Troubleshooting Guide

Nymi Connected Worker Platform

v7.0

2022-02-04

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 product 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
7.0	February 4, 2022	Updated for the CWP 1.2.1 release.
6.0	November 10, 2021	Updated for the CWP 1.2 release.
5.0	May 3, 2021	Updated to reflect Nymi Enterprise Edition rebrand to Connected Worker Platform. This update includes content for Windows Lock Control, and Smart Distancing and Contact Tracing.
4.0	February 26, 2021	Update of this document for the Nymi Enterprise Edition 3.4.0 release. This includes authentication lockout and updates to retrieving the log file.
3.0	December 18, 2020	Update of this document for the Nymi Enterprise Edition 3.3.0 release. • Updates to NES log file chapter.

Version	Date	Revision history
2.0	September 18, 2020	Update of this document for the Nymi Enterprise Edition 3.2.0 release.
1.0	April 15, 2020	This guide is reissued due to document version update. There are no content changes since Nymi Enterprise Edition 2.6.0.

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 NES Deployment Guide**

  This document provides the steps that are required to deploy the Nymi Enterprise Server (NES). This installation uses the `Nymi Token Service` to install certificates that enable communication between components. This document also provides information about deploying the Connected Worker Platform in a Citrix or RDP environment.
- **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 API for Linux Application and Developer's Guide**

  This document provides information about how to use the functionality that is available in the `NAPI` that is part of the Connected Worker Platform.
- **Nymi API C Interface Application and Developer's Guide**

  This document provides information about how to use the functionality that is available in the `NAPI` that is part of the Connected Worker Platform.
- **Nymi API WebSocket Interface Application and Developer's Guide**

  This document provides Nymi developers with an alternative way to utilize the functionality of the `Nymi SDK`, over a WebSocket connection managed by a web-based or other applications.
- **Connected Worker Platform Release Notes**

  This document provides supplemental information about the Connected Worker Platform, including new features, limitations, and known issues with the Connected Worker Platform components.

How to get product help

If the Nymi software or hardware does not function as described in this document, contact your administrator for immediate support. Alternatively, 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.

Nymi Band Application 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.

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.

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.

NES log files

The NES host has separate log files for each web service. When you encounter an issue, enable verbose mode for each web service, retry the operation, and then review the messages that appear in each log file.

Enabling Verbose Logging

When you encounter an issue, enable verbose mode for each web service, retry the operation, and then review the messages that appear in each log file. There are different log levels available for NES, they are Critical, Error, Warning, Information, and Verbose, listed in the order of increasing level of details provided in the logs.

To enable verbose logging mode, perform the following steps:

