Solution Consultant.

Determining the NES version

While troubleshooting an issue, you might require the NES version. To determine the version, connect to the NES Administrator Console, and then click **About**. The following image provides an example of the About page.

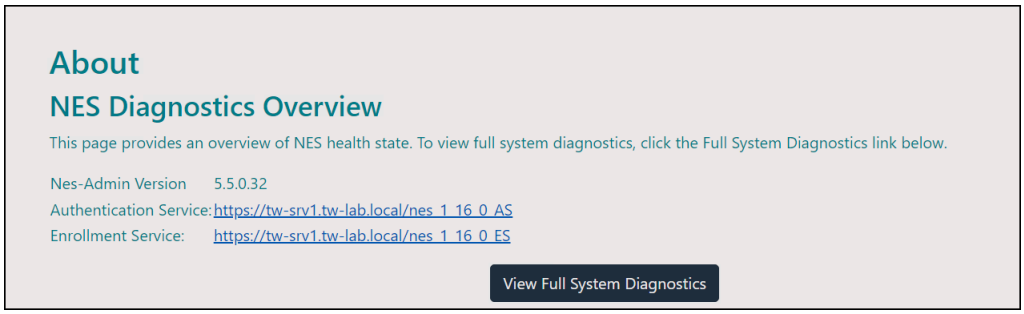


Figure 6: NES About Page

Fault code appears on the Nymi Band

When a Nymi Band experiences an issue from which it cannot automatically recover, a fault condition appears on the Nymi Band screen.

The following figure provide an example of the Nymi Band screen with a fault condition.

Figure 7: Nymi Band Screen with a Fault Condition

A fault condition contains two parts on two separate lines:

- Hexidecimal fault code
- Decimal condition line number

If a fault condition appears on the Nymi Band, in many cases you can recover the Nymi Band by performing the following step:

- Put the Nymi Band on the charger.
- Press and hold the top button for about 10-15 seconds.

If you can recover the Nymi Band, the screen goes black, and then the boot sequence messages appear.

The following table provides you with information about the meaning of each fault code and the next step action.

Table 2: Nymi Band Fault Codes

Fault Code	Meaning	Action
Starts with 0x110	Issue with the bootloader	RMA
0xD001D	Issue with the fingerprint matching algorithm	Restart*
0xD0015	Fingerprint camera failure	Create an RMA Support ticket
0xD000B	Recalibration required	Restart*
0xD0009	Error with fingerprint sensor	Restart*
Starts with 0xB000	Internal error	Restart*

Fault Code	Meaning	Action
0x60001	Internal failure	Create an RMA Support ticket
0x60002 0x60003	Hardware Abstraction Layer(HAL) error	Restart*
0x6000D	Nymi Band battery level is critically low	See *Nymi Band Does Not Charge / Fault 6000D Appears*
0x80002	Internal Serial Peripheral Interface(SPI) flash error	Restart*
0x80003	Internal SPI flash failure	Create an RMA Support ticket
0x90005	Damaged inertial measurement unit (IMU)	Create an RMA Support ticket
0x00001 0x00008 0x00013	Core error	Restart*
0xE0001	On-Body Detection(OBD) failure	Create an RMA Support ticket
0xE0003 0xE0007	OBD error	Restart*
0x140001	Memory failure	Create an RMA Support ticket
0x140005 0x190003 0x19000B	Out of memory	Restart*

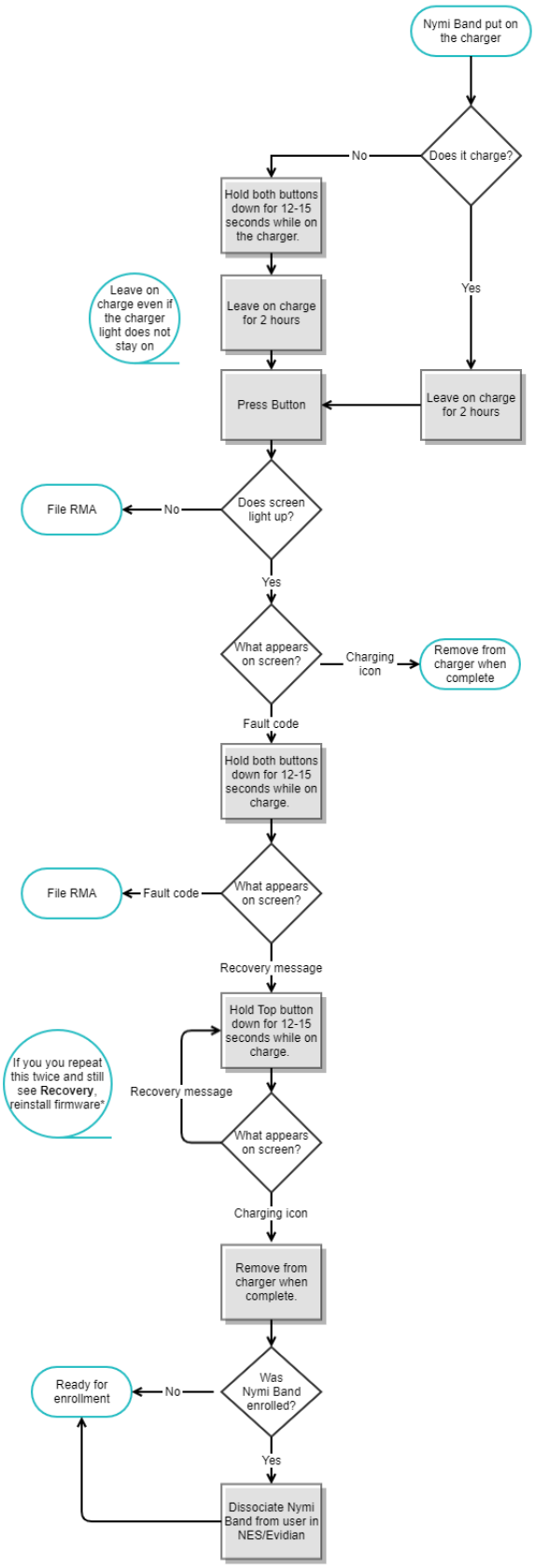
*If a restart does not resolve the issue for a particular fault code, provide the Nymi Band that is not working to your inventory manager, and contact Nymi Customer Support.

Nymi Band Does Not Charge/Fault Code 6000D Appears

When the battery level of a Nymi Band has reached a critically low level, for example, when it has been off charge for a long period of time, you might observe the following behaviour:

- When you put the Nymi Band on the charger, the Nymi Band screen flickers and the charging light on the charging cradle lights up then turns off.
- The Nymi Band screen displays a fault code that starts with 6000D.

Perform the steps in the following flowchart to recover the Nymi Band.


Nymi Band put on the charger
Does it charge?
No
Yes
Hold both buttons down for 12-15 seconds while on the charger.
Leave on charge for 2 hours
Leave on charge even if the charger light does not stay on
Leave on charge for 2 hours
Press Button
Does screen light up?
No
File RMA
Yes
What appears on screen?
Charging icon
Remove from charger when complete
Fault code
Hold both buttons down for 12-15 seconds while on charge.
What appears on screen?
Fault code
File RMA
Recovery message
Hold Top button down for 12-15 seconds while on charge.
If you you repeat this twice and still see Recovery, reinstall firmware*
Recovery message
What appears on screen?
Charging icon
Remove from charger when complete.
Was Nymi Band enrolled?
No
Ready for enrollment
Yes
Dissociate Nymi Band from user in NES/Evidian

*Refer to *Nymi Connected Worker Platform—Deployment Guide* for information about how to reinstall the Nymi Band firmware.

If the results of your workflow indicate that you should file an Return Merchandise Authorization(RMA) request, provide the Nymi Band that is not working to your inventory manager, and contact Nymi Customer Support.

Troubleshooting Nymi Band 3.0 issues

This section provides information about the errors and issues that you might encounter with the Nymi Band.

Determining the Firmware Version on Nymi Band 3.0

When troubleshooting an issue, you might require the Nymi Band firmware version. Perform the following steps to determine the firmware version on a Nymi Band.

About this task

This procedure requires you to use the Nymi Band charging cable to put the Nymi Band on charge.

Procedure

1. Remove the Nymi Band from the wrist of the user.
2. Put the Nymi Band on the charger.
3. Press and release the top and bottom button.
   The firmware version appears on the screen, as shown in the following figure.

Figure 8: Nymi Band firmware version

Nymi Band Buttons Not Working

While on charge, the Nymi Band does not perform the function associated with the button press.

For example, when you press the bottom button, the Delete User Data progress bar appears, does not proceed and then disappears.

Cause

The Firmware Updater script is running on a machine that is close to the Nymi Band and has established communication with the Nymi Band over blue tooth.

Resolution

Close the Firmware Updater script window on the machine that is running the script or move the Nymi Band to another computer that is out of Bluetooth range.

RECOVERY appears on the Nymi Band 3.0

When you wake a Nymi Band by pressing a button, the screen displays RECOVERY

Recovery firmware is pre-loaded read-only firmware version on all Nymi Bands that you cannot delete or change.

Cause

A Nymi Band goes into in the following conditions:

- Bootloader has encountered a problem with the standard firmware on the Nymi Band and switches to recovery firmware.
- A user put the Nymi Band on a charger and held the top and bottom buttons down for 20 seconds or more.

Resolution

To bring a Nymi Band out of recovery mode:

1. Put the Nymi Band on a charger.
2. Hold the top button on the Nymi Band down for at least 10 seconds, until you see the boot sequence messages appear on the screen.

When a Nymi Band enters recovery mode, the Nymi Band performs a delete user data operation. If the Nymi Band was enrolled prior to going into recovery mode, you must disassociate the Nymi Band from the user in NES (and the Evidian EAM Controller), and then instruct the user to enroll the Nymi Band again.

(Nymi Band 3.0) Authentication Failures

When authentication of the Nymi Band fails, the Nymi Band vibrates and displays a message.

Note: The Nymi Band does not vibrate if the **`Haptic Feedback on Nymi Bands`** is not enabled for the user or active group policy.

Nymi Band authentication failures occur for one of the following reasons:

- Fingerprint matching failure—when the authentication fails as a result of a fingerprint mismatch, the Nymi Band vibrates and displays a **NO MATCH** image about 1 second after the user places their finger on the fingerprint sensor and bezel. When the Nymi Band screen displays the fingerprint icon, the user can retry authentication. The message that appears on the Nymi Band screen when there are subsequent authentication failures due to fingerprint depends on the number of consecutive failures:
  - When there are less than 4 consecutive fingerprint match failures, the **NO MATCH** image appears.
  - When there are more than 3 consecutive fingerprint match failures, the Nymi Band displays a message that provides advice that can result in a successful authentication. Possible messages include **CENTER FINGER**, **WASH & DRY HAND & WRIST**, and **CLEAN BAND**.
- Liveness failure—when the authentication fails due to the inability to detect a consistent ECG signal on the wrist, the Nymi Band vibrates and displays the **NO ECG** message about 13 seconds after the user places their finger on the fingerprint sensor and bezel. When the Nymi Band screen displays the fingerprint icon, the user can retry authentication. The message that appears on the Nymi Band screen when there are subsequent authentication failures due to liveness detection issues depends on the number of consecutive failures:
  - When there are less than 4 consecutive fingerprint match failures, the **No ECG** message appears.
  - When there are more than 3 consecutive fingerprint match failures, the Nymi Band displays a message that provides advice that can result in a successful authentication. Possible messages include **SIT STLL**, **WASH & DRY HAND & WRIST**, and **DON'T MOVE**.

Troubleshooting Fingerprint Mismatch Failures

If the fingerprint authentication fails, review the following information to resolve the issue.

Ensure that:

- Fingerprint sensor is clean and dry.
  - If the fingerprint sensor is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
  - If the fingerprint sensor is wet, dry completely with a lint-free towel, and then retry authentication.
- User does not press too hard or too soft on the fingerprint sensor.
- User’s finger is clean and dry.
  - If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication.

    - If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
    - If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication.
- User places their finger on the centre of the sensor, touching the surrounding bezel.
- User keeps their finger still on the sensor and bezel during the authentication period.
- User does not lift their finger off the sensor or bezel until the authentication process completes.
- User wears the Nymi Band snugly on the wrist.
- User wears their own Nymi Band.
- User attempts authentication with the same the finger that they used during enrollment.
- User finger is not damaged, for example the user has cut their finger.

  Note: If the finger that is used for authentication is damaged, consider one of the following actions:

  - Instruct the user to authenticate by corporate credentials until the finger heals.
  - Delete the user data on the Nymi Band, and then perform re-enrollment with a different finger.

(Nymi Band 3.0 only) Troubleshooting Liveness Detection Failures

If the liveness detection fails, review the following information to resolve the issue.

Ensure that:

- Bottom sensor is clean and dry.
  - If the bottom electrode is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
  - If the bottom electrode is wet, dry completely with a lint-free towel, and then retry authentication.
- User’s finger is clean and dry.
  - If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication
  - If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
  - If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication.
- User keeps their finger still on the sensor and bezel during the authentication period.
- User's wrist is not too dry. Before authentication, wash and completely dry the wrist before putting on the Nymi Band, or rub some lotion well into the wrist, and then retry authentication.
- Nymi Band bottom electrode remains in contact with the wrist during the authentication period. If the position of bottom electrode prevents contact, remove the Nymi Band, reposition the Nymi Band on the wrist, and then try authentication again.

- User does not lift their finger off the sensor or bezel until the authentication process completes.
- Nymi Band fits snugly on the wrist and does not move around during the authentication process.
- User's wrist is not tattooed where the bottom sensor makes contact.

  Note: If the user cannot use another wrist or the Nymi Band cannot make contact with an area that is not tattooed, instruct the user to authenticate by corporate credentials.

Troubleshooting Persistent Authentication Failures (Lockout)

Lockout policies help prevent adversarial users from gaining unauthorized access to systems through brute-force attacks.

When an authentication lockout occurs, the Nymi Band displays the **See Admin** icon and prevent the user from performing additional authentication attempts. An authentication lockout occurs in the following scenarios:

- After 50 consecutive failed authentication attempts on a previously enrolled Nymi Band due to a fingerprint mismatch.
- After 3 consecutive failed attempts to complete the fingerprint template during the enrollment due to an issue with the fingerprint imaging.

The lockout persists on the Nymi Band, even if the user removes the Nymi Band. The lockout will also persist while the Nymi Band is dead or while charging.

Clear the lockout by one of the following methods:

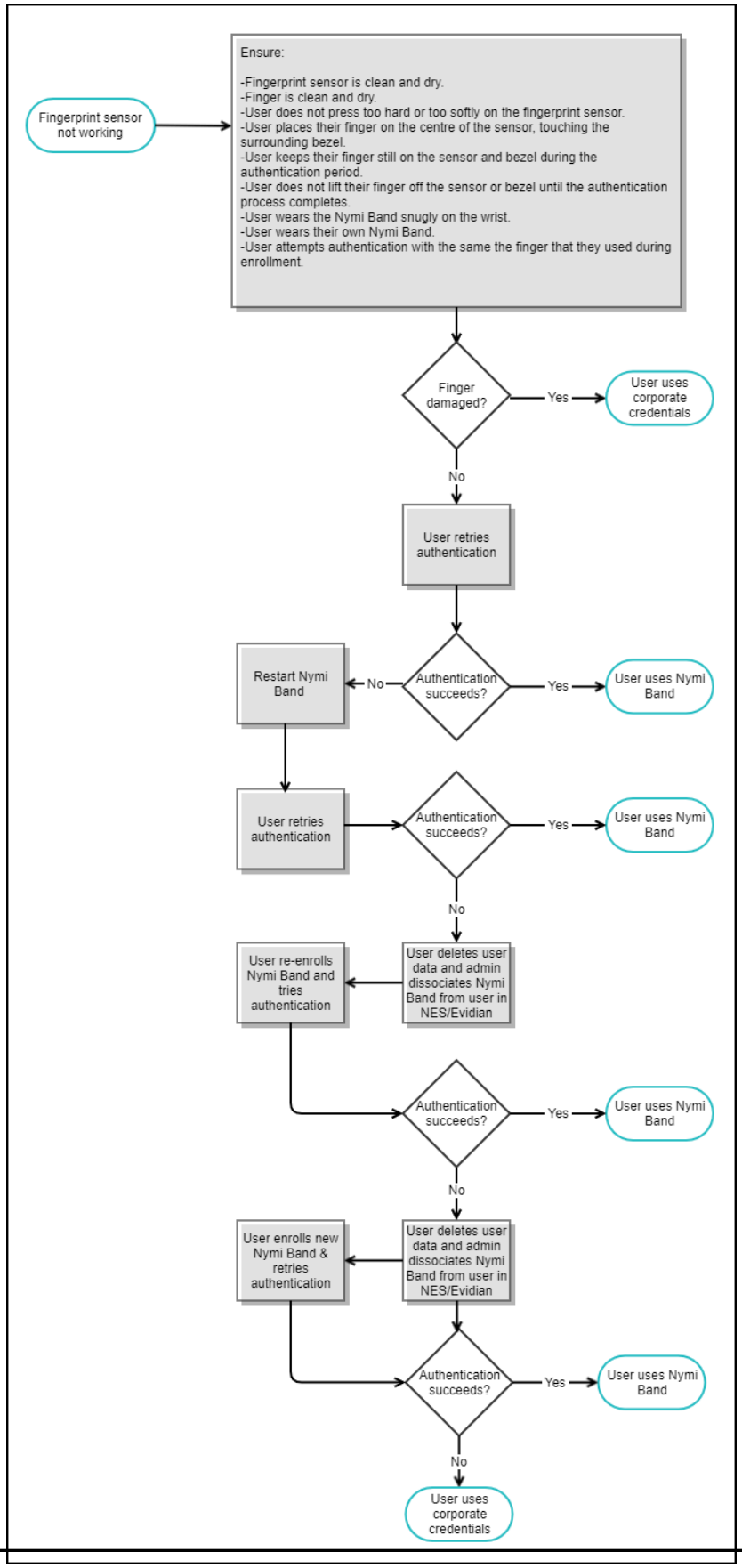
- Re-enroll the user to the Nymi Band.
- Authenticate the user with their credentials in the Nymi Band Application. A user can authenticate by using corporate credentials only if the **`Corporate Credentials Authentication`** option was enabled in the Nymi Enterprise Server(NES policy at the time of enrollment.

If the user persistently cannot authenticate to the Nymi Band, consider the following actions:

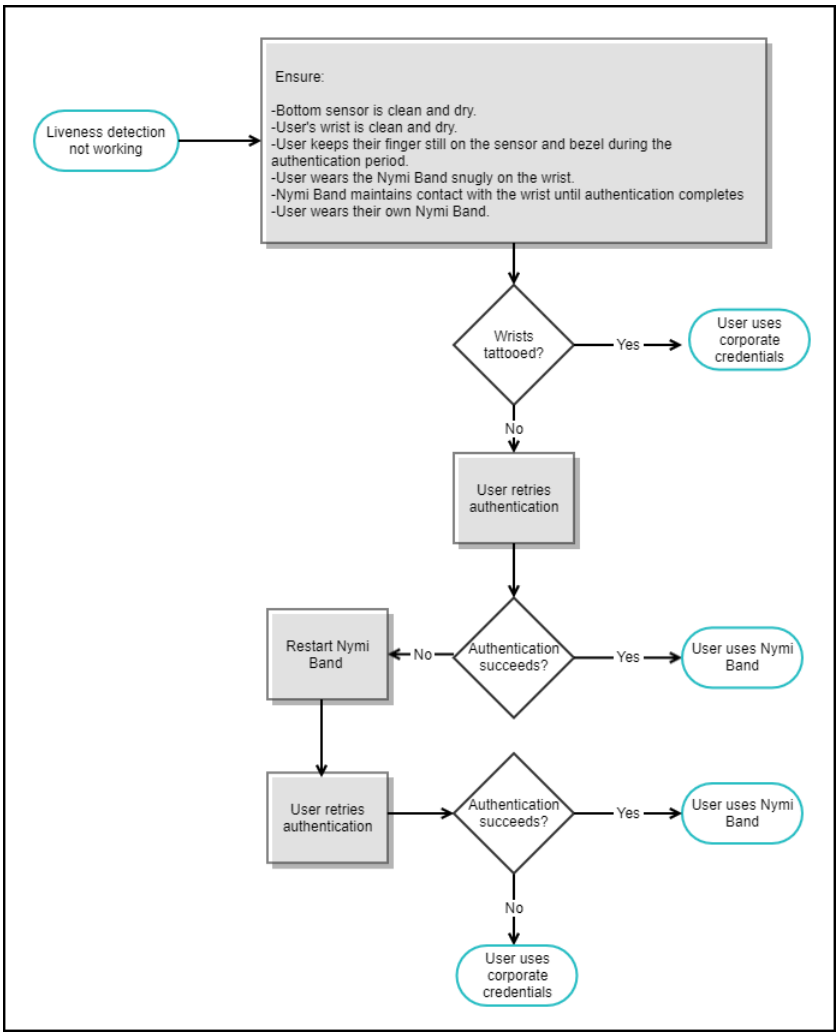
- Restart the Nymi Band and retry authentication.
- Instruct the user to log into the Nymi Band Application while wearing the Nymi Band and authenticate by corporate credentials.
- Delete the user data from the Nymi Band and then disassociate the Nymi Band from the user in NES and Evidian (if used), and then enroll with a different finger.
- Delete the user data from the Nymi Band, disassociate the Nymi Band from the user in NES and Evidian, and then enroll the user with a different Nymi Band.

(Nymi Band 3.0) Authentication Failure Workflow

Refer to the following diagram to troubleshoot persistent fingerprint authentication failures.


Fingerprint sensor not working
Ensure:
-Fingerprint sensor is clean and dry.
-Finger is clean and dry.
-User does not press too hard or too softly on the fingerprint sensor.
-User places their finger on the centre of the sensor, touching the surrounding bezel.
-User keeps their finger still on the sensor and bezel during the authentication period.
-User does not lift their finger off the sensor or bezel until the authentication process completes.
-User wears the Nymi Band snugly on the wrist.
-User wears their own Nymi Band.
-User attempts authentication with the same the finger that they used during enrollment.
Finger damaged?
Yes
User uses corporate credentials
No
User retries authentication
Authentication succeeds?
No
Restart Nymi Band
Yes
User uses Nymi Band
User retries authentication
Authentication succeeds?
Yes
User uses Nymi Band
No
User deletes user data and admin dissociates Nymi Band from user in NES/Evidian
User re-enrolls Nymi Band and tries authentication
Authentication succeeds?
Yes
User uses Nymi Band
No
User deletes user data and admin dissociates Nymi Band from user in NES/Evidian
User enrolls new Nymi Band & retries authentication
Authentication succeeds?
Yes
User uses Nymi Band
No
User uses corporate credentials

Refer to the following diagram to troubleshoot persistent liveness detection failures.



(Nymi Band 3.0) Cannot Disable Liveness Detection

The Liveness Detection option has been disabled in the active group policy or a user has been assigned to an individual user policy with the liveness detection option disabled, but the Nymi Band continues to check for liveness during authentication.

Cause

A Nymi Band continues to check for liveness during authentication for the following reasons:

The user enrolled the Nymi Band prior to the policy change but did not log into the Nymi Band Application while wearing their authenticated Nymi Band to download the change.

The firmware on the Nymi Band does not support disabling liveness detection.

Resolution

Perform the following steps to resolve the issue:

- Check the firmware version on the Nymi Band. If the Nymi Band uses firmware prior to CWP 1.1, update the firmware on the Nymi Band, and then re-enroll the user to the Nymi Band.
- If the Nymi Band firmware is CWP 1.1 or later, instruct the user to authenticate to their Nymi Band, and then log into the Nymi Band Application. The Nymi Band Application applies the settings to the Nymi Band.

(Nymi Band 3.0) Downgrading the Firmware

Downgrading of the Nymi Band firmware is not advised unless under the recommendation of Nymi Support.

Perform the following steps to downgrade the firmware on a Nymi Band.

Note: When you downgrade the firmware on a Nymi Band, a delete user data operation occurs.

1. If the Nymi Band is enrolled, disassociate the user from the Nymi Band in NES and EAM.
2. Place the Nymi Band on a charger.
3. Hold the top and bottom buttons down for at least 20 seconds, until the boot sequence messages display *recovering*.
4. When the Nymi Band screen displays **RECOVERY**, run the firmware updater script to install the firmware.
5. If the Nymi Band was enrolled to a user, instruct the user to enroll to the Nymi Band.

Dead Nymi Band 3.0

If the screen is blank on the Nymi Band and pressing any button does not wake it up, charge the Nymi Band.

Broken Nymi Band

If a Nymi Band is physically broken, for example, the screen breaks, replace the Nymi Band with a new Nymi Band.

See *Issuing a temporary Nymi Band to a user* in the *Nymi Connected Worker Platform—Administration Guide* for information about how to deactivate the existing Nymi Band for a user, and then assign a new Nymi Band to the user.

Note: Provide the Nymi Band that is not working to your inventory manager for disposal.

Lost Nymi Band

If a user loses their Nymi Band, deactivate the Nymi Band in the NES Administrator Console, and then assign a new Nymi Band to the user.