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>
   ```

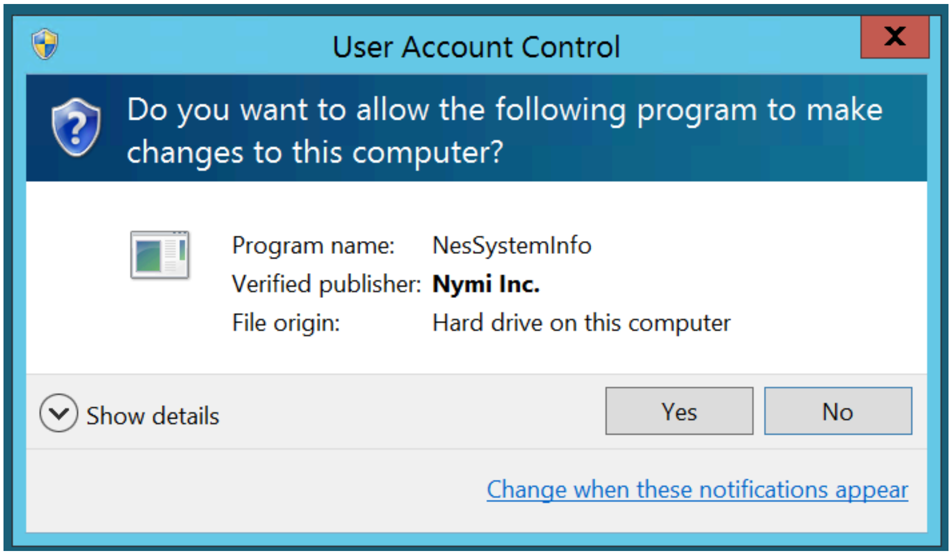
4. Restart the IIS.

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.

Follow these steps to generate a log zip file.

1. On the computer running NES, open Windows Explore and navigate to the directory that contains the NES Installation package folder in the *NesSystemInfo* subfolder.
2. Double-click `NymiSupportTool.exe`
   The `User Account Control` dialog box appears.



User Account Control

Do you want to allow the following program to make changes to this computer?

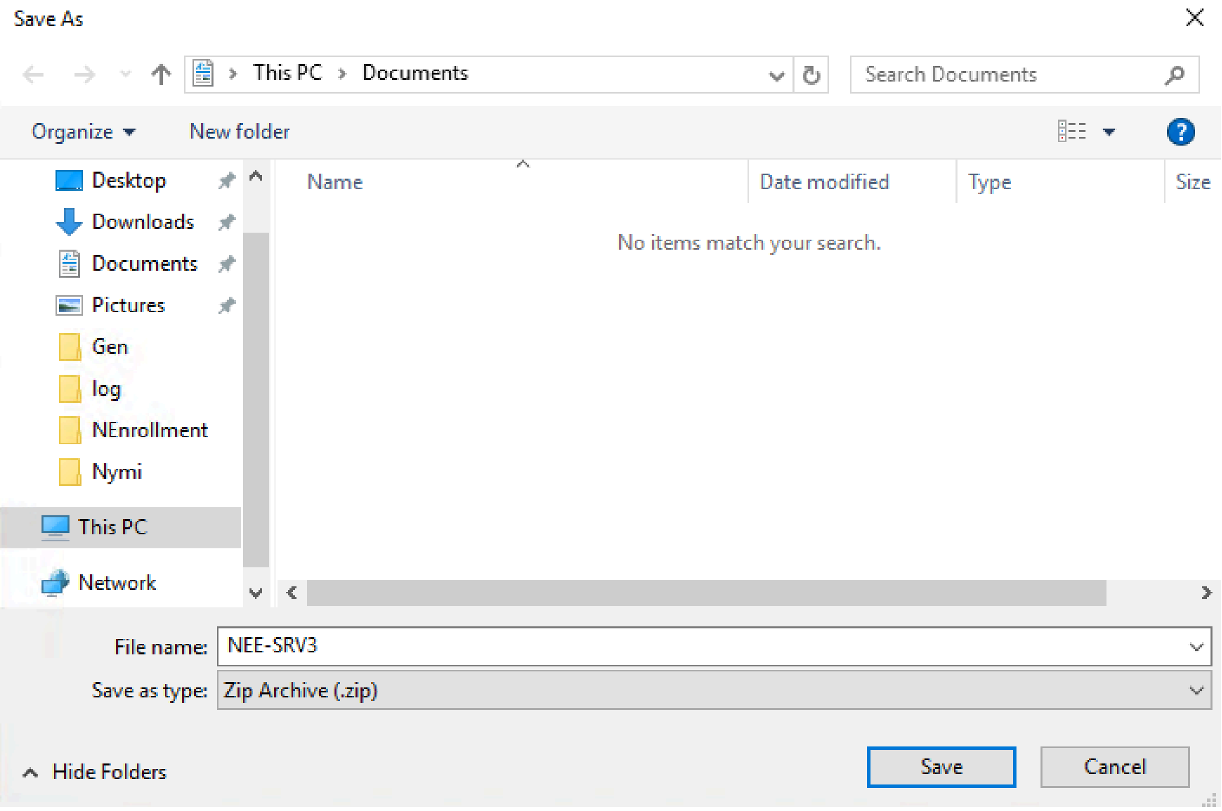
Program name: NesSystemInfo
Verified publisher: **Nymi Inc.**
File origin: Hard drive on this computer

Figure 1: The User Account Control

3. Click **Yes** to start the script.

   The script collects log information. A window appears that contains a folder with a zip file.

4. 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.



No items match your search.

File name: NEE-SRV3

Save as type: Zip Archive (.zip)