See *Issuing a temporary Nymi Band to a user* in the *Nymi Connected Worker Platform—Administration Guide* for information.

Troubleshooting Nymi Band 4.0 issues

This section provides information about the errors and issues that you might encounter with the Nymi Band.

Determining the Firmware Version on Nymi Band 4.0

While you troubleshoot an issue, you might require the Nymi Band firmware version. Perform the following steps to determine the firmware version on a Nymi Band.

Procedure

1. Remove the Nymi Band from the wrist of the user.
2. Put the Nymi Band on the charger.
3. Tap your finger on the fingerprint sensor 3 times.
   The firmware version appears on the screen, as shown in the following figure.

Figure 9: Nymi Band firmware version

(Nymi Band 4.0) Authentication Failures

When authentication of the Nymi Band fails, the Nymi Band vibrates and displays a message.

Note: The Nymi Band does not vibrate if the **`Haptic Feedback on Nymi Bands`** is not enabled for the user or active group policy.

Nymi Band authentication failures occur when the fingerprint placed on the fingerprint sensor does match the fingerprint template on the Nymi Band. When the authentication fails, the Nymi Band vibrates and displays a **NO MATCH** image about 1 second after the user places their finger on the fingerprint sensor and bezel. When the Nymi Band screen displays the fingerprint icon, the user can retry authentication. The message that appears on the Nymi Band screen when there are subsequent authentication failures due to fingerprint depends on the number of consecutive failures:

- When there are less than 4 consecutive fingerprint match failures, the **NO MATCH** image appears.
- When there are more than 3 consecutive fingerprint match failures, the Nymi Band displays a message that provides advice that can result in a successful authentication. Possible messages include **CENTER FINGER**, **WASH & DRY HAND & WRIST**, and **CLEAN BAND**.

Troubleshooting Fingerprint Mismatch Failures

If the fingerprint authentication fails, review the following information to resolve the issue.

Ensure that:

- Fingerprint sensor is clean and dry.
  - If the fingerprint sensor is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
  - If the fingerprint sensor is wet, dry completely with a lint-free towel, and then retry authentication.
- User does not press too hard or too soft on the fingerprint sensor.
- User's finger is clean and dry.
  - If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication.
  - If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
  - If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication.
- User places their finger on the centre of the sensor, touching the surrounding bezel.
- User keeps their finger still on the sensor and bezel during the authentication period.
- User does not lift their finger off the sensor or bezel until the authentication process completes.
- User wears the Nymi Band snugly on the wrist.
- User wears their own Nymi Band.
- User attempts authentication with the same the finger that they used during enrollment.
- User finger is not damaged, for example the user has cut their finger.

  Note: If the finger that is used for authentication is damaged, consider one of the following actions:

  - Instruct the user to authenticate by corporate credentials until the finger heals.
  - Delete the user data on the Nymi Band, and then perform re-enrollment with a different finger.

Troubleshooting Persistent Authentication Failures (Lockout)

Lockout policies help prevent adversarial users from gaining unauthorized access to systems through brute-force attacks.

When an authentication lockout occurs, the Nymi Band displays the **See Admin** icon and prevent the user from performing additional authentication attempts. An authentication lockout occurs in the following scenarios:

- After 50 consecutive failed authentication attempts on a previously enrolled Nymi Band due to a fingerprint mismatch.
- After 3 consecutive failed attempts to complete the fingerprint template during the enrollment due to an issue with the fingerprint imaging.

The lockout persists on the Nymi Band, even if the user removes the Nymi Band. The lockout will also persist while the Nymi Band is dead or while charging.

Clear the lockout by one of the following methods:

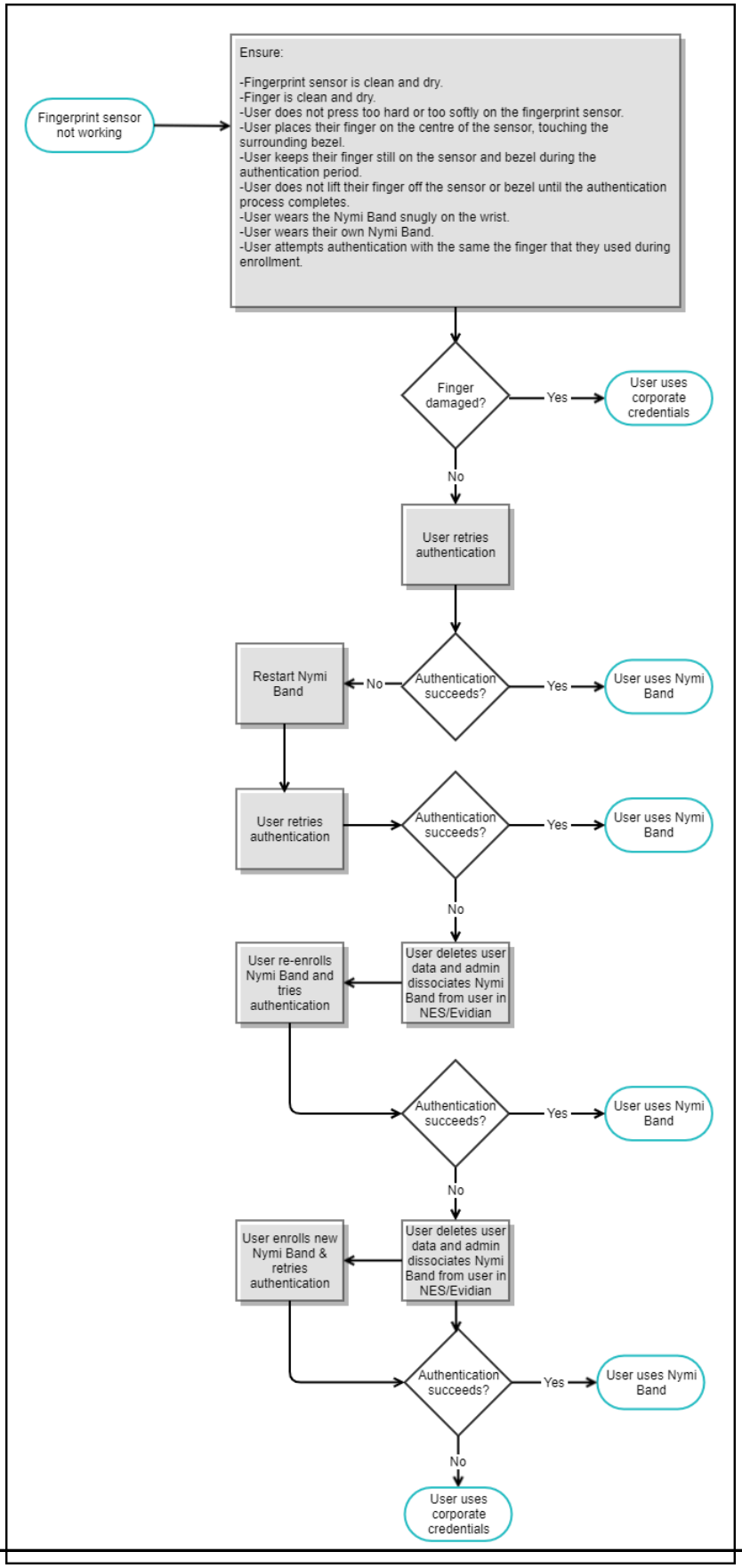
- Re-enroll the user to the Nymi Band.
- Authenticate the user with their credentials in the Nymi Band Application. A user can authenticate by using corporate credentials only if the **`Corporate Credentials Authentication`** option was enabled in the Nymi Enterprise Server(NES policy at the time of enrollment.

If the user persistently cannot authenticate to the Nymi Band, consider the following actions:

- Restart the Nymi Band and retry authentication.
- Instruct the user to log into the Nymi Band Application while wearing the Nymi Band and authenticate by corporate credentials.
- Delete the user data from the Nymi Band and then disassociate the Nymi Band from the user in NES and Evidian (if used), and then enroll with a different finger.
- Delete the user data from the Nymi Band, disassociate the Nymi Band from the user in NES and Evidian, and then enroll the user with a different Nymi Band.

(Nymi Band 4.0) Authentication Failure Workflows

Refer to the following diagram to troubleshoot persistent fingerprint authentication failures.


Fingerprint sensor not working
Ensure:
-Fingerprint sensor is clean and dry.
-Finger is clean and dry.
-User does not press too hard or too softly on the fingerprint sensor.
-User places their finger on the centre of the sensor, touching the surrounding bezel.
-User keeps their finger still on the sensor and bezel during the authentication period.
-User does not lift their finger off the sensor or bezel until the authentication process completes.
-User wears the Nymi Band snugly on the wrist.
-User wears their own Nymi Band.
-User attempts authentication with the same the finger that they used during enrollment.
Finger damaged?
Yes
User uses corporate credentials
No
User retries authentication
Authentication succeeds?
No
Restart Nymi Band
Yes
User uses Nymi Band
User retries authentication
Authentication succeeds?
Yes
User uses Nymi Band
No
User deletes user data and admin dissociates Nymi Band from user in NES/Evidian
User re-enrolls Nymi Band and tries authentication
Authentication succeeds?
Yes
User uses Nymi Band
No
User deletes user data and admin dissociates Nymi Band from user in NES/Evidian
User enrolls new Nymi Band & retries authentication
Authentication succeeds?
Yes
User uses Nymi Band
No
User uses corporate credentials

RECOVERY appears on the Nymi Band 4.0

When you wake a Nymi Band by pressing a button, the screen displays RECOVERY

Recovery firmware is pre-loaded read-only firmware version on all Nymi Bands that you cannot delete or change.

Cause

A Nymi Band goes into in the following conditions:

- Bootloader has encountered a problem with the standard firmware on the Nymi Band and switches to recovery firmware.
- A user put the Nymi Band on a charger and held the charger button down for 10 seconds or more.

Resolution

To bring a Nymi Band out of recovery mode:

1. Put the Nymi Band on charge.

   Note: Use a standalone charger and not a PowerHouse.
2. Hold the button on the charger down for at least 10 seconds, until you see the boot sequence messages appear on the Nymi Band screen.

When a Nymi Band enters recovery mode, the Nymi Band performs a delete user data operation. If the Nymi Band was enrolled prior to going into recovery mode, you must disassociate the Nymi Band from the user in NES (and the Evidian EAM Controller), and then instruct the user to enroll the Nymi Band again.

(Nymi Band 4.0) Downgrading the Firmware

Downgrading of the Nymi Band firmware is not advised unless under the recommendation of Nymi Support.

Perform the following steps to downgrade the firmware on a Nymi Band.

Note: When you downgrade the firmware on a Nymi Band, a delete user data operation occurs.

1. If the Nymi Band is enrolled, disassociate the user from the Nymi Band in NES and EAM.
2. Place the Nymi Band on a charger.

3. Hold the buttons down on the charger for at least 20 seconds, until the boot sequence messages display *recovering*.
4. When the Nymi Band screen displays **RECOVERY**, run the firmware updater script to install the firmware.
5. If the Nymi Band was enrolled to a user, instruct the user to enroll to the Nymi Band.

Dead Nymi Band 4.0

If the screen is blank on the Nymi Band and touching the fingerprint sensor does not wake it up, charge the Nymi Band.

Broken Nymi Band

If a Nymi Band is physically broken, for example, the screen breaks, replace the Nymi Band with a new Nymi Band.

See *Issuing a temporary Nymi Band to a user* in the *Nymi Connected Worker Platform—Administration Guide* for information about how to deactivate the existing Nymi Band for a user, and then assign a new Nymi Band to the user.

Note: Provide the Nymi Band that is not working to your inventory manager for disposal.

Lost Nymi Band

If a user loses their Nymi Band, deactivate the Nymi Band in the NES Administrator Console, and then assign a new Nymi Band to the user.

See *Issuing a temporary Nymi Band to a user* in the *Nymi Connected Worker Platform—Administration Guide* for information.

Troubleshooting Nymi Band Tap Issues

Review this section for information about how to resolve related to Nymi Band 3.0 and Nymi Band 4.0 taps on an NFC reader or the Bluetooth Adapter..

User Cannot Complete Authentication Tasks with the Nymi Band

When a user performs a Nymi Band tap in a Nymi-enabled Application(NEA), the authentication task does not complete.

The following messages appear in the *nymi_api.log* file:

```
INFO - Successfully got an NEA certificate from server.
INFO - Successfully stored NEA certificate.
ERROR - NSL: nsl_verify_nea_cert_chain, 2238, 14
ERROR - Error: ErrorWithMessage { error: MissingCerts, specifics: "NEA certificate chain is missing or invalid." }
INFO - sending update to nea {"operation":"init","exchange":"0","status":8000,"payload":{},"error":{"error_description":"NEA missing certificates.","error_specifics":"NEA certificate chain is missing or invalid."}}
```

Cause

Nymi issues two types of L2 certificates, a gold version (for Production customers) and a bronze version (for internal development and troubleshooting). Nymi creates separate components for each certificate type.

Error number 14, which appears in the first error message in the *nymi_api.log* file indicates that there is a mismatch between the version of a Nymi component and the L2 certificate that Nymi Enterprise Server(NES) uses.

Resolution

Contact Nymi to confirm that each component (NES, Nymi SDK, and the Nymi Band Application) is appropriate for the L2 certificate that Nymi issued for NES.

Nymi Band Tap Not Detected

In a Citrix/RDP session, when a user performs a Nymi Band tap, the Nymi-Enabled Application(NEA) does not detect the tap.

Cause

The user terminal has multiple network adapters and the network connection has switched from one network adapter to another.

In this situation, the *nymi_blueooth_endpoint.log* files does not report the error Nymi Bluetooth Endpoint is missing and also displays messages that show that the Nymi Bluetooth Endpoint reconnects to the Nymi Agent and the subscribes to a topic with a different IP address.

Resolution

Log out (not just disconnect) of the current Citrix / RDP session, and then relaunch the session, which starts a new application session and triggers Nymi API to start and subscribe to the new IP address.

Troubleshooting Deployment Error Messages

The following section provides a list of the error messages that you might encounter during deployment, and how to resolve the issues.

NES system issues after IIS removal

During NES installation, if you remove IIS and then reinstall, but do not perform a restart after the removal, the NES system may experience performance issues.

Users should follow the system warnings and perform the restart.

NES Installation Messages

The following errors may appear during the NES installation:

Message	Description	Troubleshooting
Invalid or corrupt Installation Media	Something is wrong with the installation source	Make sure all files contained in the zipped file are extracted.
IIS Error	IIS, Web Management Tools, or some of their required components are not installed properly	Add the missing components to IIS.
Domain Error : This Installer Must be Run under a Domain Account	You are not logged into the domain	Logout from the machine, then log in with valid domain user credentials.
One or more Mandatory Dependencies Failed to Install	Installer failed to install a required dependency	See the log files and report the error to Nymi Support.
One or more Prerequisites has FAILED	Not all required prerequisites are met	Refer to the Nymi Connected Worker Platform—Deployment Guide.
Error Installing Optional Dependency	Installer failed to install an optional dependency	See the log files and report the error to your Nymi Solution Consultant.
Corrupt Installation Found	A corrupt installation found	Physically delete the destination files or select another Instance Name.

Message	Description	Troubleshooting
Cannot Install	Cannot install with current settings	Review your settings.
Certificate Error - Password required	Certificate is protected by password	Supply password.
Certificate Error - Password required	Certificate failed to install	See error message and correct.
Cannot Install at this time	One or more errors are preventing installation	Check all errors and settings, correct, and try again.
Cannot Update at this time	One or more errors are preventing update	Check all errors and settings, correct, and try again.
Cannot Apply Settings at this time	One or more Errors are preventing application of settings	Check all errors and settings, correct, and try again.
Cannot Access [Directory] You can try to remove it Manually	Could Not backup a directory/ file at the destination folder due to permissions	Make sure that no other application is in the files/directory at destination folder, and try again.
IIS Service Restart FAIL	Failed to start/restart IIS Service	Manually start/restart the IIS Service.
Installation FAIL	The Application Pool Identity is set to LocalService on the IIS Window	Change the value from LocalService to another value (such as LocalSystem). Check the Review Settings Window for errors and if none are present, proceed to the Install Window.
Installation FAIL	Installation failed due to one or more errors	Check all errors and logs.

NES Silent Installation Messages

The following errors may appear during the NES installation:

Message	Description	Troubleshooting
Error setting Parameter [X] to [Y}	The parameter in the installer configuration file doesn't exist or has an illegal value.	Check the installer configuration file for errors, manually or with the graphical user interface version.
Error parsing Parameters	There is a possible syntax error in the installer configuration file.	Check the installer configuration file for errors, manually or with the graphical user interface version.
Error parsing Command Line	There is a possible syntax error in the command line.	Check command line syntax.

Message	Description	Troubleshooting
Operation Timed Out	The current operation timed out.	Specific to operation.
Error loading configuration File	Could not load installer configuration file.	Check that the installer configuration file exists in the given location.
No Instance Name Given	isInstanceName parameter is missing from the installer configuration file.	Add the missing parameter to the installer configuration file.
Error Validating Settings	Some settings have errors or could not validated.	Check the installer configuration file for errors, manually or with the graphical user interface version.
Error Updating Existing Installation	Updating existing installation failed.	Check all errors and logs.
Error Fresh Installing	New installation failed.	Check all errors and logs.
Cannot Install with this Configuration	Something is preventing the attempted Install.	Check all errors and logs.

NES Pre-requisite Check Fails With IIS Components Missing Error Message

NES installer pre-requisite check fails with the following error message:

IIS Installation FAILED: The Following IIS Components are missing: ISAPI Extensions, ISAPI Filters, ASP .NET (.NET Framework 4.7), ISAPI Extensions Binaries, ISAPI Filter Binaries.

Cause

ASP.NET was not installed.

Resolution

Install ASP.NET by performing the following steps:

1. From `Server Manager`, select **`Add Roles and Services`**.
2. Click **`Next`** until you reach the `Server Roles` screen.
3. Expand **`Web Server(IIS) > Web Server > Application Development`** and then select the latest version of ASP.NET.
4. Continue through the windows and complete the installation.
5. Retry the NES installation.

Organization Unit Error Messages

The following errors messages might appear when you specify an Organizational Unit on the Enterprise page of the NES installer.

Message	Cause	Resolution
Error: *ou_name* is not found on any of the domains	This error appears after you specify an OU and click **Test** because the OU does not exist in any of the domains that you specified in the **Domains** table.	To resolve this issue, perform one of the following actions: • Confirm that you correctly spelled the OU name. • Confirm that the OU appears in a domain that is in the Domains table, and your test of the domain entries does not return an error. • Confirm that the domain in which the OU resides is trusted by the domain in which the NES server resides.
Error: *ou_name* Multiple instances of the same OU name appear in the directory. Type the full DN of the OU instead.	This error appears after you specify an OU and click **Test** because the same OU name appears in more than once in the directory.	To resolve this issue, review the error message, which displays the distinguished name (DN) of each instance of the OU name that was found, and then specify the correct DN in the **NES API Authorization based on Organization Unit** table.

Failed to Initialize Database

The error message "Failed to Initialize Database" appears in the NES Setup wizard after you click **Install**.

The following figure shows this error message.

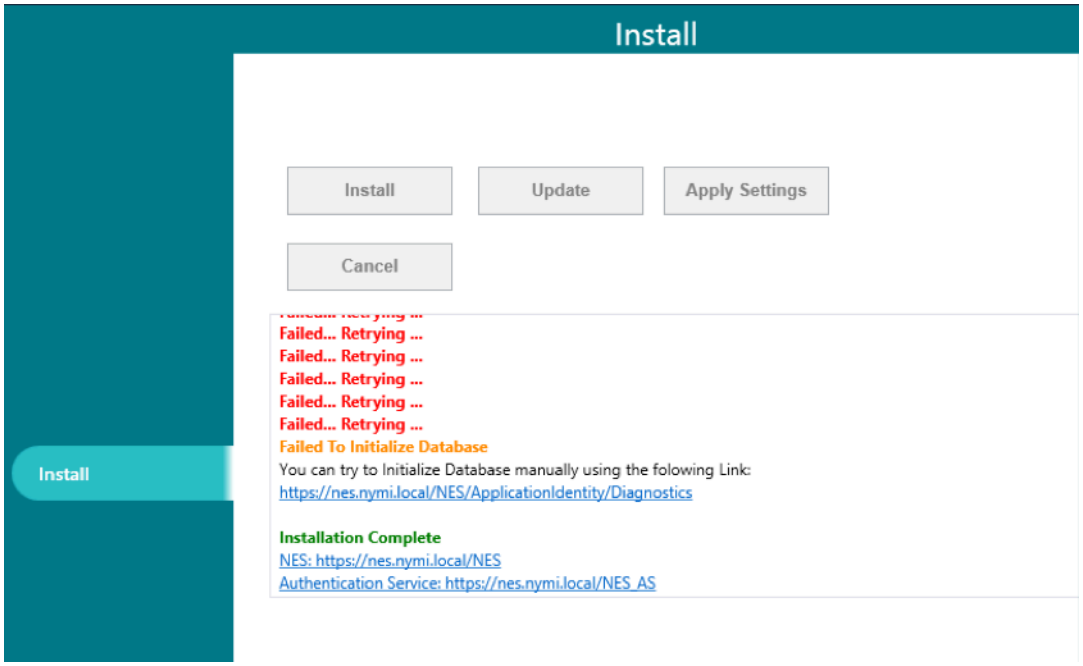


Figure 10: Failed to initialize the database

Cause

This error message appears when IIS was installed without ASP.NET 4.x.

Resolution

Install ASP.NET 4.8. The *Nymi Connected Worker Platform—Deployment Guide* describes how to install ASP .NET.

Failed Connecting to Server

The error message "Failed Connecting to Server" appears in the NES Setup wizard on the **`Database`** page after you configure the connection string for a remote SQL server, and then click **`Test`**.

Additionally, when you click **`Verify Users`**, the results also display an error. The following figure shows this error message.

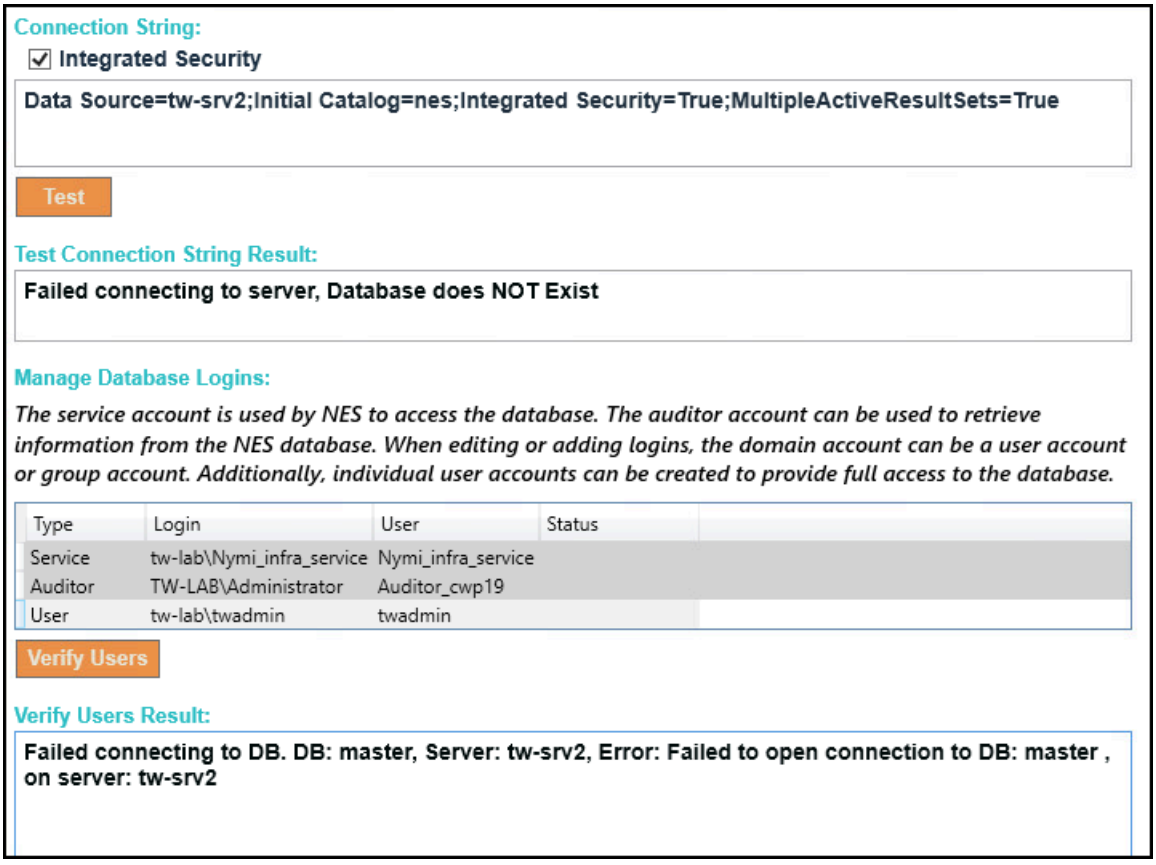


Figure 11: Failed to initialize the database

Cause

This error message appears when port 1433 is not open between the remote SQL server and the NES server.

Resolution

Open port 1433 bidirectionally between the NES and SQL servers.

SQL Server Network Interfaces, error 26;-Error Locating Server/Instance Specified

The following error message appears on the `Database` window of the NES Setup wizard:

Wait! Loading…. Error: A network-related or instance-specific error occurred while established a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that the SQL Server is configured to allow remote connections. (provider: SQL Network Interfaces, error: 26 - Error Locating Server/Instance Specified.)

Cause

NES is deployed on a Domain Controller.

Resolution

Configure NES on a machine that is not a Windows Domain Controller.

SQL Hardening Permissions Errors in SSMS

The following error message appears while creating a new Column Master key in SQL Server Management Studio (SSMS) while following steps to harden the NES Database.

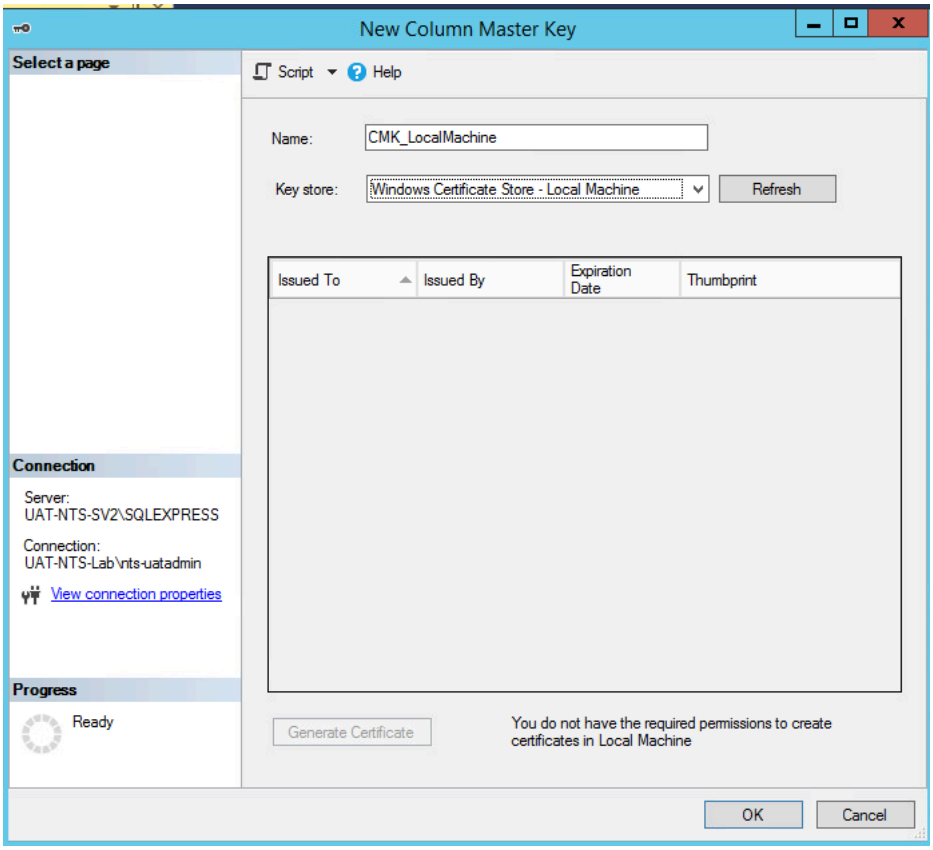


Figure 12: Permission Error in SSMS

Cause

SSMS was not run as an administrator.

Resolution

Close SSMS, and open as an administrator.

SQL Server Service Fails to Start

The MS SQL Service fails to start and the following error messages appear in the System Event Viewer log:

Schannel error in the system event log : A fatal error occurred while creating a TLS client credential. The internal error state is 10013. SQL error in the system event log: A fatal error occurred while creating a TLS client credential. The internal error code is 7024.

Cause

This error message appears you disable TLS 1.0 on the NES server and the version of MS SQL Server does not support TLS 1.2.

Resolution

To resolve this issue, perform the following steps to install a version of MS SQL server that supports TLS 1.2 and preserve the information in the NES database.

1. Enable TLS 1.0 and disable TLS 1.2.
2. Start the MS SQL Server service.
3. Install SQL Server Management Studio (ssms).
4. Download SQL Express 2017 SP1 or later.
5. Perform the following actions to backup the NES database.
    a. Connect to `IIS Manager` and stop IIS.
    b. Launch ,and then connect to the SQL instance.
    c. Expand **`Databases`**.
    d. Right-click the Nymi.nes database and then select **`Tasks > Back up`**. NOTE: If your database name is not Nymi.nes, select the name that appears in your env.
    e. From the **`Backup type`** list, select **`Full`**. Make note of the destination directory.
    f. Click **`OK`**.
    g. Start IIS.
6. Remove SQL Express 2012.
7. Restart the NES server.
8. Install SQL Express 2017.
9. Perform the following steps to restore the NES database.
    a. Run SSMS and then connect to the SQL instance.
    b. Right-click **`Databases`** and then select **`Restore Database`**.
    c. In the left navigation pane of the `Restore Database` window, click **`Options`**.
    d. Select **`Overwrite existing database (WITH REPLACE)`**.
    e. In the left navigation pane click **`General`**.
    f. In the **`Source`** section, select **`Device`** and then click the Elispses (...).
    g. On the `Select backup devices` window, click **`Add`**.
    h. Navigate to the *MSSQL11.SQLEXPRESS* subfolder and then expand **`MSSQL > Backup`**.
    i. Select the *Nymi.nes.bak* file and then click **`OK`**.
    j. On the `Select backup devices` window, click **`OK`**.
    k. Click **`Verify Backup Media`**. (no errors should appear)
    l. Click **`OK`**.
10. Perform the following steps to verify the NES database.
    a. Log into the NES Administrator Console and search for a user.

b. When the user appears, click the hypertext link and ensure that you can see the properties of the user.
c. On the **Policies** tab, edit your policy and confirm that the settings are correct.

11. Enable TLS 1.2 and confirm that NES can access the database

a. Disable TLS 1.0.
b. Enable TLS 1.2.
c. Ensure that SSL 3.0 is disabled.
d. Stop and restart the MS SQL Server service.
e. Log into the NES Administrator Console and search for a user.
f. When the user appears, click the hypertext link and ensure that you can see the properties of the user.

Failed to assign SPN on account 'CN=. …', error 0x21c7/847 # The operation failed /modification is not unique forest-wide

This message appears when you run the **setspn -S** command.

Cause

This error appears for one of the following reasons:

- The SPN already exists and is associated with a different user.
- The account that is running the SPN command does not have permission to create an SPN.

Resolution

Perform the following actions:

1. Type the following command to determine if the SPN exists: ***setspn -Q HTTP/%computername%***.
   - If an SPN is found, the output displays the details about the SPN.
   - If an SPN is not found, the output displays the message No Such SPN found.
2. If an SPN is found, type the following command to delete the existing SPN: setspn -d HTTP/%computername% `associated_user`, and the create the SPN.
3. If an SPN is not found, contact your Active Directory team to create the required SPNs.

Troubleshooting NES Administrator Console connection issues

This section provides information about the error messages that might appear while you log in to the NES Administrator Console.

The remote server returned an error (404) Not Found

This error message appears after you sign into NES Administrator Console.

Cause

Communications cannot be established with the authentication service. The following figure provides an example of the error message.

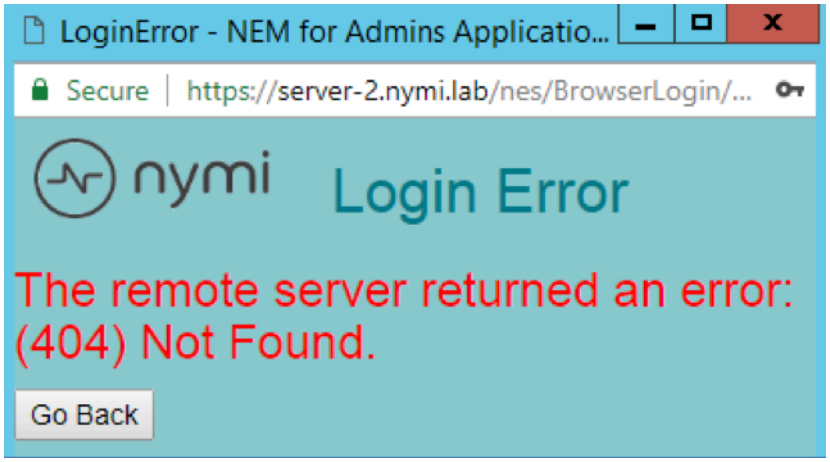


Figure 13: The remote server returned an error (404) Not Found

This issue appears when the NES Administrator Console cannot contact the Authentication Service because the Authentication Service URL is not correct, or the TLS certificate has expired.

Resolution

Perform the following actions to correct the URL in the NES configuration:

1. Log in to the NES host.
2. Edit the *C:\inetpub\nes\web.config* file.
3. Search for the string <setting name=”AuthenticationService”
4. Correct the URL in the associated <value> tag for the setting.
5. Save the *web.config* file.
6. Refresh the `System Diagnostics` page in the NES Administrator Console and confirm that the Authentication Service status is pass for applicable NES tests.

The required anti-forgery cookie "__RequestVerificationToken_L25lcw2" is not present

This error message appears after you sign into NES Administrator Console.

The following figure provides an example of the error message.

Figure 14: The required anti-forgery cookie "__RequestVerificationToken_L25lcw2" is not present

Cause

This error appears because NES server is configured to use HTTP connections.

Resolution

Perform the following actions to remove the requirement for anti-forgery cookies:

Note: Use Notepad++ or run Notepad as administrator to edit the files.

1. Create a backup copy of the following files:
   - *..\inetpub\wwwroot\nes\NES\Web.Config*
   - *..\inetpub\wwwroot\nes\NEnrollment\Web.Config*
   - *..\inetpub\wwwroot\nes\AuthenticationService\Web.Config*
2. Edit each *Web.Config* file, and then perform the following steps:
   a. Search for the string *httpCookies*
   b. Comment out the line *<httpCookies requireSSL="true" />*.

      For example ***<!-- <httpCookies requireSSL="true" /> -->***
   c. Save the file.
3. Restart `IIS`.

Username or password are incorrect

This error message appears when you attempt to log into the NES Administrator Console on a network device.

Cause

This error message can appear for multiple reasons.

Resolution

To resolve this issue, perform the following actions:

- Log in to network device with the corporate credentials of the user account to ensure that:
  - The credentials that you typed are correct.
  - The password has not expired.
  - The user is not prompted to change the password because the account option **`User must change password at next login`** is set.
- Review the latest authentication service log file located on the NES host, in *C:\ProgramData\Nymi\AuthenticationService\Default_Web_Site\AuthenticationService\log* for error messages.

  If you see the following error messages:

  - The server could not be contacted.
  - The LDAP server is unavailable.

  Ensure that network connectivity exists between the network device and the AD server.

This site can’t be reached / This page cannot be displayed

This error message appears in the browser when you attempt to connect to the NES Administrator Console.

Cause

This error message appears when the HTTPs site binding is not correct or because the IIS service on the NES host is not started.

Resolution

To troubleshoot this issue, attempt to connect to NES Administrator Console website over a non-secure connection (HTTP).

- If the browser displays the NES Administrator Console page, ensure that the HTTPS binding in IIS is configured and the SSL certificate is selected. See the *Nymi Connected Worker Platform—Deployment Guide* for information about how to configure HTTPS site bindings.
- f the browser does not display the NES Administrator Console page, ensure that the IIS service is started on the NES host.

Cannot make a secure https connection to NES Administrator Console

When you cannot make a secure HTTPS connection to the NES Administrator Console, you will see issues like the following:

- When you type the HTTPS URL for the NES web application in a web browser, you cannot establish a secure connection, as shown in the following figure.

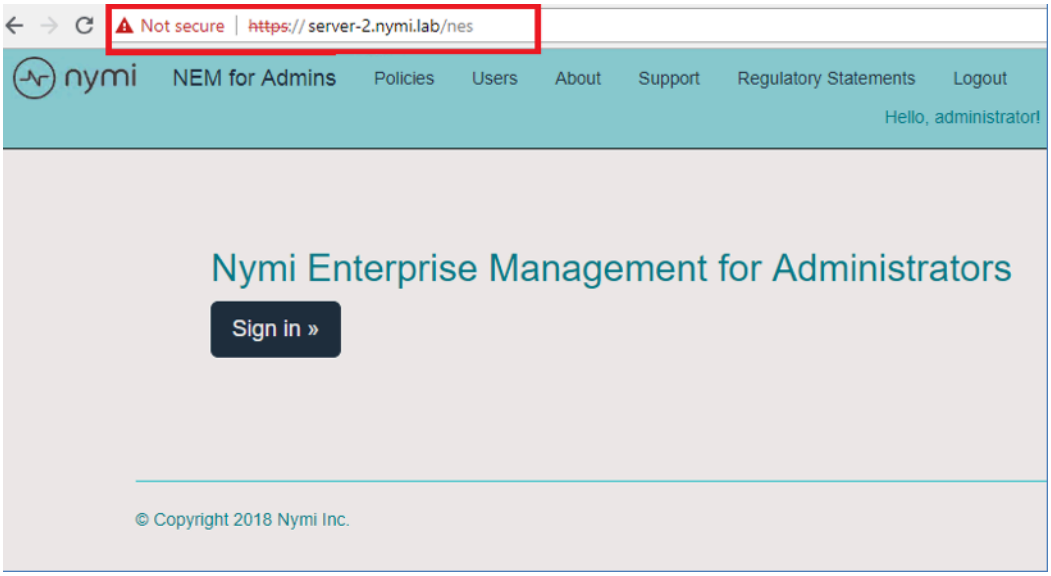


Figure 15: Cannot establish a secure connection to NES

- When you click the **`Sign in`** button, a window appears, which states that your connection is not private, and the error NET::ERR_CER_AUTHORITY_INVALID appears, as shown in the following figure.

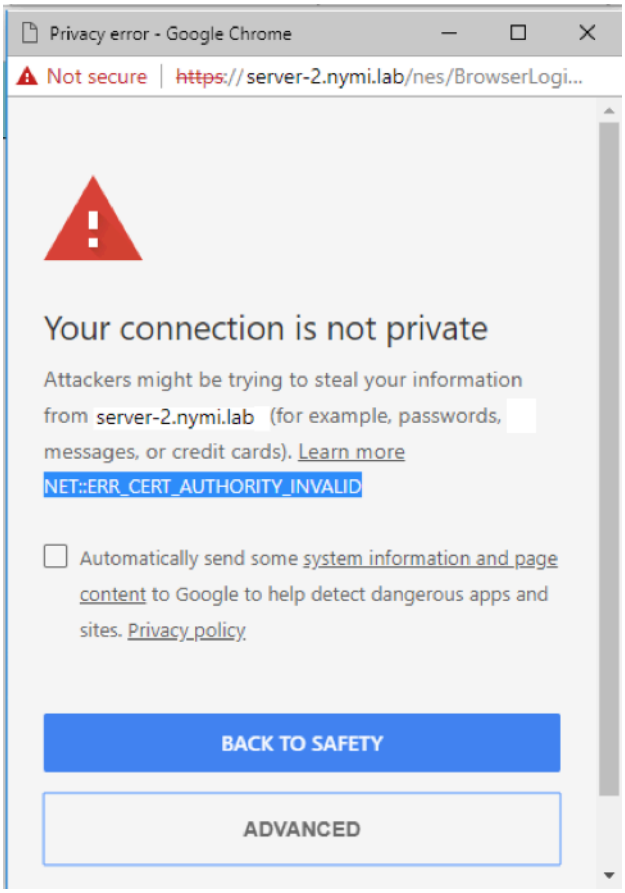


Figure 16: NET::ERR_CER_AUTHORITY_INVALID error

If you click on the **Advanced** button, and then click on the link to proceed to the web page, you can successfully log into the NES Administrator Console.

Cause

This behaviour occurs when the network terminal that you used to connect to the NES Administrator Console does not have the root certificate for the trusted root Certificate Authority installed as a trusted root.

Resolution

Import the root certificate into the Trusted Root Certificate Authority store. See *Importing root certificates* for more information.

The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel

This error message appears after you attempt to connect to NES Administrator Console.

Cause

The connection to NES is not secure.

Resolution

Ensure that the TLS server certificate has not expired and has been imported into the Trusted Root Certificate Authority store. See *Importing root certificates* for more information.

Troubleshooting NES Administrator Console Errors

This section provides information about errors that might appear when you are using NES Administrator Console.

HTTP Error 500.19 - Internal Server Error

This message can appear when you attempt to connect to the NES Administrator Console.

Cause

.NET 4.8 is not installed on the NES host.

Resolution

Install Microsoft .NET 4.8 on the NES host. The *Nymi Connected Worker Platform—Deployment Guide* describes how to install Microsoft .NET 4.8.

Failed to decrypt a column encryption key using key store provider: 'MSSQL_CERTIFICATE_STORE'

This error appears when viewing the NES System Diagnostics page, as shown in the following figure:

	L2 Cert Validity	The NES L2 certificate is valid	Pass
Database			Fail
	AE State	On!	
	Database Name	Nymi.nes	
	Writing AE	PEM == '<PEM-13:50>'.	Pass
	Reading AE	Failed to decrypt a column encryption key using key store provider: 'MSSQL_CERTIFICATE_STORE'. The last 10 bytes of the encrypted column encryption key are: 'B2-9D-5C-35-AB-E1-D4-7C-BA-19'. Keyset does not exist	Fail
	Clean up	FAIL: 0 rows saved.	Fail

Cause

The SQL database was hardened but the Application Pool Identity that was defined during the NES deployment was not set to LocalSystem.

Resolution

1. Run the NES installation wizard.
2. On the **`IIS`** tab, from the **`Application Pool Identity`** list, select **`LocalSystem`**.
3. On the **`Install`** tab, select **`Apply Settings`**.
4. Connect to the console and click **`About`**
5. Click **`View Full System Diagnostics`**, and confirm that the error does not appear in the **`Database`** section.

NES Application Pool Stopped

In `IIS Manager`, the NES Application Pool is in the Stopped state. When you start the application pool, the pool runs for a short time but stops again.

When you attempt to connect to the NES Administrator Console, a 503 error appears.

Cause 1

The password the application pool identity account has expired or changed, or the account is disabled.

Resolution 1

Correct the issue with the account, and if you changed the password, then perform the following steps to update the password in IIS.

1. In `IIS Manager`, from the navigation pane, select **`Application Pools`**.
2. Right-click the NES Application Pool, and select **`Advanced Settings`**, as shown in the following figure

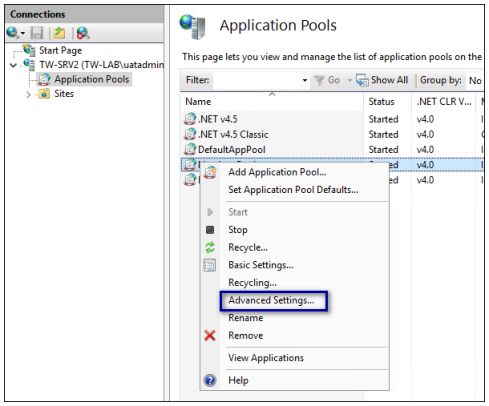


Figure 17: Application Pool Advanced Settings option

3. Click the Ellipses for the **`Identity`** setting as shown in the following figure.

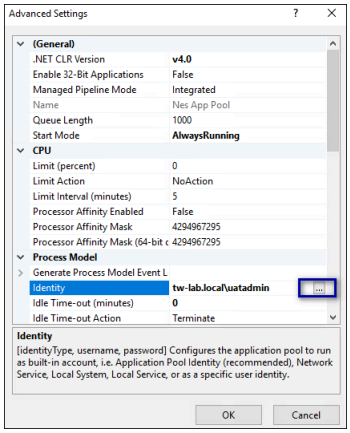


Figure 18: Application Pool Advanced Identity option

4. On the `App Pool Identity` window, click **`Set`**, as shown in the following figure.

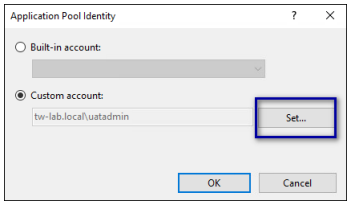


Figure 19: Application Pool Advanced Identity option

5. On the `Set Credentials` window, type the username for the application pool identity, and the new password. Click **OK**.

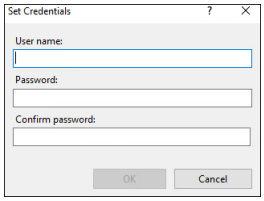


Figure 20: Application Pool Advanced Identity option

6. In `IIS Manager`, from the navigation pane, select the server name.

7. From the `Actions` menu, click **`Restart`**.

Cause 2

Microsoft Monitoring Agent is stopping the application pool.

The following error appears in the Application Event Log file:

```
Log Name: Application
Source: Application Error
Date: dd/mm/yyyy
Event ID: 1000
Task Category: (100)
Level: Error
Keywords: Classic
User: N/A
Computer: xyz
Description:
Faulting application name: w3wp.exe, version: 8.0.9200.16384, time stamp: 0x50108835
Faulting module name: PerfMon64.dll, version: 8.0.10918.0, time stamp: 0x577fd168
Exception code: 0xc0000409
Fault offset: 0x0000000000149794
Faulting process id: 0x2c38
Faulting application start time: 0x01d24405d195eb6a
Faulting application path: c:\windows\system32\inetsrv\w3wp.exe
Faulting module path: C:\Program Files\Microsoft Monitoring Agent\Agent\APMDOTNETAgent
\V8.0.10918.0\PerfMon64.dll
```

Resolution 2

Disable the `Microsoft Monitoring APM` service or remove the APM component from the application

Invalid Credentials (NES Administrator Console)

This error appears when an NES Administrator attempts to log into the NES Administrator Console and the username and password are correct.

Cause

The user account is a member of too many Active Directory groups and the Local Security Authority(LSA) cannot generate the token that NES requires to allow the login to complete.

Resolution

Reduce the group membership for the user account to 1009 or less. Refer to Microsoft for more information.

Troubleshooting Nymi Band Application Errors

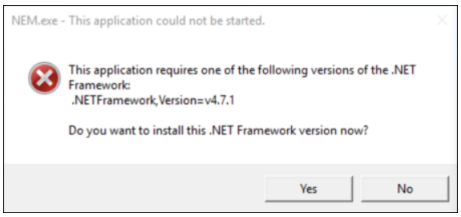
This section provides information about the errors that might appear when you log into the Nymi Band Application.

Troubleshooting Nymi Band Application Installation Errors

Review this section for error messages that might occur when you install the Nymi Band Application.

Nymi Band Application Cannot Install .net 4.7.1

This error appears when you install the Nymi Band Application and the installer cannot install .net 4.7.1.



Cause

The version of Windows 10 does not support .net 4.7.1

Resolution

Update Windows 10 to build version of 1607 or later.

Troubleshooting Nymi Band Application Startup Errors

Review this section for errors that appear when you log into the Nymi Band Application.

Invalid Credentials (Nymi Band Application)

This error appears when a user attempts to log into the Nymi Band Application and the username and password are correct. The user can log into the NES Administrator Console.

Cause

IP address of Nymi Enterprise Server(NES) was changed.

Resolution

Restart IIS to the clear cached values.

Unable to reach NES

Unable to reach NES. Please check your network connection and NES URL. Then restart the application. The NES URL in the registry at the following location.

About this task

Cause

This error occurs when opening the Nymi Band Application and under the following circumstances:

- NES URL registry setting is not correct
- Network connection issues are present
- TLS certificate was not imported on the computer running NES

Resolution

Procedure

1. Correct the NES URL by performing one of the following actions:
   - Create, if it does not already exist, the Group Policy registry key. See the Nymi Connected Worker Platform—Deployment Guide for more information.
   - Create, if it does not already exist, a local registry entry for the NES URL.
2. Run *regedit*.
3. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE*.
4. Create a new key named **`Nymi`**.
5. In the Nymi key, create a new key named **`NES`**.
6. Right-click **`NES>`**, and then select *New* > *String* value.
7. In the **`Name`** field, type **`URL`**.
8. Right-click URL and select **`Modify`**.
9. In the **`Value Data`** field, type *https://nes_servername/nes_service_name/*

   where

- nes_servername is the hostname of the NES server
- nes_service_name is the service mapping name for the NES web application

10. Click **OK**.
11. Ensure that network connectivity exists between the network terminal and the NES host.
12. Import the TLS certificate on the network terminal. See the Nymi Connected Worker Platform—Administration Guide for more information.

Failed to Get the Application Certificates

This error message appears in the Nymi Band Application. The Nymi Band Application manages certificates to secure communications between the Nymi Band and the BLE adapter. When this error appears, Nymi Band Application cannot retrieve certificates.

Cause 1

The Nymi Band Application Terminal cannot communicate with the NES server.

Resolution 1

Review the knowledge base for information about troubleshooting connectivity issues between the enrollment terminal and the NES server.

After you resolve the cause of the issue, log into the Nymi Band Application again. The certificate retrieve occurs automatically.