Figure 2: Saving Nymi Support Tool zip

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*

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 must be on the charger.

Firmware log retrieval

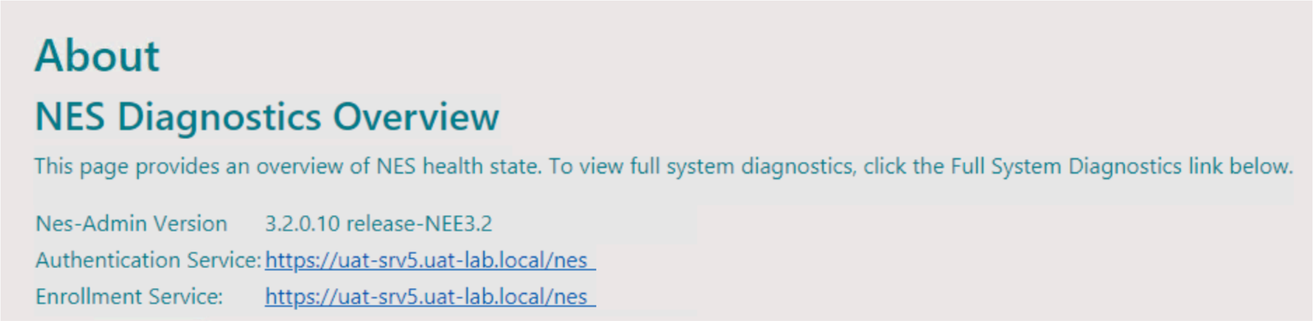
To retrieve logs from the Nymi Band, perform the following steps:

1. Place the Nymi Band on the charger and move the Nymi Band and charger close to the BLE radio antenna on the terminal (BLED112 adapter). This will ensure the logs are retrieved 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.



About

NES Diagnostics Overview

This page provides an overview of NES health state. To view full system diagnostics, click the Full System Diagnostics link below.

Nes-Admin Version 3.2.0.10 release-NEE3.2

Authentication Service: https://uat-srv5.uat-lab.local/nes

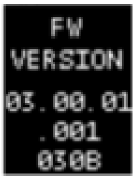
Enrollment Service: https://uat-srv5.uat-lab.local/nes

Figure 3: NES About Page

Determining Nymi Band Firmware Version

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.

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.



```
FW
VERSION
03.00.01
.001
030B
```

Figure 4: Nymi Band firmware version

Troubleshooting Nymi Band issues

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

Fault code appears on the Nymi Band

If a fault code appears on the Nymi Band, restart the Nymi Band.

See Restarting the Nymi Band in the Nymi Connected Worker Platform Administration Guide for more information.

Dead Nymi Band

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

If the charging symbol appears, then charge the Nymi Band for at least 2 hours. If the charging symbol does not appear, restart the Nymi Band. If the startup sequence and charging symbol does not appear, replace the Nymi Band with a new one. 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 assigning a new Nymi Band to the user.

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

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.

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.

Authentication Failures

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

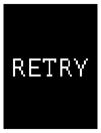


Figure 5: Authentication Failure Screen with Retry message

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 the Retry message about 1 second after the user places their finger on the fingerprint sensor and bezel.
- 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 Retry message about 13 seconds after the user places their finger on the fingerprint sensor and bezel.

Troubleshooting Fingerprint Mismatch Failures

If the fingerprint authentication fails, ensure the following:

- 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 softly 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.
- Ensure that the Nymi Band fits snugly on the wrist.

Troubleshooting Liveness Detection Failures

If the liveness detection fails, ensure the following:

- 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.
- 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.
- Ensure that the Nymi Band fits snugly on the wrist and does not move around during the authentication process.

Note: The SQL database contains a record of the failed authentication attempt. The section *Collecting Data From a Nymi Band* provides more information.

Authentication Lockout

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

Nymi Bands will temporarily lock the wearer out after 5 consecutive, failed fingerprint match attempts. Every additional failed attempt will increase the lockout duration.

Authentication lockout is present for all Nymi Bands with the firmware released with CWP 1.1. To update the Nymi Band, refer to Updating Nymi Band Firmware.

When an authentication fails, the Nymi Band vibrates and the authentication failure message appears. When the fingerprint icon appears, the user can try to authenticate again. If authentication fails 5 consecutive times (due to failed fingerprint match), the user will be temporarily locked out of their Nymi Band. During the lockout, a lock icon appears on the Nymi Band with the duration of the lockout. The first lockout persists for 1 minute and the duration will double after each failed fingerprint match, up to a maximum of 60 minutes, as shown in the image below. The Nymi Band will return to normal behavior with a successful fingerprint match.

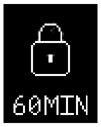


Figure 6: Fingerprint Authentication Lockout Screen

Note: The counts for authentication lockout only apply to failed fingerprint matches. Failures due to unrecognized ECG readings do not increase the count.

Clearing an Authentication Lockout

The lockout duration will persist 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 any of the following methods:

- Delete the user data associated with the Nymi Band.