Cause 2

The L2 certificate or the TLS certificate has expired.

Resolution 2

Replace the expired certificates.

Note: *Resolving Certificate issues* provides more information about replacing expired certificates.

After you replace the expired certificate on NES, log into the Nymi Band Application again. The certificate retrieve occurs automatically.

The following errors appear in the *nymi_api.log* file:

```
{"operation":"init","exchange":"41","status":2201,"payload":{},"error":{"error_description":"The requested query was not found on the NES server.","error_specifics":""}}
INFO - Acquiring lock on the update queue sender
INFO - Lock acquired on the update queue sender
DEBUG - client connection error: connection error: An existing connection was forcibly closed by the remote host. (os error 10054)
```

If an administrator connects to the NES Administrator Console from a web browser, the connection is not secure.

Cause 3

TLS Certificate was created but the Subject Alternative Name does not contain the required FQDN entries for NES.

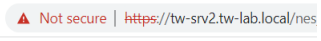
The following errors appear in the *nymi_api.log* file:

```
{"operation":"init","exchange":"41","status":2201,"payload":{},"error":{"error_description":"The requested query was not found on the NES server.","error_specifics":""}}
INFO - Acquiring lock on the update queue sender
INFO - Lock acquired on the update queue sender
DEBUG - client connection error: connection error: An existing connection was forcibly closed by the remote host. (os error 10054)
```

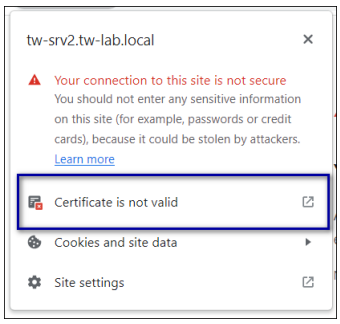
Additionally, if an administrator connects to the NES Administrator Console from a web browser, the connection is not secure.

To determine the Subject Alternative Name(s) that are defined for the TLS certificate, view the properties of the TLS certificate:

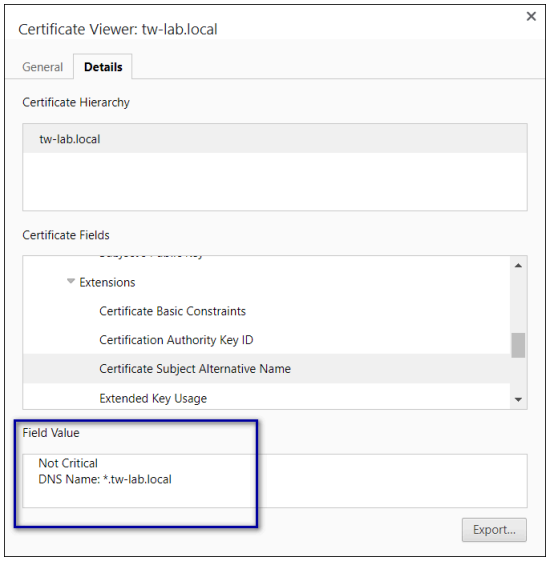
1. From a web browser, connect to the NES Administrator Console. A message appears that indicates that the connection is not secure and address bar displays an unlock symbol beside the URL, as shown in the following figure.



2. Select the unlock symbol on the address bar, and from the menu that appears, select the option to display the information about of the certificate. The following figure provides an example of the menu options that can appear and the option to select.



3. On the `Details` tab, scroll down and select the entry for Subject Alternative Name. The following figure provides an example where the FQDN of the server does not explicitly appear and the TLS is a wildcard certificate.



Resolution 3

Obtain a TLS certificate that defines the FQDN for NES in the Subject Alternative Name attribute, and then import the TLS certificate in IIS. If the NES server is in a highly available configuration that uses a load balancer, include the FQDNs for the virtual server and all the physical servers. The *Nymi Connected Worker Platform—Deployment Guide* provides more information.

Cannot connect to a Nymi Band. Nymi Bluetooth Endpoint is missing. Start the Nymi Bluetooth Endpoint service or contact your administrator

This error message appears after you log in to the Nymi Band Application.

The following figure shows the error message.

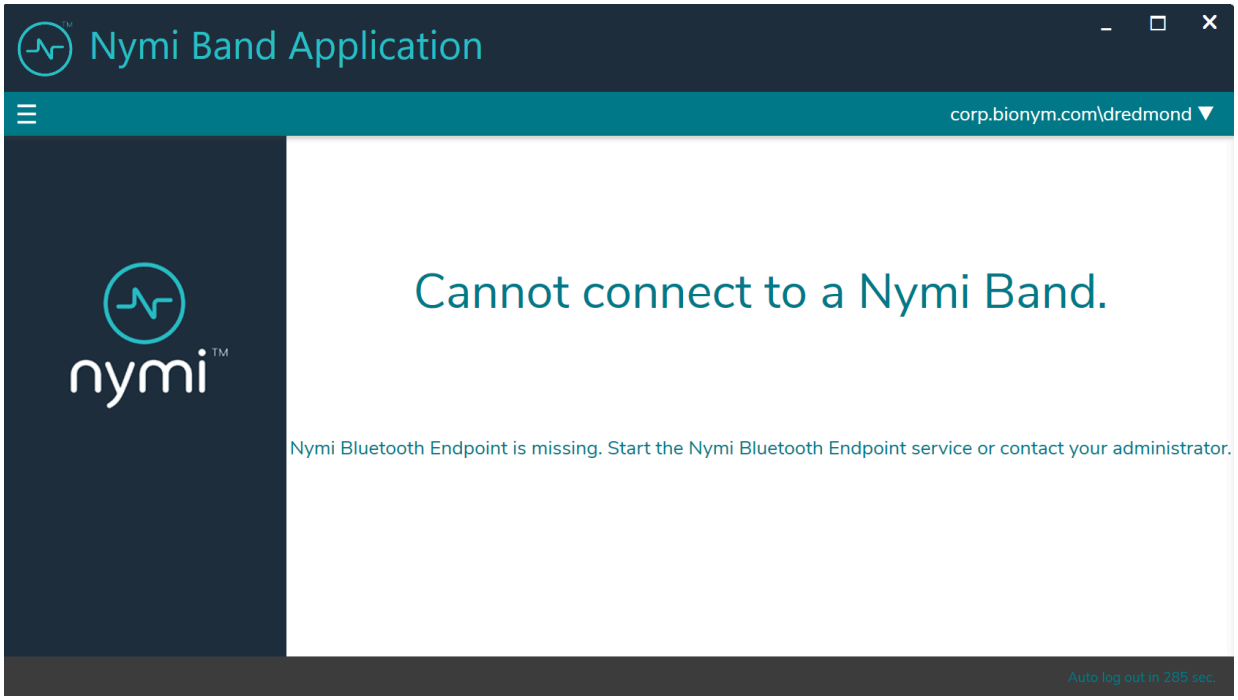


Figure 21: Cannot Connect to a Nymi Band

The *nem.log* file contains the following errors:

```
NAPI READ: {"operation":"error","exchange":null,"status":5100,"payload":{},"error":
{"error_description":"Nymi Bluetooth Endpoint is missing.","error_specifics":""}}
INFO   Band service disconnected, error code: 5100
```

Cause 1

- The Bluetooth adapter is not plugged into the Nymi Band Application Terminal.
- The Nymi Bluetooth Endpoint service is not running or needs to be reset.

Resolution 1

To resolve this issue, perform one of the following actions:

- Plug or reseat the Bluetooth adapter into a free USB port.
- Restart the Nymi Bluetooth Endpoint service.

Cause 2

The Nymi Band Application is installed on a Citrix server or RDP session host, the Nymi Bluetooth Endpoint is installed on the user terminal, but port 9120 was blocked.

Resolution 2

Configure the firewall to allow bidirectional communication over port 9120 between the Nymi Agent on the remote server and the Nymi Bluetooth Endpoint on the user terminal that accesses the remote server.

Cause 3

The Enrollment Terminal is connecting to a centralized Nymi Agent but the *nbe.toml* file is not configured with the location of the Nymi Agent.

Resolution 3

Navigate to the *C:\Nymi\Bluetooth_Endpoint* directory. If an *nbe.toml* file exists, rename the file and then restart the Nymi Bluetooth Endpoint service.

Cause 4

The user is accessing the Nymi Band Application through an RDP connection but the RDP connection host (local user terminal) does not have the Nymi Bluetooth Endpoint service running.

Resolution 4

On the RDP connection host (local user terminal), install the Nymi Bluetooth Endpoint and configure the *nbe.toml* file to specify the location of the Nymi Agent (Enrollment Terminal).

Cause 5

The Nymi Band Application connects to a centralized Nymi Agent and the load balancer has configured the Nymi Agent servers in Active/Active mode, which is an unsupported

configuration. Multiple Nymi Agent services are handling requests for the same Nymi Band Application session.

The *nymi_api.log* file includes the following error messages:

```
ERROR - serrec - Received error polling dongle: The device does not recognize the command. (os error 22)
WARN - BGADAPTER: error on dongle reader thread: receiving on an empty and disconnected channel
INFO - BLE Dongle removed.
ERROR - error terminating dongle polling thread: sending on a disconnected channel
INFO - Polling thread joined 2023-04-10 12:58:55.271998700 INFO - Adapter status changed: StateResponse
{ state: "7" }
INFO - BLE Dongle connected.
```

Resolution 5

On the load balancer, configure the Nymi Agent servers in Active/Standy mode.

Cannot connect to a Nymi Band. Nymi Agent is missing. Start the Nymi Agent service or contact your administrator

This error message appears after you log into the Nymi Band Application.

The following figure shows the error message.

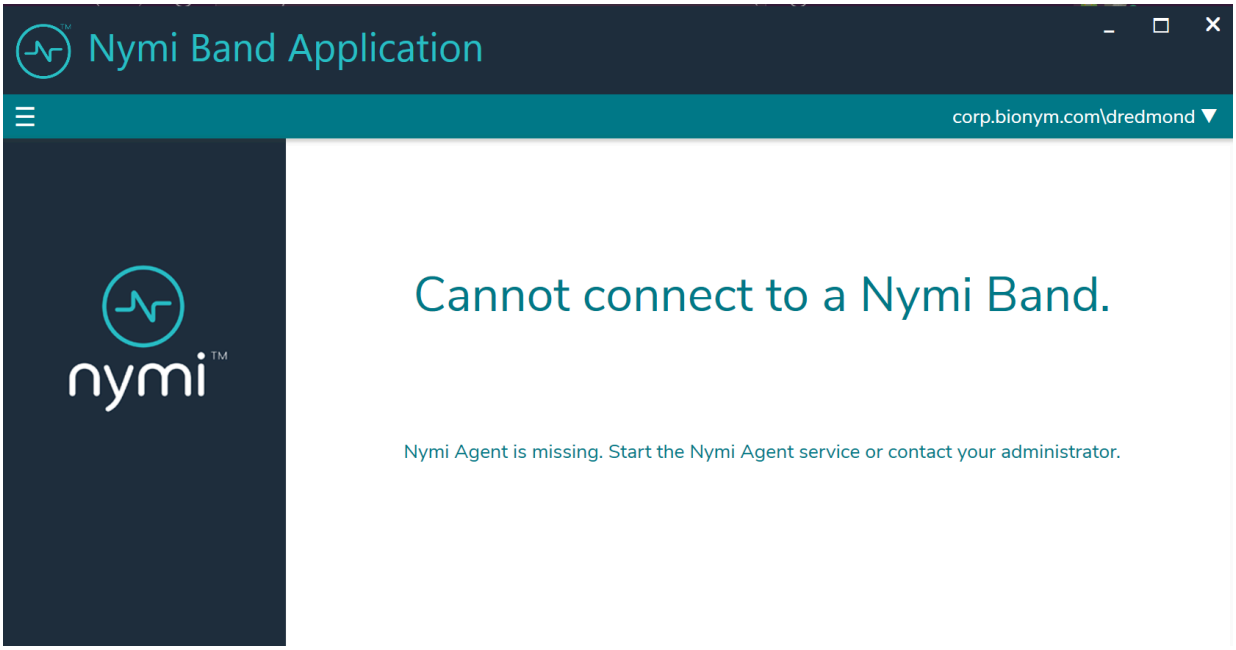


Figure 22: Nymi Agent is missing error

Cause 1

The Nymi Agent service is not running on the Nymi Band Application Terminal.

Resolution 1

Perform the following steps to start the Nymi Agent service.

- Open the Window `Services` and locate the Nymi Agent service.
- Start the Nymi Agent service.
- Close the Nymi Band Application.

- Open and log in to the Nymi Band Application.

Cause 2

In a centralized Nymi Agent configuration, the firewall between the Nymi Band Application Terminal host and the Nymi Agent server does not allow websocket traffic over port 9120.

The *nymi_api.log* file on the client machine has the following errors:

```
INFO - connecting to Agent at ws://server.ca:9120/socket/websocket
ERROR - Could not connect to websocket server. Attempting to connect again.
INFO - sending update to nea {"operation":"error","exchange":null,"status":4000,"payload":{},"error":
{"errordescription":"Nymi Agent missing.","errorspecifics":""}}
```

Resolution 2

Update the firewall port rules.

Windows N Edition Does not Display All Content

On a Windows N Edition enrollment terminal, content does not appears as expected in some windows within the Nymi Band Application.

The following figure provides an example.

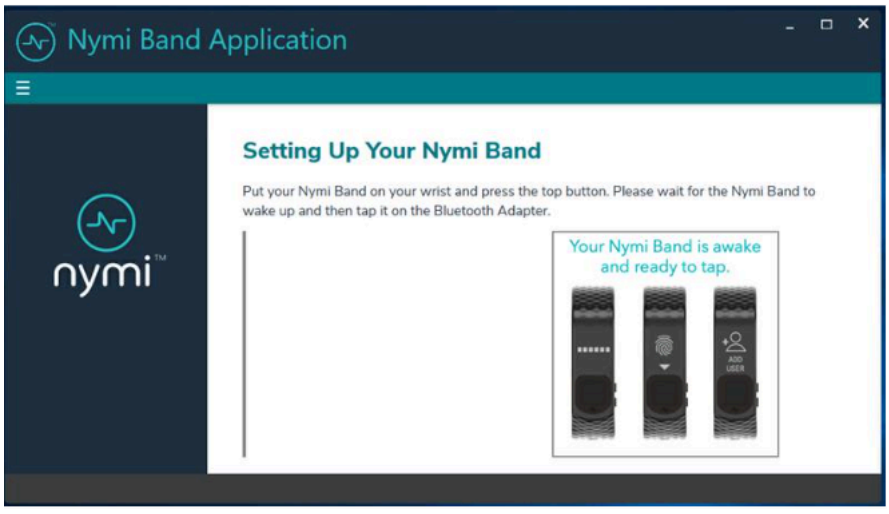


Figure 23: Nymi Band Application missing video content

Cause

By default Windows N Edition does not include the optional Media Pack, which NBANymi Band Application requires to display multimedia content.

Resolution

To obtain the media feature pack, perform one of the following actions:

- For Windows 10, version 1909 and later, navigate to **`Start > Settings > Apps & features > Optional features`**. Click **`Add a feature`**. From the list of available optional features, select **`Media Feature Pack`**.
- For Windows 10 versions that are earlier than 1909, download and install the media feature pack from Microsoft.
- For Windows 11, navigate to **`Start > Settings > Apps > Optional features`**. Next to **`Add an optional feature`**, select **`View features`**, and then form the list of optional features, select the Media Feature Pack.

Troubleshooting Enrollment Errors

Review this section for errors that might appear during the enrollment and re-enrollment errors.

A user does not exist for this Nymi Band in NES. Delete the user data on the Nymi Band, and then restart enrollment process

This error message in the Nymi Band Application on the Setting Up Your Nymi Band screen.

Cause

This error message appears when a user performs an enrollment with a Nymi Band that was previously enrolled to another user, and is still associated to the other user in Nymi Enterprise Server(NES).

Resolution

To resolve this issue, perform the following actions:

1. Delete the user data on the Nymi Band.
2. Log into the NES Administrator Console as an administrator and perform a search of the Nymi Band by serial number.
3. Delete the Nymi Band for the associated user.
4. Perform the enrollment again.

Authenticate to your Nymi Band

This message appears when logging into the Nymi Band Application to complete enrollment of your Nymi Band or to authenticate by using corporate credentials.

The following figure shows this error message.

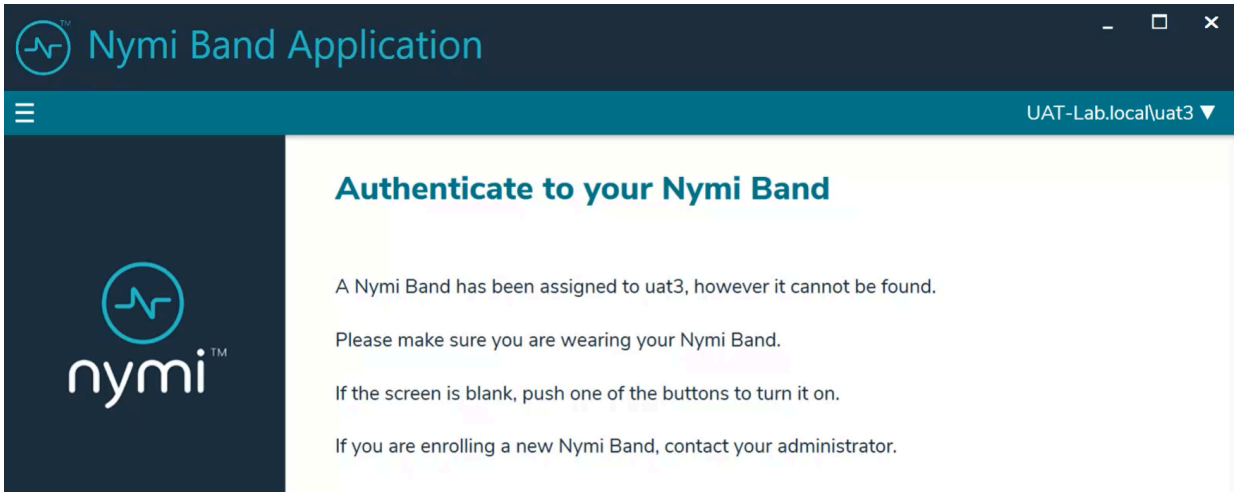


Figure 24: Cannot find your Nymi Band

Cause

This error can appear for the one of the following reasons:

- The user that logged into the Nymi Band Application is associated with a Nymi Band, but the Nymi Band Application cannot detect the Nymi Band.
- The Delete User Data process was performed on the Nymi Band, but the Nymi Band is still associated with a user account in NES.

Resolution

To resolve this issue, perform one of the following actions

- Wear the Nymi Band and authenticate. The error message disappears.
- An NES Administrator must Log in to the NES Administrator Console and perform the following steps to delete the Nymi Band association with the user.

  1. Edit the user account that is associated with the Nymi Band.
  2. Delete the Nymi Band association.

3. Ask the user to attempt to enroll the Nymi Band again.

Cannot perform re-enrollment because the NES policy settings do not allow re-enrollment.

This error message appears when a user taps an unenrolled Nymi Band in the Nymi Band Application.

Cause

The Nymi Band is already assigned to the user in the Nymi Enterprise Server(NES) that the Nymi Band Application connects to and the NES policy does not allow self service re-enrollment. The Nymi Band Application connects to an Nymi Enterprise Server(NES) that allows registration only.

Resolution

1. Log into the NES Administrator Console of the Enrollment NES.
2. In the NES Administrator Console, select **Search**.
3. In the **Search** field, type the full or partial username, first name, or last name of the user.
4. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
5. Select the Domain\username link of the user to open the **User Details** page.
6. Click the Serial Number of the original Nymi Band. The Nymi Band page appears.
7. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **Disconnect**. On the Disconnect page, scroll down and then click **Disconnect**.
8. On the Disconnect screen, scroll to the bottom and select **Disconnect**.
9. Instruct the user to attempt re-enrollment again

Cannot perform re-enrollment because this Nymi Band was previously assigned to another user and the credentials are non-transferrable.

This error message appears when a user taps an unauthenticated Nymi Band in the Nymi Band Application.

Cause

The Nymi Band is SEOS-enabled and already assigned to the user in the Nymi Enterprise Server(NES). You cannot re-enroll a Nymi Band that is associated with another user.

Resolution

1. Log into the NES Administrator Console for the Enrollment NES.
2. In the NES Administrator Console, select **Search**.

3. In the **Search** field, type the full or partial username, first name, or last name of the user.
4. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
5. Select the Domain\username link of the user to open the **User Details** page.
6. Click the Serial Number of the original Nymi Band. The Nymi Band page appears.
7. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **Disconnect**. On the Disconnect page, scroll down and then click **Disconnect**.
8. On the Disconnect screen, scroll to the bottom and select **Disconnect**.
9. Instruct the user to attempt re-enrollment again

Cannot perform re-enrollment because the NES policy settings do not allow re-enrollment of a Nymi Band that is assigned to another user.

This error message appears when a user taps an unauthenticated Nymi Band in the Nymi Band Application.

Cause

The Nymi Band is already assigned to a different user in the Nymi Enterprise Server(NES) that the Nymi Band Application connects to and the NES policy does not allow self service re-enrollment of a Nymi Band that is assigned to another user.

Resolution 1

Change the active NES group policy to allow self-service re-enrollment of the Nymi Band of another user.

1. Log into the NES Administrator Console.
2. Click **Policies**.
3. Edit the active group policy.
4. Select **Allow a user to re-enroll / re-register to any active Nymi Band**, and then click **Save**.
5. Instruct the user to attempt re-enrollment.

Resolution 2

Perform the following steps to manually re-enroll the Nymi Band.

1. Log into the NES Administrator Console of the Enrollment NES.
2. In the NES Administrator Console, select **Search**.
3. In the Search page, select the **Nymi Bands** option.
4. In the **Search** field, type the serial number of the Nymi Band (located on the back of the Nymi Band).
5. Select the Domain\username link of the user to open the **User Details** page.

6. Click the Serial Number of the original Nymi Band. The `Nymi Band` page appears.
7. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **`Disconnect`**. On the Disconnect page, scroll down and then click **`Disconnect`**.
8. On the `Disconnect` screen, scroll to the bottom and select **`Disconnect`**.
9. Instruct the user to attempt re-enrollment again.

Enrollment Cannot Proceed. Time on the Enrollment Terminal is Out of Sync with the Time on the Nymi Enterprise Server

This error messages appears during enrollment on the `Setting Up You Nymi Band` screen in the Nymi Band Application.

The following figure shows the error message in the Nymi Band Application.

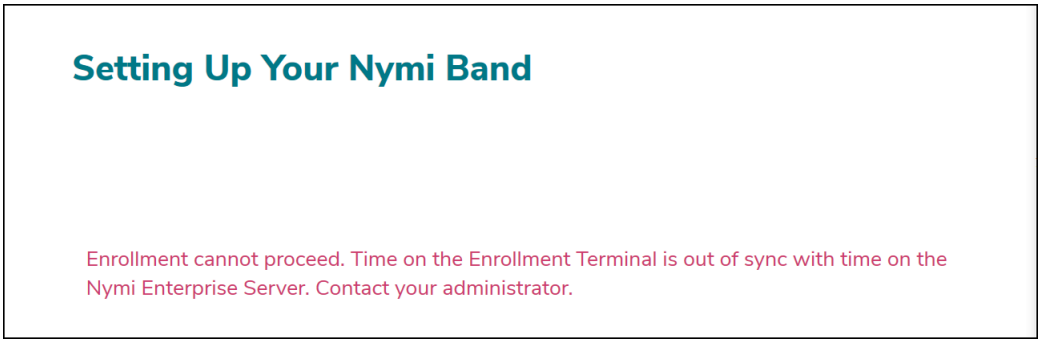


Figure 25: Time on the Enrollment Terminal is Out of Sync with the Time on the Nymi Enterprise Server

Cause

The clock on the enrollment terminal is not in sync with the clock on the Domain Controller.

Resolution

Contact your IT Department to sync the clock on the enrollment terminal with the Domain Controller.

Enrollment Cannot Proceed. Contact Your Administrator

This error message appears in the Nymi Band Application during enrollment.

The following figure shows the error message in the Nymi Band Application.

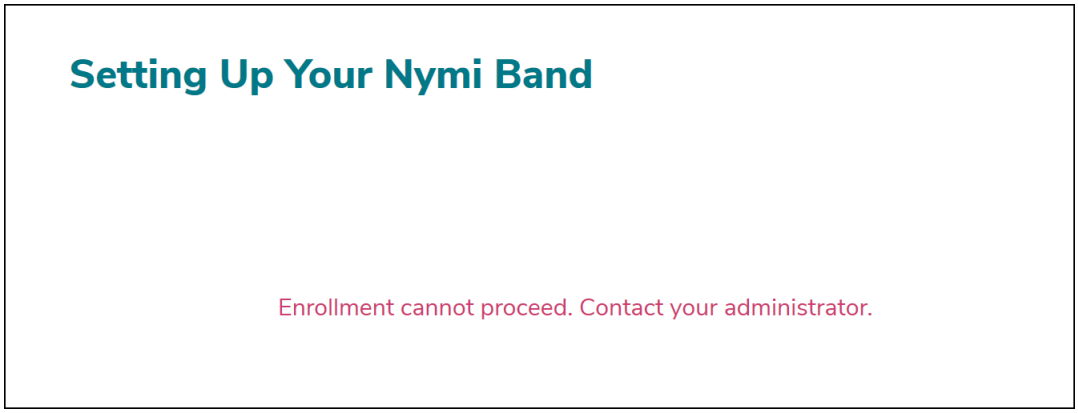


Figure 26: Enrollment Cannot Proceed

The following errors appear in the *nem.log* file:

```
ERROR FAILURE - UpdateBand(api/NymiBands/14): BadRequest - 'Bad Request' - uri:'https://server_name/
iis_instance_name/api/NymiBands/14' - headers: " Response content: {"Message":"{\"ResponseCode\":12,\"Description\":
\"Adv Key 1 cannot be generated due to CMAC mismatch.\"}"}
ERROR Failed at Update, api/NymiBands/14
NEM.Server.WebApiException Bad Request
```

Cause 1

The L2 certificate that Nymi Enterprise Server(NES) uses does not match the L2 certificate that the Nymi Band Application provides to the Nymi Band.

Resolution 1

To resolve this issue:

1. Log into NES and perform the following actions:
   a. Run NES installer.
   b. On the `Location` tab, in the **`Instance name`** field, type the IIS instance name, and then click **`Test`**. Confirm that the **`Results`** box displays Success Update / Re-Install. If you see New Install in the output, ensure that you typed the correct IIS instance name.
   c. On the `Certificates` tab, ensure that you select the correct L1 and L2 certificates, and the PFX file that corresponds to the L1 and L2 certificates.
   d. On the `Install` tab, click **`Apply Settings`**.
2. On the enrollment terminal, delete the files in the *%APPDATA%\Nymi\NSL* folder for the user account that logs into the enrollment terminal.

Cause 2

NES generated an incorrect CMAC.

Resolution 2

Perform one of the following actions:

- Update NES to Connected Worker Platform(CWP) 1.18.0 or later, which contains a fix for this issue.
- Perform a Delete User Data operation on the Nymi Band, and then re-enroll the Nymi Band. If you do not allow self-enrollment, dissociate the Nymi Band from the user in the NES Administrator Console before the user attempts the re-enrollment.

  Note: If you encounter the issue again, repeat the steps to re-enroll.

Failed to read details from the Nymi Band. Install a supported Nymi Runtime version or check bluetooth connectivity

The error message appears when on the `Setting up Nymi Band` window in the Nymi Band Application.

Cause

The Nymi Runtime version is not correct or Nymi Band Application has lost connectivity with the Nymi Band.

Resolution

To resolve this issue, perform the following steps:

- Ensure that version of the Nymi Runtime software on the enrollment terminal is supported by NES and the Nymi Band Application. The *Connected Worker Platform Release Notes* provides more information.
- Ensure that the user keeps the Nymi Band within bluetooth range of the Bluetooth adapter that is connected to the enrollment terminal.

Fingerprint creation failed, try again

This error message appears in the Nymi Band Application when you attempt to create the fingerprint profile on the Nymi Band.

Cause

This error message appears when the sensor could not complete the fingerprint capture, for example, when a user distracted and does not touch the Nymi Band screen as instructed.

Resolution

Click **`Start`** and retry fingerprint enrollment.

Not Found

This error message appears in the Nymi Band Application during enrollment.

The following errors appear in the *nymi_api.log* file:

```
ERROR  FAILURE - AddEnrollmentEventEntry(api/EnrollmentEvents): NotFound - 'Not Found' - uri:'https://
nes_server/instance/api/EnrollmentEvents' - headers: '' Response content: {"Message":"No HTTP resource was found that
 matches the request URI 'https://nes.qalab.nymi.com/CWP-2785-Fix/api/EnrollmentEvents'."}
ERROR  Failed at Create <Nymi.Model.NesModel.EnrollmentEvent>, api/EnrollmentEvents
NEM.Server.WebApiException Not Found
ERROR  Failed to save config into band.
NEM.Server.WebApiException Not Found
```

Cause

NES does not support the Nymi Band Application version.

Resolution

Update the Nymi Band Application to the version that matches NES.

Nymi agent is missing. Start the Nymi agent service or contact your administrator

This error message appears when after you log into the Nymi Band Application in an environment where the enrollment terminal connects to a remote Nymi Agent.

The following errors appear in the *nymi_api.log* file:

```
ERROR  FAILURE - AddEnrollmentEventEntry(api/EnrollmentEvents): NotFound - 'Not Found' - uri:'https://
nes_server/instance/api/EnrollmentEvents' - headers: '' Response content: {"Message":"No HTTP resource was found that
 matches the request URI 'https://nes.qalab.nymi.com/CWP-2785-Fix/api/EnrollmentEvents'."}
ERROR  Failed at Create <Nymi.Model.NesModel.EnrollmentEvent>, api/EnrollmentEvents
NEM.Server.WebApiException Not Found
ERROR  Failed to save config into band.
NEM.Server.WebApiException Not FoundINFO - connecting to Agent at ws://agent_server_name:9120/socket/
websocket
ERROR - Could not connect to websocket server. Attempting to connect again.
INFO - sending update to nea {"operation":"error","exchange":null,"status":4000,"payload":{},"error":
{"errordescription":"Nymi Agent missing.","errorspecifics":""}}
```

Cause

The firewall between the Nymi Band Application host and the Nymi Agent server does not allow websocket traffic over port 9120.

Resolution

Update the firewall port rules to enabled bi-directional communication between the enrollment terminal and the Nymi Agent server.

Troubleshooting Post Enrollment Nymi Band Application Errors

Review this section for information about error messages that appear when you log into the Nymi Band Application after enrollment, for example, to authenticate by corporate credentials or to apply Nymi Enterprise Server(NES) policy changes on the Nymi Band.

Failed to Fetch Firmware Version

This error message appears in the Nymi Band Application when you log in to Nymi Band Application with an unauthenticated Nymi Band.

The following figure show the error messages that appears in the Nymi Band Application.

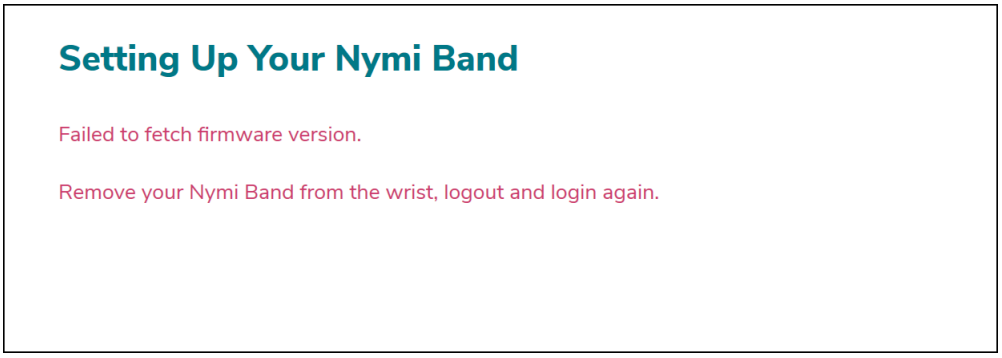


Figure 27: Failed to Fetch Firmware Version

Cause

Nymi Band Application timing issue.

Resolution

1. Log out of the Nymi Band Application, and then log back into the Nymi Band Application.

Troubleshooting Legacy Nymi Band Application Errors

Review this section for errors related to older versions of Nymi Band Application.

Enrollment URL is not set. Contact your administrator.

This error message appears when an user types their username and password on the `Sign in` window, and then clicks Sign in.

Cause

The Enrollment URL is not defined in the active group policy.

Resolution

An NES Administrator must log in to the NES Administrator Console and ensure that the value in the **`Enrollment URL`** field for the active group policy is correctly defined.

Band error: (3010) Operation timed out

This error message appears in the Nymi Band Application when you type the setup code and click **`Begin`**.

Cause

The network terminal cannot establish or maintain Bluetooth communications with the Nymi Band.

Resolution

Perform the following actions and retry the operation after each action, until the operation completes successfully.

- Place the Nymi Band close to the Bluetooth adapter and click **`Begin`** again.
- Stop and restart the Nymi Bluetooth Endpoint service.
- Reseat the Bluetooth adapter in the USB port.
- Confirm that the Bluetooth adapter (Bluegiga Bluetooth Low Energy) appears in **`Device Manager > Ports`** and that the device status states that it is working properly.
- Reboot the terminal.

Band error: (3000) Operation timed out

This error message appears in the Nymi Band Application when you type the setup code and click **Begin**.

The network terminal cannot communicate with the NES host.

Cause

The network terminal cannot communicate with the NES host.

Resolution

Type the setup code again and click **Begin**. If the operation fails again, confirm that a reliable network connection exists between the network terminal and the NEShost.

Troubleshooting Nymi Band Application Erorrs (IT/OT-Specific)

Connected Worker Platform(CWP) 1.18.0 and later provides support for the Nymi IT/OT Solution.

This section provides information about errors that users might encounter during the enrollment, registration, re-enrollment, and re-registration processes.

Cannot perform enrollment because this domain {domain_name} allows registration only.

This error message appears when a user taps an unauthenticated Nymi Band in the Nymi Band Application.

The following message also appears:

Before you register an additional account to your Nymi Band, first enroll in a domain that allows enrollment.

Cause

The Nymi Band Application connects to an Nymi Enterprise Server(NES) that allows registration only.

Resolution

Instruct the user to perform their enrollment on a Nymi Band Application Terminal in the identity domain that supports enrollment.

Cannot Complete Operation. This domain {domain} allows enrollment

only. This Nymi Band is not assigned to you in NES.

This error message appears when a user taps an authenticated Nymi Band in the Nymi Band Application.

The following message also appears:

If you want to enroll, delete the user data and retry the operation. If you want to register an additional account to your Nymi Band, perform the registration on the correct NBA.

Cause 1

User wants to register the Nymi Band but the Nymi Enterprise Server(NES) that the Nymi Band Application connects to allows enrollments only.

Resolution 1

Instruct the user to perform their registration on a Nymi Band Application Terminal in the identity domain that supports registration.

Cause 2

The user wants to perform a self-service re-enrollment on an enrollment terminal but has not performed the delete user data operation on the Nymi Band.

Resolution 2

Instruct the user delete the user data on the Nymi Band and then attempt re-enrollment again.

Cannot perform re-registration because the NES policy settings do not allow you to re-register an additional account to your Nymi Band.

This error message appears when a user taps an authenticated Nymi Band in the Nymi Band Application.

Cause

User wants to re-register the Nymi Band but the Nymi Enterprise Server(NES) that the Nymi Band Application does not allow re-registration.

Resolution 1

Change the active NES group policy on the Registration NESto allow self-service re-registration of the Nymi Band.

1. Log into the NES Administrator Console for the Registration NES.
2. Click **`Policies`**.
3. Edit the active group policy.
4. Select **`Allow a user to re-enroll / re-register to any active Nymi Band`**, and then click **`Save`**.
5. Instruct the user to attempt re-registration.

Resolution 2

Instruct the user to perform their registration on a Nymi Band Application Terminal in the identity domain that supports re-registration. If an identity domain that supports re-registration does not exist:

1. Instruct the user to delete the user data on the Nymi Band.
2. Remove the Nymi Band association with the user account on the Enrollment NES and Registration NES.
3. Instruct the user to enroll their Nymi Band with the Nymi Band Application in identity domain that support enrollment.
4. Instruct the user to attempt the Nymi Band registration again.

Note: Nymi recommends that your policy settings on all NES servers in all identity domains match, for example, all support re-enrollment and re-registration or none support re-enrollment and re-registration.

Cannot perform re-registration because this Nymi Band was previously assigned to another user and the credentials are non-transferrable.

This error message appears when a user taps an unauthenticated Nymi Band in the Nymi Band Application.

Cause

The user manually re-enrolled a SEOS-enabled Nymi Band; however, the CWP Administrator did not disassociate the Nymi Band from the previous user on the Registration NES. You cannot re-register a SEOS-enabled Nymi Band that is associated with another user.

Resolution

1. Log into the NES Administrator Console of the Registration NES.
2. In the NES Administrator Console, select **`Search`**.
3. In the **`Search`** field, type the full or partial username, first name, or last name of the user.
4. Click **`Search`**. The `Search` page displays the user, or a list of users that match the search criteria.
5. Select the Domain\username link of the user to open the **`User Details`** page.
6. Click the Serial Number of the original Nymi Band. The `Nymi Band` page appears.
7. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **`Disconnect`**. On the Disconnect page, scroll down and then click **`Disconnect`**.
8. On the `Disconnect` screen, scroll to the bottom and select **`Disconnect`**.
9. Instruct the user to attempt re-registration again.

Cannot Complete the Operation. Delete user data on the Nymi Band and Click Start Over to restart enrollment or registration.

This error message appears when a user taps an authenticated Nymi Band in the Nymi Band Application.

Cause

The Nymi Band was previously registered or enrolled in the NES, but a CWP Administrator has disconnected the Nymi Band from the user account in NES.

Resolution

1. Instruct the user to delete the user data on the Nymi Band.
2. Instruct the user to enroll their Nymi Band with the Nymi Band Application in identity domain that supports enrollment.
3. Instruct the user to attempt the Nymi Band registration again.

Cannot Complete Operation.

This error message appears when a user taps an unauthenticated Nymi Band in the Nymi Band Application.

The following message also appears:

To enroll this Nymi Band, delete the user data on the Nymi Band, and then click Start Over. To register an additional account to this Nymi Band, authenticate, and then click Start Over. If you cannot authenticate to the Nymi Band, confirm that this Nymi Band is assigned to you. Contact your administrator for assistance.

Cause 1

User wants to authenticate a Nymi Band with corporate credentials but the target NES does not allow corporate credentials authentication.

Resolution 1

Instruct the user to perform their corporate credentials authentication on a Nymi Band Application Terminal in the identity domain that supports corporate credentials authentication.

Cause 2

The user is attempting to perform a self-service re-registration on a registration terminal.

Resolution 2

Instruct the user to authenticate to their Nymi Band and then attempt the re-registration again.

Cause 3

The user is attempting to perform a self-service re-enrollment on an enrollment terminal but has not performed the delete user data operation.

Resolution 3

Instruct the user delete the user data on the Nymi Band and then attempt re-enrollment again.

Insufficient memory on the Nymi Band to support the registration

This error message appears when a user taps an unauthenticated Nymi Band in the Nymi Band Application.

The following figure shows the error message that appears in the Nymi Band Application.

Figure 28: Insufficient memory on the Nymi Band to support the registration

The following message also appears in the Authentication Service log file on the Registration NES:

WebException - The remote server returned an error: (503) Server Unavailable.

Cause

The Registration NES was unavailable during registration and the Nymi Band Application retries the registration operation and writes data to the Nymi Band until the Nymi Band runs out of available memory.

Resolution

Instruct the user to:

1. Perform a Delete User Data on the Nymi Band.
2. Enroll their Nymi Band on the Enrollment Terminal
3. Confirm that Registration NES available, and then try registration again on the Registration Terminal.

Troubleshooting Lock Control

This chapter provides information about how to resolve issues related to locking and unlocking a user terminal with Nymi Lock Control.

Troubleshooting Nymi Lock Control statuses

After you successfully log in, a Nymi Lock Control icon appears in the system tray. When you hover over the icon, the Nymi Lock Control status appears, as shown in the following figure.

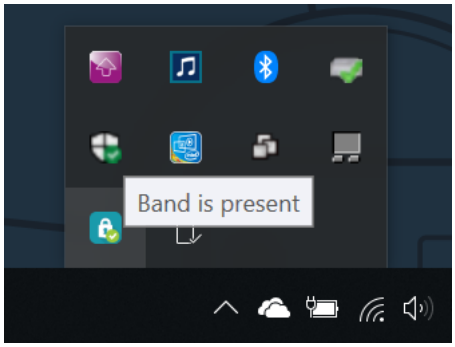


Figure 29: Nymi Lock Control Band is Present status

The following table provides more information about the statuses that can appear.

Table 3: Nymi Lock Control Statuses and Resolutions

Message	Cause	Resolution
Band is absent	Nymi Lock Control cannot detect an authenticated Nymi Band in the Bluetooth range.	• Bring the Nymi Band closer to the terminal. • Wear and authenticate the Nymi Band

Message	Cause	Resolution
No active band	• User that is currently logged into the terminal has not authenticated to a Nymi Band. • Nymi Band for the user is not active in NES.	• Use Nymi Band Application to enroll the user with a Nymi Band. • Edit the properties of the user in NES and ensure that the Nymi Band is active for the user. • Ensure the NES active policy enables Lock Control.
Nymi Lock Control connection error	• Nymi Lock Control cannot detect the Bluetooth adapter. • A Nymi service is not running.	• Ensure that the operating system can detect the Bluetooth adapter. • Ensure that the Nymi Agent and Nymi Bluetooth Endpoint services are running.
Searching for band	Nymi Lock Control is attempting to detect the Nymi Band.	n/a
Getting band info	Nymi Lock Control is starting and contacting NES to retrieve information about the user.	n/a
Getting band info failed	Nymi Lock Control cannot contact NES and the logged in user has not previously tapped to get access to the terminal.	• Ensure that network connectivity exists between the terminal and the NES host. • Ensure that the NES host is powered on. • Ensure the terminal is on the same domain as NES.

Known Issues with Windows 7

The following table summarizes known issues when using Nymi Lock Control and Nymi Credential Provider on Windows 7 user terminals.

Table 4: Known issue with Windows 7

Issue	Workaround
Only one NFC reader can be plugged in at a time. More than one will cause failures.	n/a

Issue	Workaround
User cannot tap to unlock the user terminal on the Login screen.	If the Windows screen displays Press CTRL-ALT-DEL, then the user must perform the key sequence before attempting to tap to log in with Nymi Lock Control.
The Nymi user tile shown may show a different user than the last logged in user.	None. Regardless of which user tile appears on screen, when a user taps to log in, they will be logged into the correct account.
In some rare instances, the Windows login screen may become unresponsive.	If the login screen does not recover automatically within a couple of minutes, the user might have to restart the user terminal.
User cannot unlock the user terminal with their Nymi Band immediately after hibernate mode on Microsoft Surface tablets.	After exiting hibernation mode, log in with a username and password. Subsequent attempts to lock and unlock with the Nymi Band will succeed.

Cannot unlock the screen when another user is logged into a Windows 7 terminal

If a user is logged into a terminal, another Nymi Band user cannot perform an NFC tap to unlock the terminal.

Cause

Limitation in Windows 7

Resolution

To access a terminal when another Nymi Band user is logged into the terminal, first, click the **`Switch User`** button, and then perform an NFC tap.

Note: In some instances, incorrect error messaging appears when a user attempts to login.

Cannot log in to the network terminal immediately after the terminal locks

When the network terminal locks and the user immediately taps the Nymi Band against the NFC reader, the terminal does not unlock.

Resolution

Wait a few seconds and then tap the Nymi Band against the NFC reader.

Cannot unlock terminal, something went wrong

A user cannot unlock the terminal with Nymi Lock Control tap and when attempting to login with Nymi Credential Provider, a message appears stating that "something went wrong".

Cause

- User password has expired.
- User password has changed in the Active Directory, and the change has not been reflected in NES.
- No connection to NES.
- Terminal is on a different domain from NES.

Resolution

To resolve this issue, perform one of the following actions:

1. If your password is expired, you will be prompted to change your password. Perform the following steps:
   a. Click **OK**.

      The `Nymi Credential Provider` window appears prompting the user for their password.
   b. Click the **Sign-in** option.
   c. Select the Key icon.
   d. Enter the current password for the user and then click **OK**.

      A message appears and states that the password has expired.
   e. Click **OK**. A window appears to update the password.
   f. In the **Password** field, type the current password.
   g. In the **New password** field, type a new password.
   h. In the **Confirm password** field, type the new password again.
   i. Press **Enter**.

      A message appears advising that the password has changed. Desktop appears.
   j. Log into the Nymi Band Application with your new credentials while wearing your authenticated Nymi Band.
2. If the user terminal is not connected to NES, fix connectivity issues.
3. If the user terminal is on a different domain from NES, put the user terminal on the NES domain.

Cannot unlock the terminal after bringing it out of sleep mode

When a user wakes a user terminal from sleep or hibernation mode, and then taps the Nymi Bandagainst the attached NFC reader, the terminal does not unlock. The user can log in by using the Nymi Credential Provider.

Cause

To conserve battery life, the user terminal is configured to suspend USB devices when the terminal is in power mode. When a user wakes the user terminal, the USB devices are not reactivated until after the user logs in to the terminal.

Resolution

To resolve this issue, perform one of the following actions:

- Create a Windows group policy to disable **`USB Selective Suspend`**.
- Manually disable the **`USB Selective Suspend`** option on each terminal. For example, on Windows 10, perform the following steps:

  1. Open **`Power Options`**, and then click **`Additional Power Settings`**.

     The following figure provides an example of the `Power Options` window.

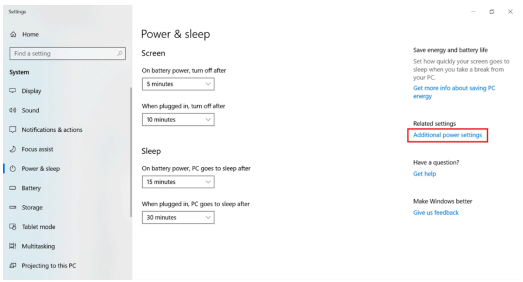


Figure 30: Additional Power options

  2. In the `Choose or customize a power plan` screen, click the **`Change plan settings`** link, which appears beside the power plan.

     The following figure provides an example of the `Choose or customize a power plan` screen.

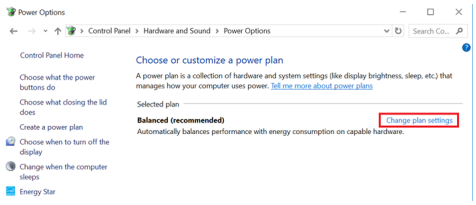


Figure 31: Choose or customize a power plan screen

3. On the `Edit Plan Settings` window, click `Change advanced power settings`.

   The following figure shows the `Edit Plan settings` window.

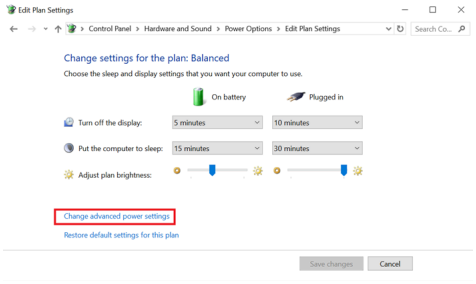


Figure 32: Edit Plan Settings screen

4. In the `Advanced settings` window, perform the following steps:

   a. Expand **`USB settings > USB selective suspend setting`**
   b. From the **`On battery`** list, select **`Disabled`**.
   c. From the **`Plugged in`** list, select **`Disabled`**.
   d. Click **`OK`**.

   The following figure provides an example of the `Advanced settings` window.

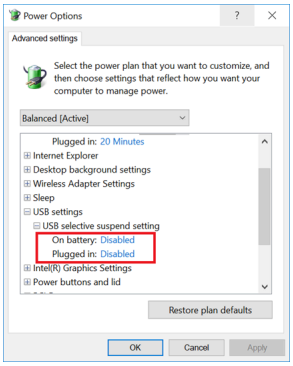


Figure 33: Advanced Settings window

5. Close the `Edit Plan Settings` and `Power options` windows.

Disconnect from agent

This error message appears on the Login screen when you try to unlock the user terminal by an NFC tap or by using Nymi Credential Provider

Cause

The Nymi Agent service is not started on the user terminal.

Resolution

Log in to the terminal with a username and password, and then start the Nymi Agent service.

Nymi Bluetooth Agent is missing

This error message appears on the Login screen when you try to unlock the user terminal by an NFC tap or by using Nymi Credential Provider.

Cause

The Nymi Bluetooth Endpoint service is not started on the user terminal.

Resolution

Log in to the terminal with a username and password, and then start the Nymi Bluetooth Endpoint service.

Nymi Bluetooth Agent is missing

This error message appears on the Login screen when you try to unlock the remote desktop by an NFC tap or by using Nymi Credential Provider.

The *nymi_api.log* file also includes the following error message:

```
DEBUG - client connection error: connection error: An existing connection was forcibly closed by the remote host. (os error 10054)
```

Cause

Network configuration such as Network Address Translation (NAT) is configured and redirecting traffic to a different IP address for the VMWare Horizon client.

Resolution

Log in to the user terminal and perform the following steps:

1. Run **regedit.exe**
2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Nymi*.
3. Right-click **`Nymi Lock Control`**, and then select **`New > String value`**.
4. In the **`Value`** field, type ***ViewClientVariable***.
5. Double-click ***ViewClientVariable*** and in the **`Value Data`** field, type `ViewClient_Broker_Remote_IP_Address`.
6. Click **`OK`**.

Cannot find band. Please enter your password, or retry

This error message appears on the Nymi Credential Provider screen after you attempt to use Nymi Credential Provider to unlock the desktop.

Cause

The Nymi Band is worn on the wrist of the user but is not authenticated.

Resolution

Authenticate the Nymi Band, and then attempt the Nymi Credential Provider login again.

User Terminal Does Not Lock

When you enable the NES policy option Lock when away, the desktop does not lock when the user removes their Nymi Band or when the user moves out of Bluetooth range and the on screen countdown reaches 0.

Cause

Group policy object(GPO) settings prevent the desktop lock.

Resolution

Ensure that your Group Policy Object(GPO) settings do not push the *Do not display the lock screen* configuration option to the Nymi Lock Control user terminals.

The user is not registered with the Nymi Enterprise

This error message appears on the Nymi Credential Provider screen when the user performs an NFC tap or attempts to use Nymi Credential Provider to unlock the desktop.

Cause

Reasons that this error can messages appear include:

- Nymi Band is authenticated in a domain that differs from the domain that the user terminal is on.
- Nymi Band is authenticated to the user, but the IT Administrator has deleted the Nymi Band association with the user in NES

Resolution

Contact the IT Administrator to enroll the Nymi Band in the correct domain.

Application is missing NES Certificates

This error message appears when you tap to unlock the desktop.

Cause

The user terminal is in a different domain from the NES server and could not communicate with NES to obtain the required certificates.

Resolution

Ensure that DNS is correctly configured with referrers / conditional referrer to resolve the domain names in a multidomain configuration.

The Account Password Has Been Changed. Please Login With Your New Password.

This error message appears when you tap to unlock the desktop.

The following figure provides an example of the error message.

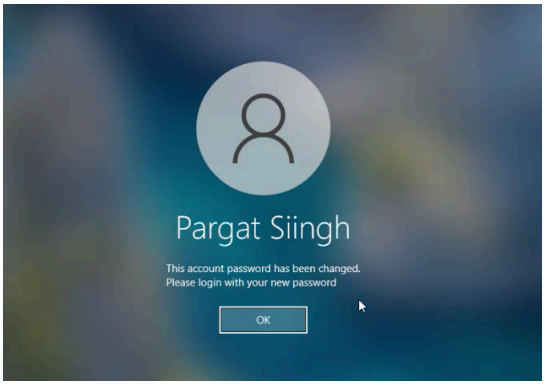


Figure 34: The Account Password Has Been Changed. Please Login With Your New Password.

Cause

The user changed their the password for their Active Directory account.

Resolution

Click **OK**, and then when prompted, type the username and new password. The Desktop unlocks and subsequent taps to unlock succeed.

Something Went Wrong. Please Try Again

This error message appears when you tap to unlock the desktop.

The following figure provides an example of the error message.

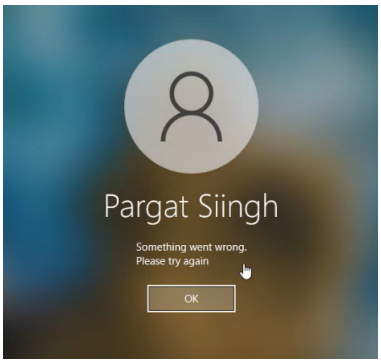


Figure 35: Something went wrong. Please try again.

Cause

The user account is locked or disabled in Active Directory.

Resolution

Unlock or enable the account for the Nymi Band user in Active Directory, and then instruct the user to try a Nymi Band tap again.

Error: Invalid Credentials. Please Try Again

This error message appears when you tap to unlock the desktop.

The following figure provides an example of the error message.

Figure 36: Something went wrong. Please try again.

Cause

The user typed an incorrect password.

Resolution

Click **OK** and then type the correct password.

NEA is missing certificates

This error message appears when starting Nymi Lock Control.

Cause

Nymi Lock Control cannot contact NES to retrieve certificates.

Resolution

To resolve this issue, perform the following actions

1. Ensure that a network connection exists between the user terminal and NES
2. In the **`System Tray`**, right-click the Nymi Lock Control icon and select **`Quit`**.
3. In `Windows Explorer`, navigate to the *%appdata%\Roaming\Nymi\NSL* folder.
4. Delete the subfolders in the *NSL* folder
5. Start Nymi Lock Control by double-clicking the Desktop icon.

Nymi Lock Control re-initalizes and downloads the NEA certificates.

Troubleshooting Connectivity Issues

Review this section for information about how to troubleshoot basic and advanced connectivity issues.

Troubleshooting Basic Connectivity Issues

The Nymi Enterprise Edition (NEE) and Connected Worker Platform(CWP) solutions rely on bidirectional communications between components over TCP ports.

1. Perform the following steps to troubleshoot connectivity issues between the NES server and other components in the solution, such as the enrollment terminal, user terminals or the centralized Nymi Agent server.
2. On the component machine, from a command prompt type the following commands to confirm that the machine can communicate with the NES server (and that output returns the correct IP addresses and names):

   Table 5:

Component 1	Component 2	Default TCP Port
NES server	User Terminals	80/443 (depending on configuration of NES)
User Terminals	Nymi Agent server	9120
RDP/Citrix client	Nymi Agent server	9120
NES Administrator Console machine	NES server	80/443 (depending on configuration of NES)

3.
```
ping FQDN_NES_server
ping shortname_NES_server
ping ip_address_NES_server
nslookup FQDN_NES_server
nslookup shortname_NES_server
nslookup ip_address_NES_server
```

4. On the NES server from a command prompt type the following commands to confirm that the NES server can communicate with the client (and that output returns the correct IP addresses and names):

```
ping FQDN_component_machine
ping shortname_component_machine
ping ip_address_component_machine
nslookup FQDN_component_machine
nslookup shortname_component_machine
nslookup ip_address_component_machine
```

Using netsh to Trace Communications

Use the **netsh trace** command to capture communication activities between the user terminal and the NES server, while performing the action that fails.

About this task

For example, to troubleshoot the issue where a user terminal cannot retrieve Nymi-enabled Application(NEA) certificates from NES, perform the following steps:

Procedure

1. On the NES server, open up a command prompt as administrator, and then type ***netsh trace start capture=yes tracefile=.\capture_server.etl scenario=internetserver***
2. On the user terminal, open up a command prompt as administrator, and then type ***netsh trace start capture=yes tracefile=.\capture_client.etl scenario=internetclient***
3. Delete all the files in the *C:\Windows\System32\config\systemprofile\AppData\Roaming\Nymi\NSL\randomstring\ksp* directory
4. Perform the action to trigger the certificate retrieval.

   For example:

   - If a user terminal the Evidian EAM Client software cannot retrieve certificates, restart the Enterprise Access Management Security Services service.
   - If the enrollment terminal cannot retrieve the certificates, log into the Nymi Band Application.
5. Wait about a minute and then from the command prompt on both the user terminal and the NES server, type ***netsh trace stop***

   The **netsh** command records the command line output into the filename that you specified with the **tracefile** option in the current directory.
6. Optional, to convert the output file to a text file, type the following command ***netsh trace convert input=filename.etl***

   The command creates a text file with the same name as the *.etl* file in the current directory.
7. For ease of analysis, retrieve .etl file from the machine and use the etl2pcapng tool to convert the file into to a *.pcapng* file.

8. Use an application such as WireShark to analyze the output to determine the communication path between components.

Troubleshooting Bluetooth Issues

Bluetooth Low Energy (BLE) communication between the Nymi Band and the user terminal requires a BLE radio antenna via Nymi-provided BLED112 adapter. The solution presented in this section cover issues resulting from irregular BLE adapter placement and fluctuations in received signal strength indication (RSSI) values.

BLE functionality using a BLED112 adapter requires Nymi Bluetooth Endpoint. Nymi Bluetooth Endpoint is included with the installation of Nymi Runtime.

A Nymi Bluetooth Endpoint configuration file (*nbe.toml*) is provided with the installation of Nymi Bluetooth Endpoint and is located in *C:\Nymi\Bluetooth_Endpoint*. The *nbe.toml* contains default values for the received signal strength indication (RSSI) required to perform an action, such as tapping with the Nymi Band. Refer to *Edit the nbe.toml File* in the Nymi Connected Worker Platform—Administration Guide for more information. Refer to Editing the nbe.toml File on page 113 for guidance on configuring the Bluetooth sensitivity for BLE tap and Nymi Lock Control.

Nymi Bluetooth Endpoint Status Indicator

In Connected Worker Platform(CWP) 1.19.0 and later, the Nymi Bluetooth Endpoint installation, includes the Nymi Bluetooth Endpoint Status Indicator application.

The Nymi Bluetooth Endpoint Status Indicator is an application that runs in the system tray and provides you with the following features:

- Visual method to determine the state of the Nymi Bluetooth Endpoint service
- Ability to troubleshoot issues with the state of the Nymi Bluetooth Endpoint without reviewing the log files
- Ability to restart the Nymi Bluetooth Endpoint with a user account that does not have local administrator privileges to the user terminal.

One of two system tray icons appear for the Nymi Bluetooth Endpoint Status Indicator:

Icon	Description
	This failure icon appears when the Nymi Bluetooth Endpoint encounters one of the following issues: • Cannot connect to the Nymi Agent. • Cannot connect to the Bluetooth adapter. • State of the Nymi Bluetooth Endpoint service is Stopped, Disabled, or Manual (and not started).
	This success icon appears when the all the following conditions are true: • The Nymi Bluetooth Endpoint can connect to the Nymi Agent. • The Nymi Bluetooth Endpoint can connect to the Bluetooth adapter. • The state of the Nymi Bluetooth Endpoint serivce is Started.

Troubleshooting Nymi Bluetooth Endpoint Status Indicator status errors

For status information, hover over the icon. The status information appears in a pop-up over the icon.

The following figure provides an example of the status information when the Nymi Bluetooth Endpoint cannot connect to the Bluetooth adapter:

The following sections summarize the status information messages that can appear when you hover over the Nymi Bluetooth Endpoint Status Indicator and steps that you can perform to resolve the issue.

Bluetooth Adapter is missing

This error message appears when the Nymi Bluetooth Endpoint cannot connect to the Bluetooth adapter.

Resolution

To resolve this issue, ensure that the Bluetooth adapter is plugged into a USB port on the user terminal. If the Bluetooth adapter is plugged into the user terminal, perform one or more of the following actions:

- Remove and re-insert the Bluetooth adapter.
- Insert the Bluetooth adapter into a different USB port on the user terminal.

Nymi Bluetooth Endpoint service is stopped or unreachable

This error message appears when the Nymi Bluetooth Endpoint Status Indicator detects that the Nymi Bluetooth Endpoint service is stopped or in an unresponsive state.

Resolution

Right-click the Nymi Bluetooth Endpoint Status Indicator and click **`Restart`**.

If the restart attempt fails, review the *C:\Nymi\BluetoothEndpointSystemTrayIcon\logs\BluetoothEndpointSystemTrayIcon.log* files for more information.

Failed to connect to Nymi Agent. Duplicate endpoint ID or Failed to connect to Nymi Agent

These message appears when the Nymi Bluetooth Endpoint cannot communicate with the Nymi Agent service.

Resolution

To resolve this issue, right-click the Nymi Bluetooth Endpoint Status Indicator, and then click **`Info`** to see more detailed information, including the URL that Nymi Bluetooth Endpoint uses to connect to the Nymi Agent, as defined in the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file.

If the Agent URL value is incorrect, edit the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file, and then restart the Nymi Bluetooth Endpoint service.

If the Agent URL value is correct, perform the following steps:

- Connect to machine that runs Nymi Agent, and confirm that the Nymi Agent service is running. Nymi Agent.
- If you use a centralized Nymi Agent, confirm that the user terminal and Nymi Agent server can establish a connection on the port that is defined in the *Agent_URL* value:

  1. On the user terminal, open a Powershell prompt, and then type ***tnc -p `port_number` FDQN_agent_server***

     Where *`port_number`* is port number is 9120 by default and *FDQN_agent_server* is the FQDN of the centralized Nymi Agent server.

     A value for *TcpTestSucceeded* that is *`False`* indicates that the client cannot communicate with the Nymi Agent server on the port, and might indicate that you need to update Firewall rules.
  2. On the centralized Nymi Agent, open a Powershell prompt, and then type ***tnc -p port_number FDQN_agent_server***

     Where *port_number* is port number is 9120 by default and *FDQN_user_terminal* is the FQDN of the user terminal.

     A value for *TcpTestSucceeded* that is *`False`* indicates that the Nymi Agent server cannot communicate with the user terminal on the port, and might indicate that you need to update Firewall rules.

Editing the nbe.toml File

About this task

The Nymi Bluetooth Endpoint installation creates a configuration file (*nbe.toml*) in the located in *C:\Nymi\Bluetooth_Endpoint* folder on Windows, and the */usr/bin* directory on HP Thin Pro. This file contains the default values that control BLE tap behavior with the Nymi Band and Bluetooth adapter.

Procedure

1. Make a copy of the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file (On HP Thin Pro, */usr/bin/nbe.toml*).
2. Edit the *nbe.toml* file with a text editor in administrator mode.
3. Edit the RSSI values in the file, as outlined in the following table.

Table 6: RSSI Values

RSSI Value	Default	Description
rssi_window_tap	10	This determines the duration the Nymi Band must be within tap-distance of the BLE radio antenna to complete a tap. A larger value increases the duration required to perform and decrease the sensitivity.
rssi_window_long	50	This determines the frequency that Nymi Bluetooth Endpoint checks the distance between the BLE radio antenna and the Nymi Band. Nymi Bluetooth Endpoint tracks trends in these changes to trigger a Nymi Lock Control action, such as **`keep unlocked when present`**, **`lock when away`**, or **`unlock when present`**.

RSSI Value	Default	Description
rssi_tap_threshold	-42 (must be 0 or negative)	This determines the range at which a tap event will occur. A smaller negative value means a closer distance to the BLE antenna. BLE tap is disabled by default (value = 0). **Enter a non-zero, negative number to enable BLE tap**. Nymi recommends an RSSI value of -42. If the Nymi Band maintains a minimum distance specified by *rssi_tap_threshold*, for the duration of time that is defined by *rssi_window_tap*, a BLE tap is performed.
rssi_cutoff_close	-70 (must be 0 or negative)	This determines the outer range of the close distance-threshold (excluding tap distance) for Nymi Lock Control. Enter 0 to bypass the proximity functionality of Nymi Lock Control. If the Nymi Band maintains a close distance to the BLE radio antenna and the RSSI values measured are within the *rssi_cutoff_close* value, Nymi Lock Control keeps the user terminal unlocked. If the Nymi Band moves away from the BLE radio antenna, and the RSSI values measured are on a decreasing trend and goes from the *rssi_cutoff_close* value to the *rssi_cutoff_far* value, Nymi Lock Control locks the user terminal.

RSSI Value	Default	Description
rssi_cutoff_far	-75 (must be negative)	This determines the outer range of the far distance-threshold (excluding tap distance) for Nymi Lock Control. If the Nymi Band moves towards the BLE radio antenna, and the RSSI values measured are on an increasing trend and goes from the *rssi_cutoff_far* value to the *rssi_cutoff_close* value, Nymi Lock Control unlocks the user terminal.

4. Save the *nbe.toml* file.
5. Restart the Nymi Bluetooth Endpoint.

   On Windows:

   a. Press the Windows key on the keyboard, or click the start button on the toolbar. Enter "Services" in the search bar. The Services application window appears.
   b. Search for **`Nymi Bluetooth Endpoint`** in the Services application.
   c. Right-click **`Nymi Bluetooth Endpoint`** and restart it.

   On HP Thin Pro:

   a. Stop the Nymi Bluetooth Endpoint service by typing ***killall -9 nbed***.
   b. Start the Nymi Bluetooth Endpoint by typing ***/usr/bin/nbedstart***.

Results

Once restarted, the Nymi Bluetooth Endpoint application will be updated with the edits made in the *nbe.toml* file. Updated BLE tap intent and Nymi Lock Control settings will be implemented on the user terminal. If the *nbe.toml* file is not present, Nymi Bluetooth Endpoint behaves under default settings.

BLE Tap Doesn't Work

When you tap your Nymi Band to the BLED112 adapter a tap intent is initiated. BLE taps cannot occur if the BLE radio antenna in the BLED112 adapter does not receive a strong signal from the Nymi Band.

Cause

- The BLED112 adapter is defective.
- The *nbe.toml* file is configured incorrectly.
- There is no clear line-of-sight, or there are objects between the BLE radio antenna and the Nymi Band. Objects will reduce the signal strength received by the antenna.

- The Nymi Band is too far away.
- The Nymi Band is moved away from the BLE radio antenna too quickly.

Resolution

1. Ensure you are tapping the Nymi Band near the BLE radio antenna on the BLED112 adapter.
2. If a BLED112 adapter is used, check that the BLED112 adapter is inserted into a functional USB port. Insert the adapter into another USB port if the port is defective.
3. Go to *C:\Nymi\Bluetooth_Endpoint* and check the *rssi_tap_threshold* parameter in the *nbe.toml* file. The RSSI value should be a non-zero, negative number. Nymi recommends a value around -42. If this value is 0, BLE tap is disabled.
4. Restart Nymi Bluetooth Endpoint on the terminal by going to the **`Services`** application (type "services" in the Windows Start menu). Right-click **`Nymi Bluetooth Endpoint`** and click **`Restart`**.
5. If **`Nymi Bluetooth Endpoint`** is not available, re-install Nymi Runtime and ensure Nymi Agent is included in the installation. Nymi Agent will include Nymi Bluetooth Endpoint.

Nymi Bluetooth Endpoint is Missing (Nymi Runtime)

The error message appears when the Nymi Bluetooth Endpoint attempts to connect to the Nymi Agent.

The *nymi_bluetooth_endpoint.log* file contains the following errors:

```
INFO - Joining new topic: #bluebox:www.xxx.yyy.zzz - {}
                ERROR - Leaving channel: bluebox:www.xxx.yyy.zzz due to: "Channel already joined"
                DEBUG - Replying to reference 1: Response { topic: "bluebox:www.xxx.yyy.zzz", reference:
                Some("1"), payload: Object {"response": Object {"reason": String("Channel already joined")}, "status":
                String("error")}, event: "phx_reply" }
                DEBUG - Send okay: ()
                ERROR - Error in run websocket reconnect loop: ChannelError(ChannelAlreadyJoined)
                INFO - Attempting to reconnect to Agent at ws://hostname:9120/socket/websocket...
                ERROR - Websocket connection closed with code: Error, and reason:
                ERROR - Error sending WS disconnect event: sending on a closed channel
```

The *nymi_agent.log* file contains the following errors:

```
                Start Call: Phoenix.Channel.Server.start_link/?
                Restart: :temporary
                Shutdown: 5000
                Type: :worker
                  I -- CONNECT Smith.API.APISocket
                Transport: :websocket
                Connect Info: %{}
                Parameters: %{}
```

```
I -- Replied Smith.API.APISocket :ok
E -- #PID<0.12686.4> Tried to join existing bluebox:www.xxx.yyy.zzz
  2024-02-16 08:54:42.147 E -- GenServer #PID<0.12686.4> terminating
    ** (KeyError) key :bluebox_id not found in: %{}
    (smith) lib/smith/api/channels/bluebox_channel.ex:57: anonymous fn/2 in
Smith.API.BlueboxChannel.terminate/2
    (logger) lib/logger.ex:867: Logger.normalize_message/2
    (logger) lib/logger.ex:690: Logger.__do_log__/3
    (smith) lib/smith/api/channels/bluebox_channel.ex:56: Smith.API.BlueboxChannel.terminate/2
    Last message: {:join, Phoenix.Channel.Server}
```

Cause

This issue can occur for one of the following reasons:

- Two user terminals have the same IP address
- The user terminal has multiple network connections configured and the user temrinal has switched to another network and received a new IP address.

Resolution

Ensure that each user terminal has a unique IP address. In the event of a network switch, restart the Nymi Bluetooth Endpoint service on the user terminal.

Troubleshooting Nymi WebAPI errors

This section provides you with information about the errors that might appear when you configure Nymi Agent to use Nymi WebAPI

WebAPI Disabled or Nymi Agent Service Stops

Misconfiguration of the Nymi WebAPI can result in the disabling of WebAPI or when you start the Nymi Agent service, the service immediately stops.

The *C:\Nymi\NymiAgent\nymi_agent.log* file provides more information about the cause of the issue.

The following section provides a summary of error message that might appear in the log file as well as several causes and resolutions.

Error logging in to NES: Negotiate error" Authorization has been denied for this request

The error message appears in the *nymi_agent.log* file when the centralized Nymi Agent starts. The Nymi Agent also stops running.

The *nymi_agent.log* file also contains the following messages:

```
I -- Logging in to NES using Negotiate. NES Settings: #NymiCore.NesLogin<cacertfile: nil, credentials_location: nil,
directory_service_id: "nes", nes_url: "https://hostname", verify: :verify_peer, ...>
E -- Error logging in to NES: "Negotiate error: \"Authorization has been denied for this request.\""
E -- WebAPI Start failed: Check WebAPI settings and restart
```

Cause

Misconfigured *nymi_agent.toml* file.

Resolution

To resolve this issue, perform the following steps on the centralized Nymi Agent server:

1. Edit the *C:\Nymi\NymiAgent\nymi_agent.toml* file.
2. Uncomment the *credentials_location* parameter, and then save the file.

3. Restart the Nymi Agent service.

The following figure shows the *credentials_location* parameter setting in the *nymi_agent.toml* file.

```
#
# The (optional) folder containing the encrypted service account information to use when
# logging into NES.
credentials_location = "certs/"
```

Figure 37: credentials_location parameter

Error logging in to NES: Negotiate error: \"WinHTTPConnect returned null. GetLastError: 0\"

The error message appears in the *nymi_agent.log* file when the Nymi Agent starts. The Nymi Agent also stops running.

The *nymi_agent.log* file also contains the following messages:

```
I -- Logging in to NES using Negotiate. NES Settings: #NymiCore.NesLogin<cacertfile: nil, credentials_location: nil,
directory_service_id: "nes", nes_url: "https://hostname", verify: :verify_peer, ...>
E -- Error logging in to NES: "Negotiate error: \"WinHTTPConnect returned null. GetLastError: 0\""
E -- WebAPI Start failed: Check WebAPI settings and restart
```

Cause

Misconfigured *nymi_agent.toml* file.

Resolution

To resolve this issue, perform the following steps on the centralized Nymi Agent server:

1. Edit the *C:\Nymi\NymiAgent\nymi_agent.toml* file.
2. Correct the values for *nes_url* and *directory_service_id* parameters, and then save the file.
3. Restart the Nymi Agent service.

The following figure shows the *nes_url* and *directory_service_id* parameter settings in the *nymi_agent.toml* file.

```
# The host URL for the NES server. This should include only
# the protocol and hostname portion of the URI. Required for WebAPI.
nes_url = "https://tw-srv1.tw-lab.local/"
#
# The NES Directory and Policy Service (DPS) name.
# Check the "About" tab on the NES admin page to find the correct Application Name.
# Application name will be entered for the directory_service_id, eg. NES_DPS.
# Required for WebAPI.
directory_service_id = "nes
```

Figure 38: nes_url and directory_service_id parameters

Error logging in to NES: "Basic Authentication error: \"Perform basic auth with username and

password.: Basic Authentication query returned with a status code of 401 Unauthorized

The error message appears in the *nymi_agent.log* file when the Nymi Agent service starts.The Nymi Agent also stops running.

The *nymi_agent.log* file also contains the following messages:

```
I -- Logging in to NES using service account with username: nymi_infra_service
E -- Error logging in to NES: "Basic Authentication error: \"Perform basic auth with username and password.: Basic Authentication query returned with a status code of 401 Unauthorized.\""
E -- WebAPI Start failed: Check WebAPI settings and restart
```

Cause

Misconfigured Nymi Infrastructure Service Account account.

Resolution

To resolve this issue, perform the following steps on the centralized Nymi Agent server:

1. Re-install Nymi Runtime.
2. On the Nymi Infrastructure Service Account window, include the domain name when you specify the Service Account username, and ensure that you type the correct password.

   The following figure shows the Nymi Infrastructure Service Account window.

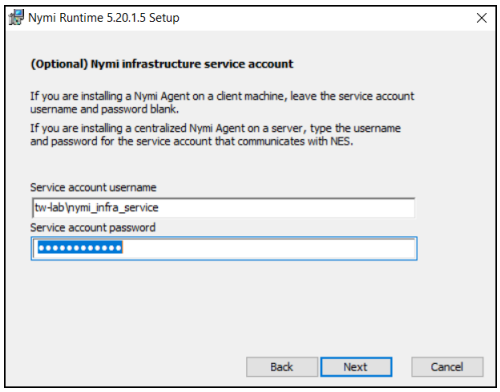


Figure 39: Nymi infrastructure service account window

3. Complete the installation, and then review the *nymi_agent.log* file to confirm that the WebAPI starts without error.

"Error logging in to NES: "Basic Authentication error: \"Perform basic auth on {url} with username and password.\""

The error message appears in the *nymi_agent.log* file when the Nymi Agent service starts. The Nymi Agent also stops running.

The *nymi_agent.log* file contains the following messages:

```
I -- Logging in to NES using service account with username: nymi_infra_service
E -- "Error logging in to NES: "Basic Authentication error: \"Perform basic auth on {url} with username and password.\"
E -- WebAPI Start failed: Check WebAPI settings and restart
```

Cause 1

Misconfigured Nymi Infrastructure Service Account account username or password.

Resolution 1

To resolve this issue, perform the following steps on the centralized Nymi Agent server:

1. In the *C:\Nymi\NymiAgent* folder, create a text file named *creds.txt* that contains two lines with the following values:
   - Username of the Nymi Infrastructure Service Account
   - Password of the Nymi Infrastructure Service Account
2. Open a Command prompt with the **`Run as Administrator`** option.
3. From the command prompt change to the *C:\Nymi\NymiAgent\Tools* directory, and type the following command:

   cryptoutil.exe encrypt-service-account -i C:\Nymi\NymiAgent\creds.text -o C:\Nymi \NymiAgent

   The *Cryptoutil* tool creates the following files in the *C:\Nymi\NymiAgent\certs* folder:
   - credentials-contains the encrypted credentials for the Nymi Infrastructure Service Account
   - Private key
   - Public key
4. Permanently delete the *C:\Nymi\NymiAgent\creds.txt* file.

Cause 2

Misconfigured *directory_id* value in the *nymi_agent.toml* file.

error trying to connect: "tcp connect error: No connection could be made because the target machine actively refused it. (os error 10061)

The error message appears in the *nymi_agent.log* file when the Nymi Agent service starts. The Nymi Agent also stops running.

The *nymi_agent.log* file also contains the following messages:

```
I -- Logging in to NES using Basic and encrypted credentials. NES Settings: #NymiCore.NesLogin<cacertfile:
nil, credentials_location: "certs/", directory_service_id: "nes", nes_url: "https://hostname", verify: :verify_peer, ...></
cacertfile:>
I -- Decrypting credentials using RSA key: c:/Nymi/NymiAgent/certs/key.der
I -- Logging in to NES using service account with username: username
E -- Error logging in to NES: "Basic Authentication error: \"Perform basic auth with username and password.:
Generate request for basic auth query.: error sending request for url (https://hostname/nes/api/BasicLoginWithToken):
error trying to connect: tcp connect error: No connection could be made because the target machine actively
refused it. (os error 10061)
```

Cause

The Nymi Agent cannot connect to IIS.

Resolution

To resolve this issue, perform the following steps:

1. Log into the NES machine and start the IIS service.
2. Start the Nymi Agent service on the centralized Nymi Agent server.
3. Review the *nymi_agent.log* file to confirm that the WebAPI starts without error.

Error logging in to NES: "Unable to load the credentials for BasicLoginWithToken due to a missing credentials file.

After you configure the *nymi_agent.toml* file and restart the Nymi Agent service, the Nymi Agent service stops.

The *nymi_agent.log* file reports the following errors:

```
ERROR - Error logging in to NES: "Unable to load the credentials for BasicLoginWithToken due to a missing
credentials file.
If you do not intend to use an infrastructure service account please comment the credentials_location line in your
nymi_agent.toml.
Otherwise, please generate the infrastructure service account login information using cryptoutil.exe"
```

Cause

This issue appears because the *nymi_agent.toml* is configured to use BasicLoginWithToken but the credentials of the Nymi Infrastructure Service Account account were not encrypted during the Nymi Agent installation.

Resolution

To resolve this issue, perform the following steps:

1. From the command prompt change to the *C:\Nymi\NymiAgent\Tools* directory, and type the following command: ***cryptoutil.exe encrypt-service-account -i C:\Nymi\NymiAgent \creds.text -o C:\Nymi\NymiAgent***

   The *Cryptoutil* tool creates the following files in the *C:\Nymi\NymiAgent\certs* folder:

   - credentials-contains the encrypted credentials for the Nymi Infrastructure Service Account
   - Private key
   - Public key
2. Permanently delete the *C:\Nymi\NymiAgent\creds.txt* file.
3. Place following files in the *C:\Nymi\NymiAgent\certs* folder.
   - CA root certificate bundle in PEM format
   - Server certificate in PEM format
   - Server certificate private key in PEM format
4. Restart the Nymi Agent service.

WARN - WebAPI disabled! Missing CA Certificate Chain file: c:/Nymi/NymiAgent/certs/cert_name

The error message appears in the *nymi_agent.log* file when the Nymi Agent service starts.

Cause 1

Misconfigured *nymi_agent.toml*.

Resolution 1

To resolve this issue, perform the following steps in the Nymi Agent server:

1. Edit the *nymi_agent.toml* file.
2. Correct the value that is defined for the *cacertfile* parameter in the [webapi] section. Ensure that the path to the cert and filename are correct, and that a "/" does not appear before the folder name.
3. Restart the Nymi Agent service.

Cause 2

Nymi WebAPI is configured for WSS but the certificate files are not in the *certs* folder.

Resolution 2

To resolve this issue, copy the following files to the *C:\Nymi\NymiAgent\certs* folder, and the restart the Nymi Agent service.

- CA root certificate bundle in PEM format (when you use a Trusted Root CA only)
- Server certificate in PEM format
- Server certificate private key in PEM format

WS:Closed Message when NEA connects to Agent URL

The error message appears when the Nymi-enabled Application(NEA) attempts to connect to the Agent URL server.

Cause

Nymi Agent uses secure websocket (wss) and the TLS key file is encrypted.

Resolution

To resolve this issue, generate the TLS key file in an unencrypted PEM format, and then perform the following actions on the Nymi Agent server:

1. Replace the key file in the *C:\Nymi\NymiAgent\certs* folder.
2. If required, edit the *nymi_agent.toml* file and edit the key file name that is defined by the *keyfile* parameter.
3. Restart the Nymi Agent service.

Troubleshooting SPN Issues

You can configure the Nymi Enterprise Edition and Connected Worker Platform(CWP) solutions use Kerberos to authenticate service requests between components such as the NES server, user terminals and centralized Nymi Agent. Service principal names (SPNs) uniquely identifies the NES instance for HTTP and HTTPS communication.

About this task

When the SPN is not set correctly for the Application Pool Identity account, communication between the NES server and other components in the solution infrastructure to fail.

To troubleshoot and resolve SPN issues, perform the following step on the NES server:

Procedure

1. Determine which account is assigned to the Application Pool Identity.
   a) Open `IIS Manager` and expand the server. Select **`Application Pools`**.
   b) In the **`Application Pools`** table, make note of the account that is specified in the **`Identity`** column.
      In the following example, the Application Pool Identity is LocalSystem.
2. Open a command prompt as Administrator, and then type the following command to view the existing SPN entries that are associated with the Application Pool Identity account:

   setspn -l %computername% | App_Pool_Identity

   Note: Only include ***| App_Pool_Identity*** if the Application Pool Identity is not a local account, such as *NetworkService*, or *LocalSystem*.

   The following output provides an example of correctly configured SPNs, which include the HTTP entries:

   ```
   Registered ServicePrincipalNames for CN=TW-SRV2,CN=Computers,DC=TW-Lab,DC=local:
   HTTP/Tw-Srv2.tw-lab.local
   HTTP/TW-SRV2
   WSMAN/TW-Srv2
   WSMAN/TW-Srv2.TW-Lab.local
   RestrictedKrbHost/TW-SRV2
   HOST/TW-SRV2
   RestrictedKrbHost/TW-Srv2.TW-Lab.local
   HOST/TW-Srv2.TW-Lab.local
   ```

3. If the HTTP SPN is not set to the correct Application Pool Identity, delete the existing entries by typing the following commands:

   setspn -d HTTP/%computername% %computername% setspn -d HTTP/ %computername%.%userdnsdomain% %computername%

where *%userdnsdomain%* is replaced with the DNS name or Fully Qualified Domain Name (FQDN) of the NES domain if the If the user account that is performed the **setspn** command is a member of a domain that differs from domain.

4. Type the following commands to set the SPN to the Application Pool Identity account:

   setspn -S HTTP/nes_hostname:port nes_hostname | App_Pool_Identity setspn -S HTTP/nes_hostname.domain:port nes_hostname | App_Pool_Identity

   Where:

   - *nes_hostname* is the hostname of the NES server.
   - *:port* is required only when NES is not configured for traffic on the standard ports (HTTP/80, HTTPs/443) domain is replaced with the DNS name or Fully Qualified Domain Name (FQDN) of the NES domain if the user account that is performing the **setspn** command is a member of a domain that differs from the NES domain.
   - *App_Pool_Identity* is the name of the Application Pool Identity account.

   When the command completes successfully, output similar to the following appears.

   ```
   Checking domain DC=TW-Lab,DC=local

   Registering ServicePrincipalNames for CN=TW-SRV2,CN=Computers,DC=TW-Lab,DC=local
   HTTP/Tw-Srv2.tw-lab.local
   Updated object
   ```

5. If the NES server is clustered and netBIOS domain name of the NES server differs from the FQDN of the public domain, type the following command:

   setspn -S HTTP/%computername%.publicdomain:port# %computername% | App_Pool_Identity

   where:

   - nes_hostname is the hostname of the NES server.
   - :port is required only when NES is not configured for traffic on the standard ports (HTTP/80, HTTPs/443)
   - publicdomain is replaced with the FDQN domain name of NES cluster.
   - *App_Pool_Identity* is the name of the Application Pool Identity account.

Resolving certificate issues

This section provides information about how to determine if the certificates that the components of the Connected Worker Platform use have expired and how to replace expired certificates.

Note: For information about L2 Certificate Expiry, see Resolving certificate issues

Determining if a certificate expired

This section describes how to determine if the TLS or Root CA certificate has expired.

TLS certificate

Perform the following steps on the NES host, in `IIS Manager` to review information about the TLS server certificate.

- In the `Connections` navigation pane, expand ***`Computer_Name`***, and then in the **`IIS`** section, double-click **`Server Certificates`**.
- In the `Server Certificates` window, review the date in the **`Expiration Date`** column to determine if the TLS certificate has expired.

Root CA certificate

Perform the following steps on a network device that has the Root CA certificate in the Trusted Root Certification Authorities store.

- In `Control Panel`, select **`Manage Computer Certificates`**.
- In the `certlm` window, expand **`Trusted Root Certification Authorities > Certificates`**.
- Review the date in the **`Expiration Date`** column to determine if the Root CA certificate has expired.

Replacing an expired root certificate

Before a network device can access the NES Administrator Consoleand the Nymi Band Application, a valid root CA certificate must exist in the Trusted Root Certification Authorities store.

About this task

While logged into the user terminal as a local administrator, use the `certlm` application to import the root CA certificate into the Trusted Root Certification Authorities store. For example, on Windows 10, perform the following steps:

Procedure

1. In `Control Panel`, select **`Manage Computer Certificates`**.
2. In the `certlm` window, right-click **`Trusted Root Certification Authorities`**, and then select **`All Tasks > Import`**.

   The following figure shows the `certlm` window.

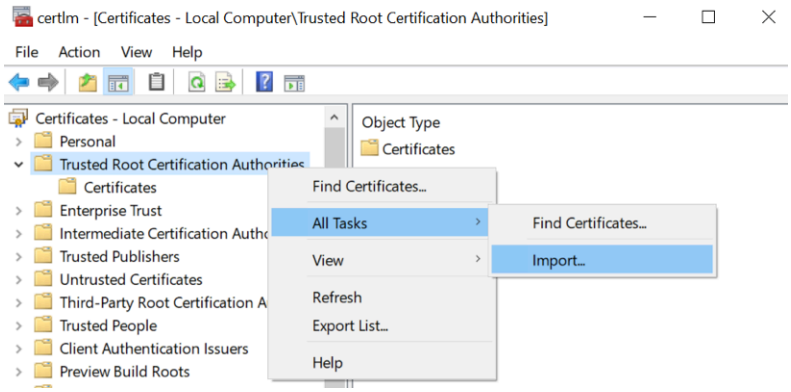


Figure 40: certlm application on Windows 10

3. On the `Welcome to the Certificate Import Wizard` screen, click **`Next`**.

   The following figure shows the `Welcome to the Certificate Import Wizard` screen.

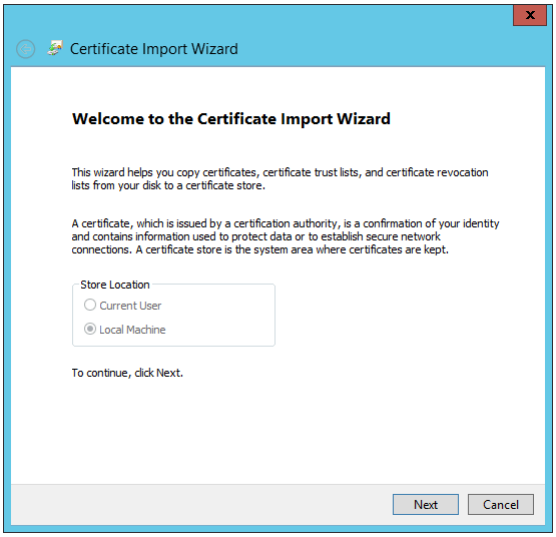


Figure 41: Welcome to the Certificate Import Wizard screen

4. On the `File to Import` screen, click **`Browse`**, navigate to the folder that contains the root certificate file, select the file, and then click **`Open`**.
5. On the `File to Import` screen, click **`Next`**.

The following figure shows the `File to Import` screen.

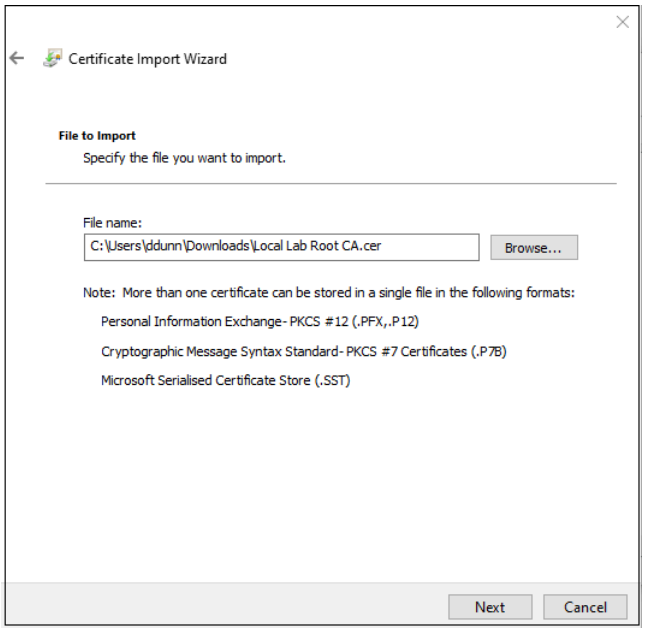


Figure 42: File to Import screen

6. On the `Certificate Store` screen, accept the default value **`Place all certificates in the following store`** with the value **`Trusted Root Certification Authorities`**, and then click **`Next`**.
7. On the `Completing the Certificate Import Wizard` screen, click **`Finish`**.

What to do next

You must replace the certificate on the NES host and all network devices that communicate with the NES host.

Replacing an expired TLS certificate

Perform the following steps on the NES host to replace an expired TLS certificate.

1. Open `IIS Manager`.
2. In the `Connections navigation` pane, expand *`Computer_Name`*, and then in the **`IIS`** section, double-click **`Server Certificates`**.

   Note: If you cannot find **`Server Certificates`**, click the **`Features View`** tab, which appears at the bottom of the window.
3. In the `Actions` navigation pane, on the right side of the window, click **`Import`**.
4. In the `Import Certificate` window perform the following actions:

   a. In the **`Certificate file (.pfx)`** field, click the ellipsis (…) button.
   b. Change the extension list to **`*.*`**.

c. Browse to the location of the TLS certificate, select the certificate file, and then click **Open**.
d. In the **Password** field, type the password that was used to encrypt the private key.
e. In the **Select Certificate Store** list, select **Web Hosting**.
f. Click **OK**.

5. In the Connections navigation pane, expand ***Computer_Name*** **> Sites**.
6. Right-click **Default Web Site**, and then select **Edit Bindings**.
7. Select **https** and then click **Edit**.
8. In the **SSL certificate** list, select the name of the new TLS certificate.
9. Click **OK**.
10. Click **Close**.

Using Self Signed TLS Certificate

Nymi recommends that you use a TLS certificate that is created by a Trusted CA. If you cannot obtain this certificate, you can create a self-signed certificate.

To deploy a self signed certificate, you must perform the following actions, as described in the following section:

- Create the self-signed certificate in IIS
- Modify the site bindings in IIS to use the self-signed certificate
- Confirm that NES uses the self signed certificate
- Export the self-signed certificate in IIS
- Import the self-signed certificate on the enrollment terminal and each user terminal

Creating a Self Signed Certificate

Use IIS Manager to create a self signed certificate.

About this task

Procedure

1. In the Connections navigation pane, select the server name, and then double-click **Server Certificates**, as shown in the following figure.

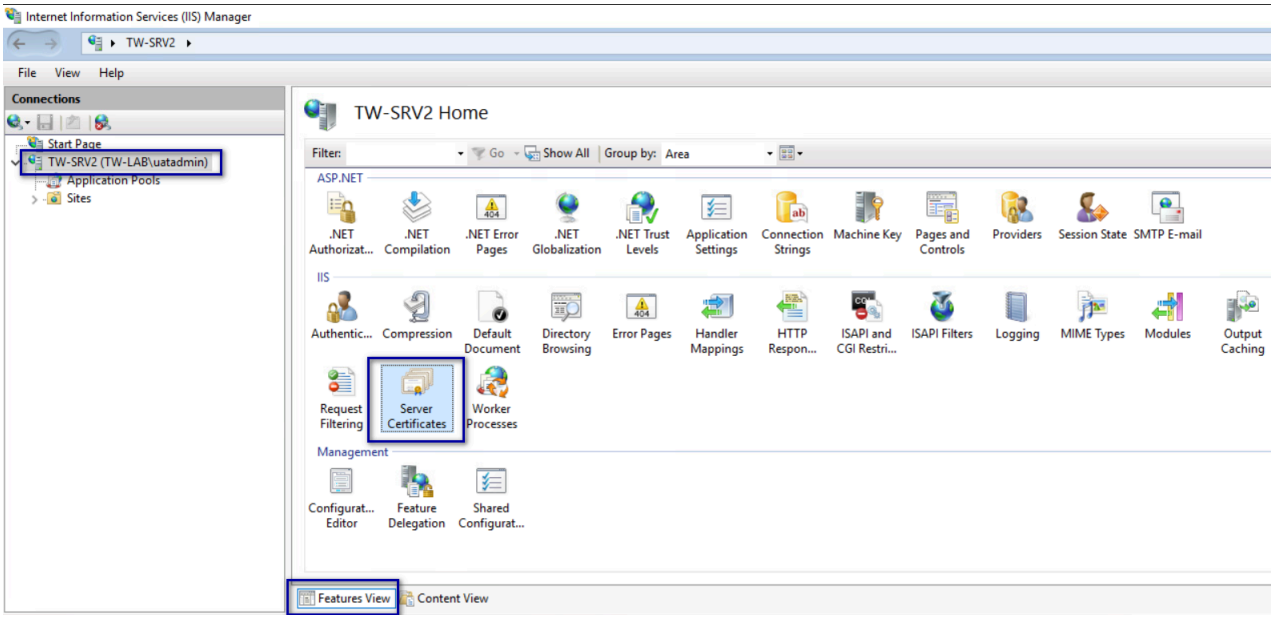


Figure 43: Server Certificates option in IIS Manager

2. From the `Actions` pane, click **`Create Self Signed Certificate`**.
3. In the `Specify a friendly name for the certificate` field, specify a name of your choosing to identify the certificate, and then click **`OK`**.
   The new certificate appears in the `Server Certificates` window.

Editing IIS Binding

Bind the Self Signed Certificate to the default web site

About this task

Perform the following actions in IIS Manger

Procedure

1. In the `Connections navigation` pane, expand ***`Computer_Name`*** **`> Sites`**.
2. Right-click **`Default Web Site`**, and then select **`Edit Bindings`**.
3. Select **`HTTPs`**, and then click **`Edit`**
4. From the **`SSL Certificate`** list, select the self signed certificate, and then click **`OK`**.
5. Click **`Close`**.

Restarting IIS

Use an account with administrative privileges to restart IIS.

Procedure

1. From the Start menu, click `Run`.
2. In the Open box, type `cmd`, and click `OK`.
3. At the command prompt type, ***iisreset/noforce***.
   IIS attempts to stop all services before restarting. The `IISReset` command-line utility waits up to one minute for all services to stop.

Validating the TLS Certificate in NES

Perform the following steps to validate that NES uses the self signed certificate.

Procedure

1. Connect to the NES Administrator Console in a browser by typing ***https://`nes_server`/`NES_service_name`*** or ***http://`nes_server`/`NES_service_name`*** depending on the NES configuration, where:
   - *`nes_server`* is the Fully Qualified Domain Name (FQDN) of the NES host.
   - *`NES_service_name`* is the service mapping name for the NES web application. The default service mapping name is *nes*.

     For example, ***https://nes.cwp.company.com/nes***.

     Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.
2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click **`Sign In`**.
3. On the main menu, click **`About`**.
   The `System Diagnostics` page appears.
4. Click **`View Full System Diagnostics`**. When the test completes, review the status of the diagnostic test results and confirm that the TLS certificate test displays a **Pass** status, as shown in the following figure.

Exporting the Self Signed Certificate

Use `IIS Manager` to export the self signed certificate.

About this task

You will import this certificate on each user terminal and the enrollment terminal.

Procedure

1. Open `IIS Manager`.
2. In the `Connections` navigation pane, select the server name, and then double-click **`Server Certificates`**, as shown in the following figure.

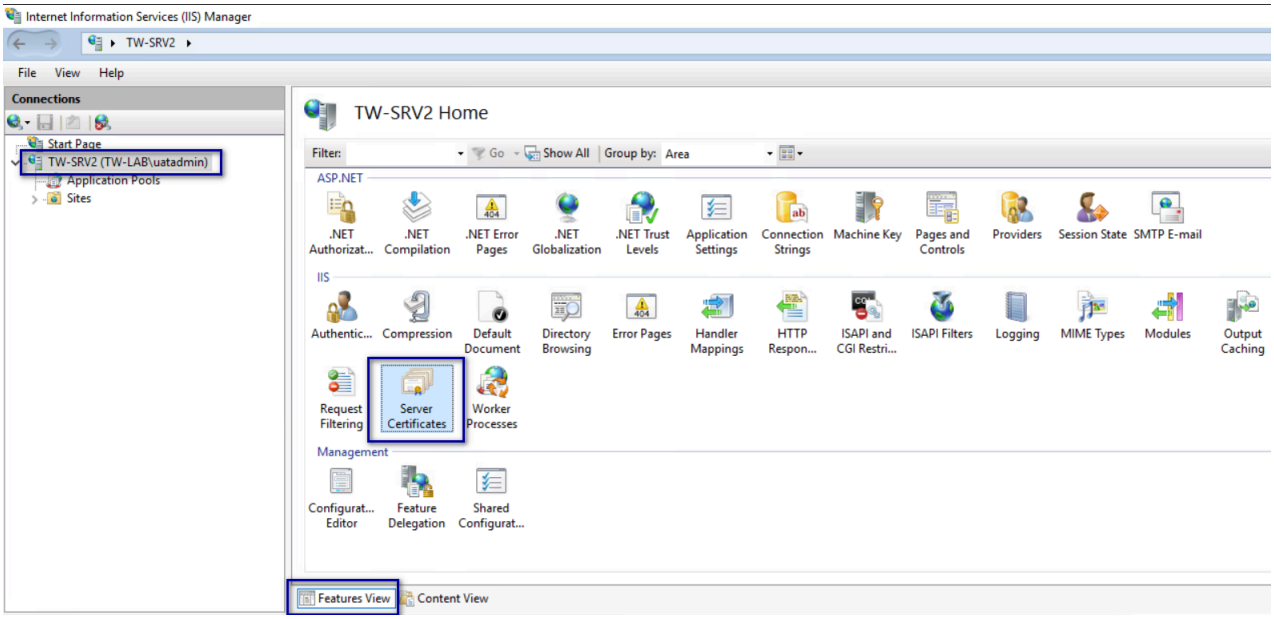


Figure 44: Server Certificates option in IIS Manager

3. In the **`Server Certificates`** list, right-click the self signed certificate, and then select **`Export`**.
4. In the `Export Certificate` window, provide a name for the certificate.
5. In the **`Password`** and **`Confirm password`** fields, type a password for the certificate file.
6. Click **`OK`**.
   The PFX file is stored in the *Documents* folder for the user that performed the action.

Importing Self Signed Certificate

Perform the following steps on the enrollment terminal and all user terminals.

About this task

Log into the machine with a user that has local administrator access.

Procedure

1. Obtain a copy of the exported self signed certificate (PFX file).
2. Right-click the certificate file, and then select **`Install PFX`**.
3. In the `Open File - Security Warning` dialog, click **`Open`**.
   The Certificate Import Wizard dialog box opens.
4. On the `Welcome to the Certificate Import Wizard` page, in the **`Store Location`** page, select **`Local Machine`**, as shown in the following figure.

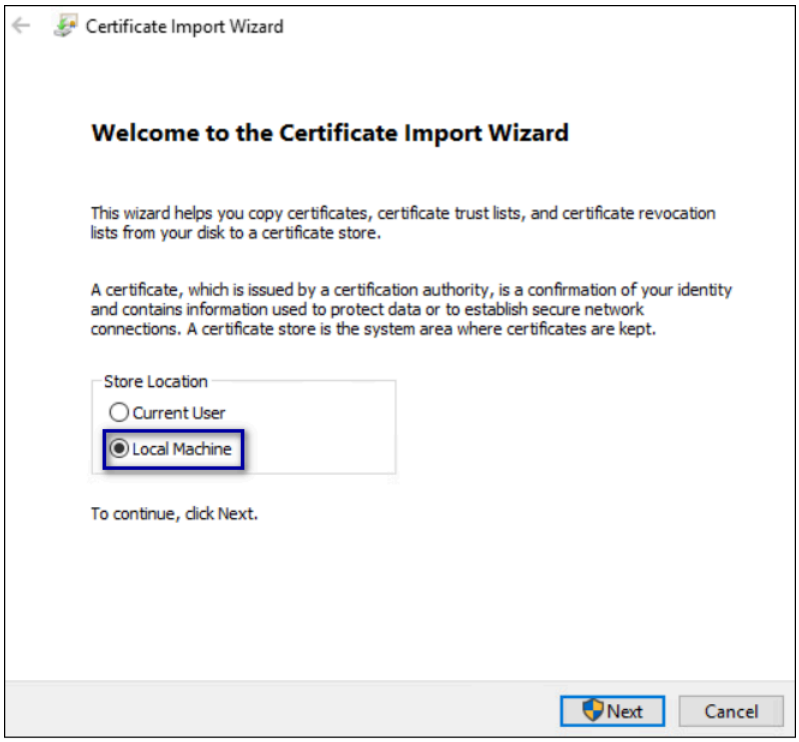


Figure 45: Local Machine Store Location

5. Click **`Next`**.
6. On the `User Account Control` window, click **`Yes`**.
7. On the `Files to import` page, ensure that the self signed certificate file appears in the **`File name`** field, and then click **`Next`**.
8. On the `Private Key Protection` page, in the `Password` field, type the private key password, and then click **`Next`**.

   The following figure provides an example of the `Private Key Protection` page.

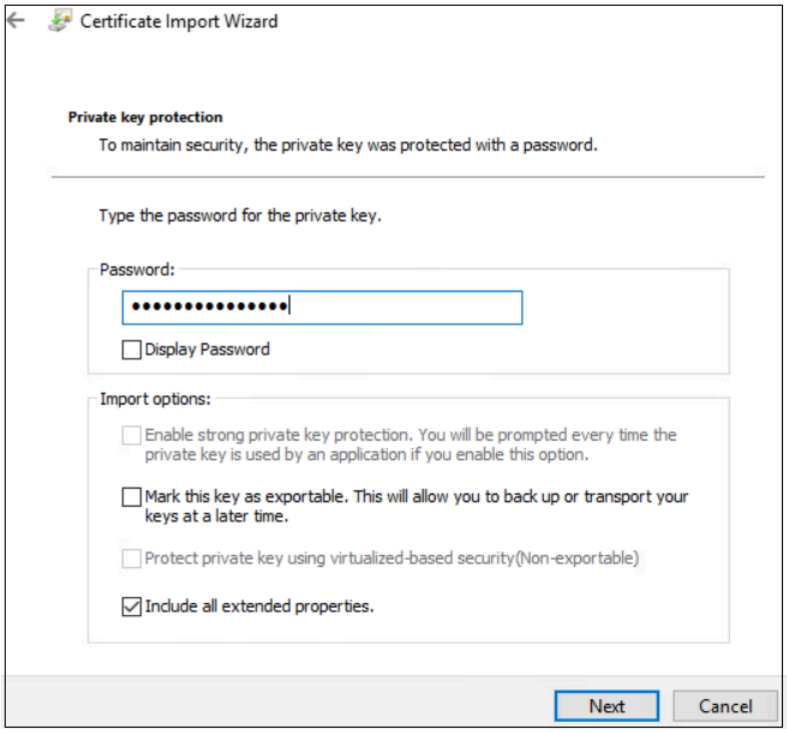


Figure 46: Private Key Protection Page

9. On the `Certificate Store` page, select **`Place all certificates in the following store`** then click **`Browse`**.
10. Select **`Trusted Root Certification Authorities`**.
11. Click **`Next`**.
12. On the `Completing the Certificate Import Wizard` page, click **`Finish`**.
13. On the `Certificate Import Wizard` dialog, click **`OK`**.

Replacing the L1 and L2 Certificates

The Nymi solution requires L1 and L2 certificates to support secure communications. Nymi delivers the L1 and L2 certificates in a fullchain PKCS12 file, which has an expiration date. You must replace the certificates before the expiration date, to continue to use the Nymi solution.

The PKCS12 file (fullchain.p12) contains the following key and certificates.

- L1 certificate
- L2 certificate
- L2 private key

Note: Nymi provides these file in a zip file that is protected by a password. Nymi provides the password to you separately from the file package.

Perform the following steps to replace the certificates:

- Delete the existing L1 and L2 certificates.
- Importing the Nymi-provided full chain certificate.
- Provide the Application Pool Identity account with access to the private key.
- Restart the IIS.

Deleting Existing Certificates

Perform the following steps to delete the L1 and L2 certificates.

Procedure

1. Right-click **`Start`**, select **`Run`**, and then type ***Manage Computer Certificates***.
2. In the `Console` window, in the left navigation pane, expand **`Certificates > Intermediate Certificates Authorities > Certificates`**.
3. Delete the L1 and L2 certificates.

   The following figure provides an example of the L1 and L2 certificates.

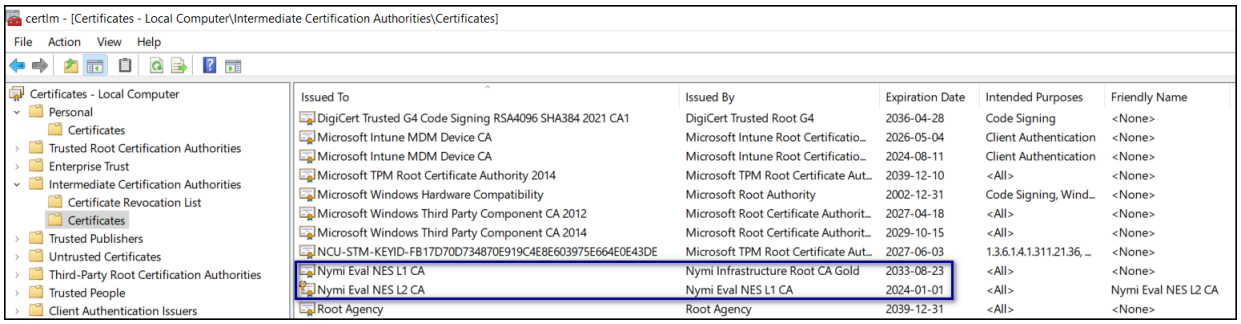


Figure 47: L1 and L2 Certificates in Intermediate Certificate Store

Importing Certificates

Perform the following steps to import the certificates on the NES host.

Procedure

1. Extract the certificate zip file to a directory.
2. Right-click the *fullchain.p12* certificate file, and then select **`Install PFX`**, as shown in the following figure.

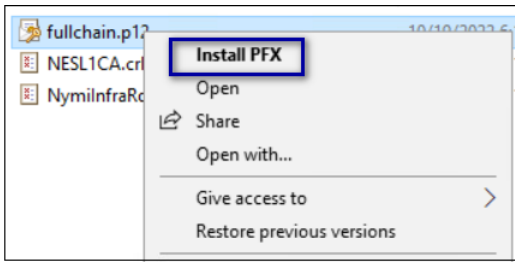


Figure 48: Install PFX Option

3. In the `Open File - Security Warning` dialog, click **`Open`**.

   The Certificate Import Wizard dialog box opens.

4. On the `Welcome to the Certificate Import Wizard` page, in the **`Store Location`** page, select **`Local Machine`**, as shown in the following figure.

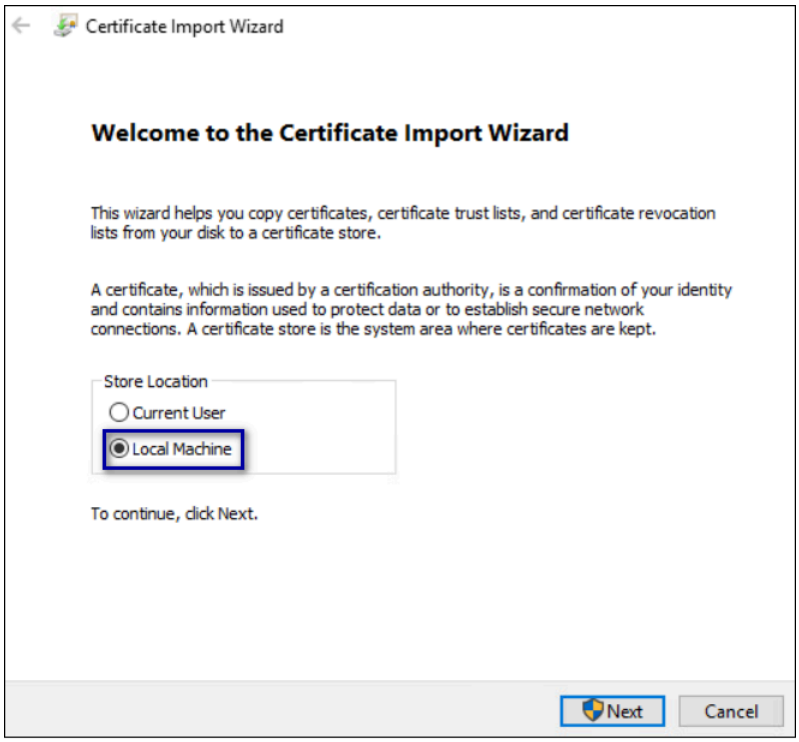


Figure 49: Local Machine Store Location

5. Click **`Next`**.
6. On the `User Account Control` window, click **`Yes`**.
7. On the `Files to import` page, ensure that the fullchain.p12 file appears in the *File* name field, and then click **`Next`**.
8. On the `Private Key Protection` page, in the `Password` field, type the Nymi-provided private key password, and then click **`Next`**.

   The following figure provides an example of the `Private Key Protection` page.

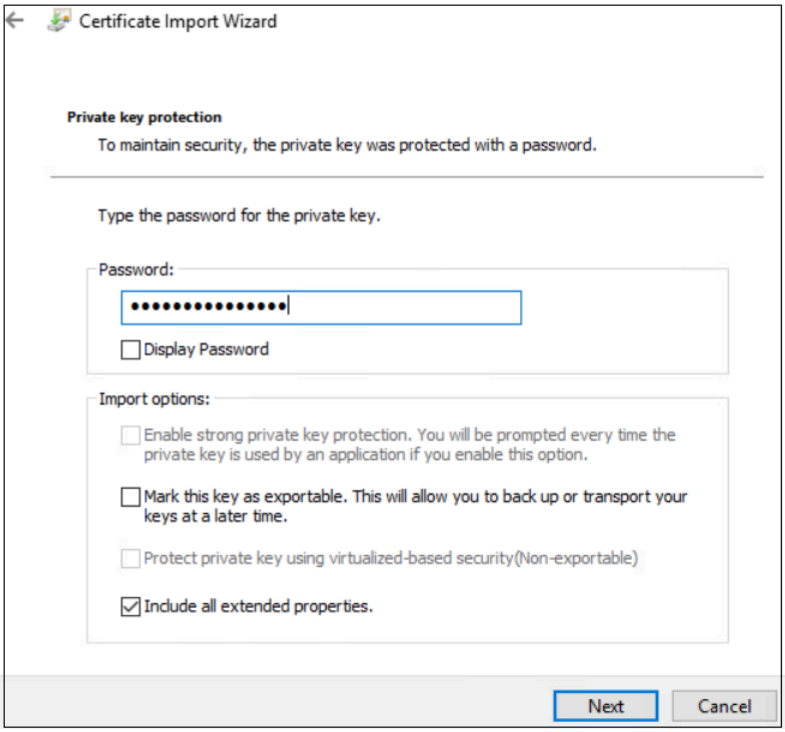


Figure 50: Private Key Protection Page

9. On the `Files to import` page, ensure that the *fullchain.p12* file appears in the **`File name`** field, and then click **`Next`**.
10. On the `Certificate Store` page, leave the default option Automatically select the certificate store based on the type of certificate, and then click **`Next`**.

    This options ensures all the certificates in the certification path (Root, Intermediate) are placed in the correct store. The following figure provides an example of the Certificate Store page.

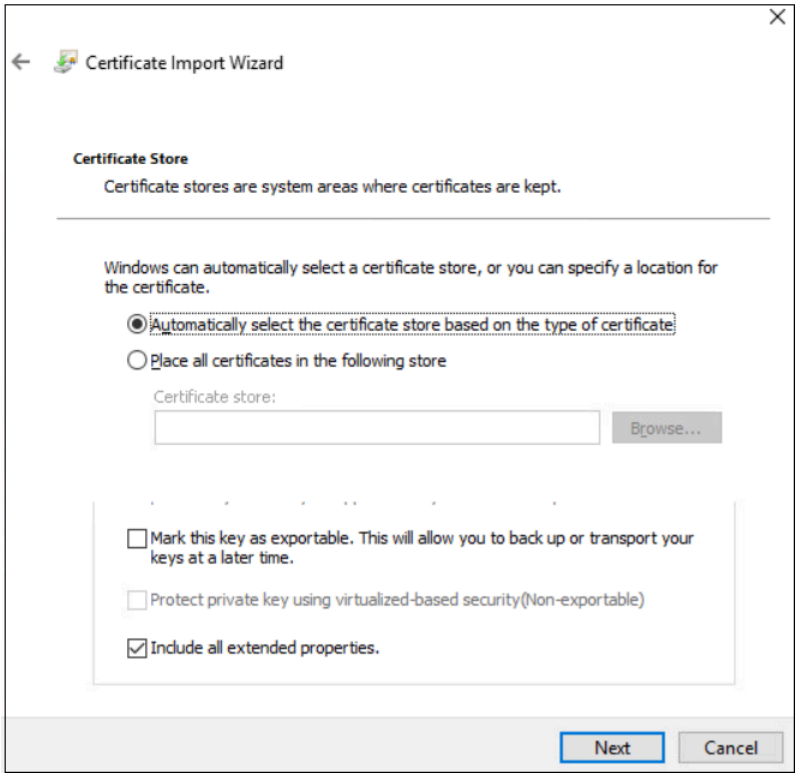


Figure 51: Certificate Store Page

11. On the `Completing the Certificate Import Wizard` page, click **`Finish`**.
12. On the `Certificate Import Wizard` dialog, click **`OK`**.

Managing Private Keys

If the account used for the NES IIS Application Pool is not LocalSystem, perform the following procedure to grant Application Pool Identity account access to the L2 private key.

Procedure

1. From the `Windows Start Menu`, type ***Manage Computer***, and then select `Manage Computer Certificates`.
   The `certlm` window appears.
2. Navigate to **`Personal > Certificates`** folder.
   A list of certificates displays.
3. Right-click the NES L2 CA and select **`All Tasks`** and then select **`Manage Private Key...`**.
4. On the `User Account Control` dialog, click Yes.
5. Select the **`Security`** tab and then click the **`Add`** button.
6. In the new window, click **`Add`**, which opens the **`Select Users, Computers, Service Accounts, or Groups`** window.

7. Type the account that you selected for the NES Application Pool, and then click **OK**.
8. In the **Permissions** area, under **Allow** column, select the **Read** permission.

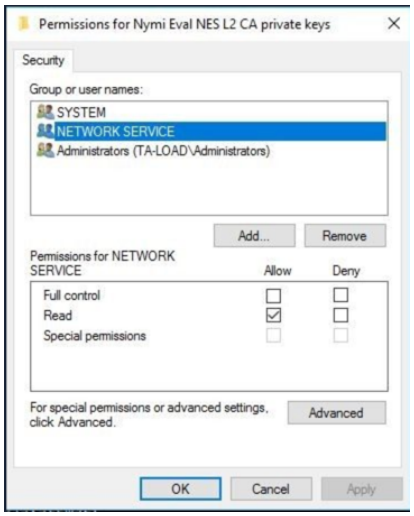


Figure 52: Setting Private Key Permissions

9. Click **OK**.

Moving the L2 Certificate

Perform the following steps to move the L2 certificate from the Personal store to the Intermediate Certification store.

Procedure

1. Expand **Intermediate Certification > Certificates** and then move the NES L2 CA certificate from **Personal > Certificates** to the **Intermediate Certification > Certificates**

   You can move the file by dragging and dropping it from one folder to the other folder.
2. In **Intermediate Certification > Certificates**, verify that the NES L2 CA certificate has a key.

   When the L2 certificate has a key, a key symbol displays in the upper-left corner of the L2 certificate icon.
3. Record the expiration date of the NES L2 CA certificate (shown in the Expiration Date column) in the Certificate Expiration Dates table, that was provided in the Nymi Connected Worker Platform—Deployment Guide.
4. Close the `certlm` window.

Restarting IIS

Use an account with administrative privileges to restart IIS.

Procedure

1. From the Start menu, click `Run`.
2. In the Open box, type `cmd`, and click `OK`.
3. At the command prompt type, ***iisreset/noforce***.
   IIS attempts to stop all services before restarting. The `IISReset` command-line utility waits up to one minute for all services to stop.

Updating Certificates in Nymi Enterprise Server

When you replace a Nymi Eval L1 and L2 certificate with a production L1 and L2 certificate, you must run the Nymi Enterprise Server(NES) installation wizard and select the new certificates.

About this task

Perform the following steps on the NES server.

Procedure

1. From the directory that contains the extracted NES installation package, run *..\NesInstaller \install.exe.*
2. On the `User Access Control` window, click **`Yes`**.
3. On the `Open File - Security warning` window, click **Run**.
4. On the left navigation pane, click **`Location`**, and then perform the following steps.
   a) In the **`Install Root`** field, confirm that the path to the NES services is correct, as it was specified during the initial deployment.

      The default location is *C:\inetpub\wwwroot*.
   b) In the **`Instance Name`** field, type the descriptive name that was specified during the initial deployment for the NES web application instance name. For example, NES. See Configuration Attribute Values in the Nymi Connected Worker Platform—Deployment Guide.

      Note: Ensure that the values that you specify in the **`Install Root`** and **`Instance Name`** match the values that you specified when you deployed the previous version of NES. When the values that you specified in the **`Install Root`** and **`Instance Name`** are correct, the **`Location`** test results will show Install Type: Update/ Re-Install. If there is no match for the values entered, the **`Location`** test results will show New Installation for the Install Type. The following figure provides an example of the **`Location`** window for an NES upgrade.

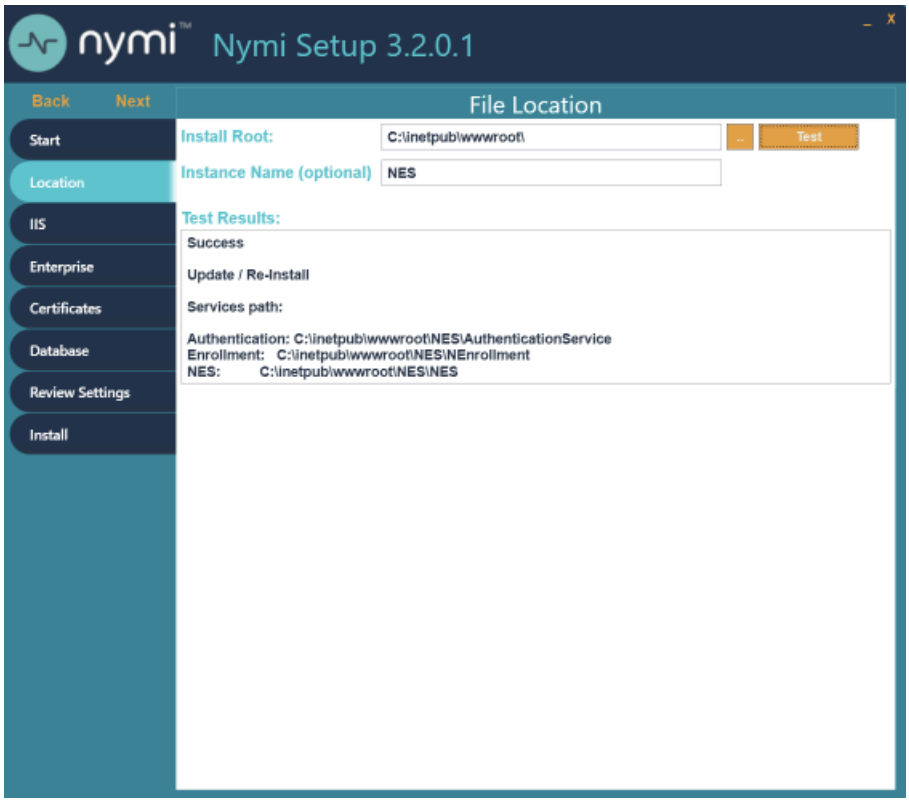


Figure 53: Update / Reinstall installation type

5. In the left navigation pane, select `IIS`, and confirm that values that appear are correct.
6. Review the contents of the `Enterprise` tab, and confirm that values that appear are correct.
7. In the left navigation pane, click **`Certificates`**, and perform the following actions.
   a) From the **`Level One Certificate`** list, select the L1 certificate from the list.
      The L1 certificate name is in the form *`enterprise_name`* ***NES L1*** CA.
   b) From the **`Level Two Certificate`** list, select the L2 certificate.
   c) For NES 1.14.2 and later, from the **`Full Chain`** list, click the ellipses (...) and navigate to the folder that contains Full Chain PFX certificate file, and then select the file.
   d) For NES 1.14.2 and later, in the `Password Required` pop-up, type the Full Chain certificate password, and then click **`OK`**.

   The following figure provides an example of the `Certificates` page.

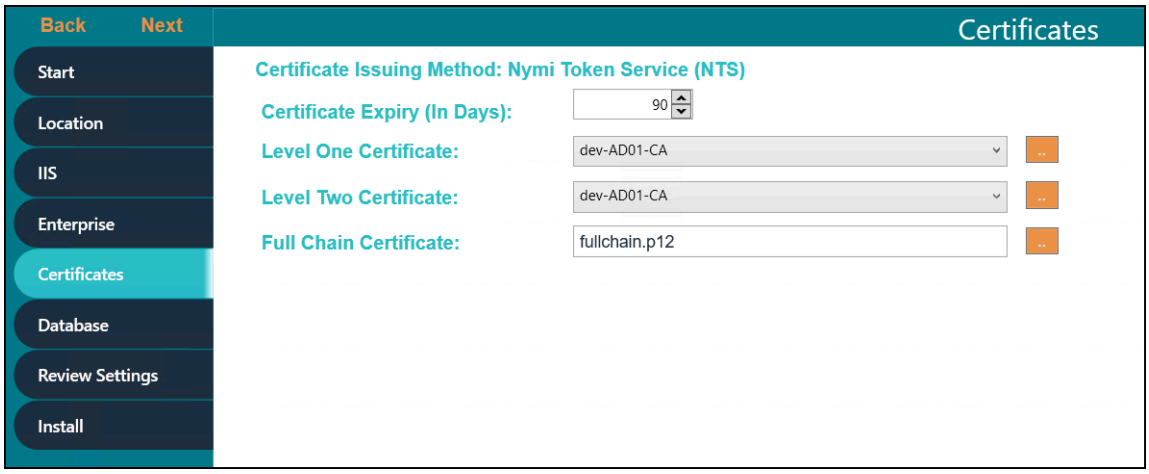


Figure 54: Certificates page in the NES Setup wizard

8. In the left navigation pane, click `Database`, and confirm that values that appear are correct.
9. In the left navigation pane, click `Review Settings`. The parameters for the NES installation are displayed for final review. Click **`Test`** to verify the configuration. Review the test results and address any errors if applicable.
10. In the left navigation pane, click `Install`, and then click **`Update`**.

    Note: If the update option is not available, the **`Install Root`** or **`Instance Name`** fields on the **`Location`** tab are not the same values that were specified when you deployed the previous NES version.
11. On the `Update NES` window, click **`Yes`** to reapply the configuration.
    The `Install` window display the status of the update process.
12. When the `Install` window displays the Installation Complete message, close the `Nymi Setup` window.

Submitting a Support Request

You can submit a support request to Nymi from the NES Administrator Console.

About this task

Procedure

1. In the NES Administrator Console, click **Support**.
2. Click **Submit a ticket**.
3. In the **Subject** field, provide a short description of the issue and the name of your company.
4. From the **Submit a request list**, select the appropriate option for your issue, for example, Nymi Customers - Technical Support.
5. In the **Description** field, provide the details about the issue that you are seeing.
6. Optionally, attach the Nymi Band Application log files and NES support tool output.
7. Click **Submit**.

Note: For information on the NES support tool, refer to the Nymi Connected Worker Platform—Administration Guide for more information.

Published in Canada.
Nymi Inc.
Toronto, Ontario
www.nymi.com