- 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 NES policy at the time of enrollment.

Note: Consider re-enrolling the user to the Nymi Band with another fingerprint if the user is repeatedly locked out with their fingerprint.

Fingerprint sensor not working

If you suspect that the fingerprint sensor is broken, clean the fingerprint sensor on the Nymi Band, and then ask the user to attempt authentication again.

If the fingerprint sensor is still not working, review the following workflow chart to troubleshoot the issue.

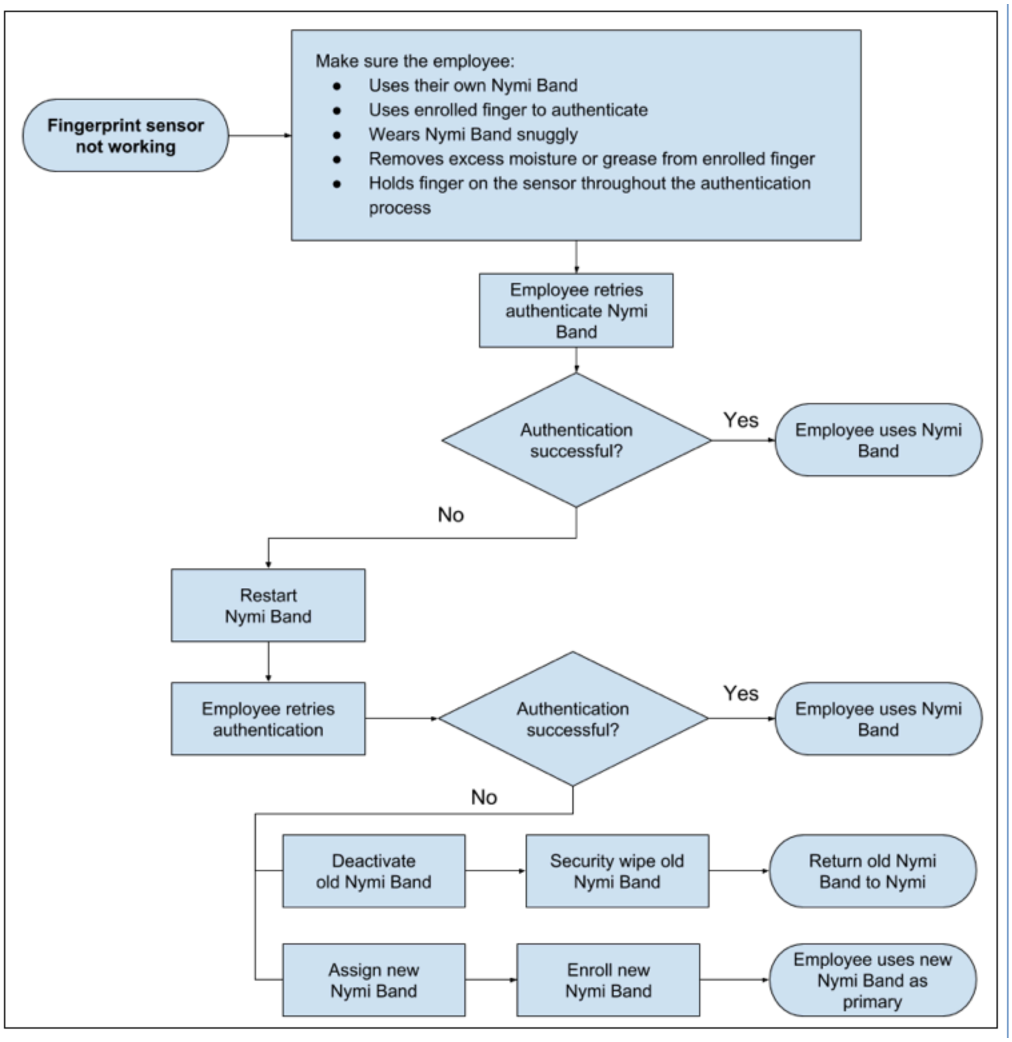

Fingerprint sensor not working
Make sure the employee:
Uses their own Nymi Band
Uses enrolled finger to authenticate
Wears Nymi Band snuggly
Removes excess moisture or grease from enrolled finger
Holds finger on the sensor throughout the authentication process
Employee retries authenticate Nymi Band
Authentication successful?
Yes
Employee uses Nymi Band
No
Restart Nymi Band
Employee retries authentication
Authentication successful?
Yes
Employee uses Nymi Band
No
Deactivate old Nymi Band
Security wipe old Nymi Band
Return old Nymi Band to Nymi
Assign new Nymi Band
Enroll new Nymi Band
Employee uses new Nymi Band as primary

Figure 7: Troubleshooting when the fingerprint sensor is not working

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 20 for guidance on configuring the Bluetooth sensitivity for BLE tap and Nymi Lock Control.

Editing the nbe.toml File

A backup configuration file is installed on the user terminal when the `Nymi Bluetooth Endpoint` is installed or updated. This file, *nbe.default.toml*, contains the default values that control BLE tap behavior with the Nymi Band and BLE adapter. Use the values in the *nbe.default.toml* file as a template for the *nbe.toml* file. These files are located in *C:\Nymi\Bluetooth_Endpoint\* on Windows, and */usr/bin/nbe.toml* on HP Thin Pro.

Note: `Nymi Bluetooth Endpoint` will only recognize RSSI values in the *nbe.toml* file. Retain a backup of a useful configuration by copying the *nbe.toml* file and renaming it.

Table 2: Default configuration settings for `Nymi Lock Control` and BLE tap intent

nbe.toml Entry	Default Value	Description
agent_url	"ws://127.0.0.1:9120/socket/websocket" (do not change)	Identifies the location of the agent URL. The default value shown in this table is generated if the agent is installed locally. If the agent URL is installed centrally (via remote installation), the hostname of the URL will be different. **The agent_url must be present when using an *nbe.toml* file.**
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`**.

nbe.toml Entry	Default Value	Description
rssi_tap_threshold	0 (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 a duration *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_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.

1. Make a copy of the *C:\Nymi\Bluetooth_Endpoint\nbe.default.toml* file (On HP Thin Pro, */usr/bin/nbe.default.toml*), and name the file *nbe.toml*.
2. Edit the *nbe.toml* file with a text editor.
3. Edit the RSSI values in the file. Refer to the descriptions in the table above.
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`.

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`.

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 NES 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.
Cannot Install	Cannot install with current settings	Review your settings.
Certificate Error - Password required	Certificate is protected by password	Supply password.

Message	Description	Troubleshooting
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.
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.

Message	Description	Troubleshooting
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-requsite 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

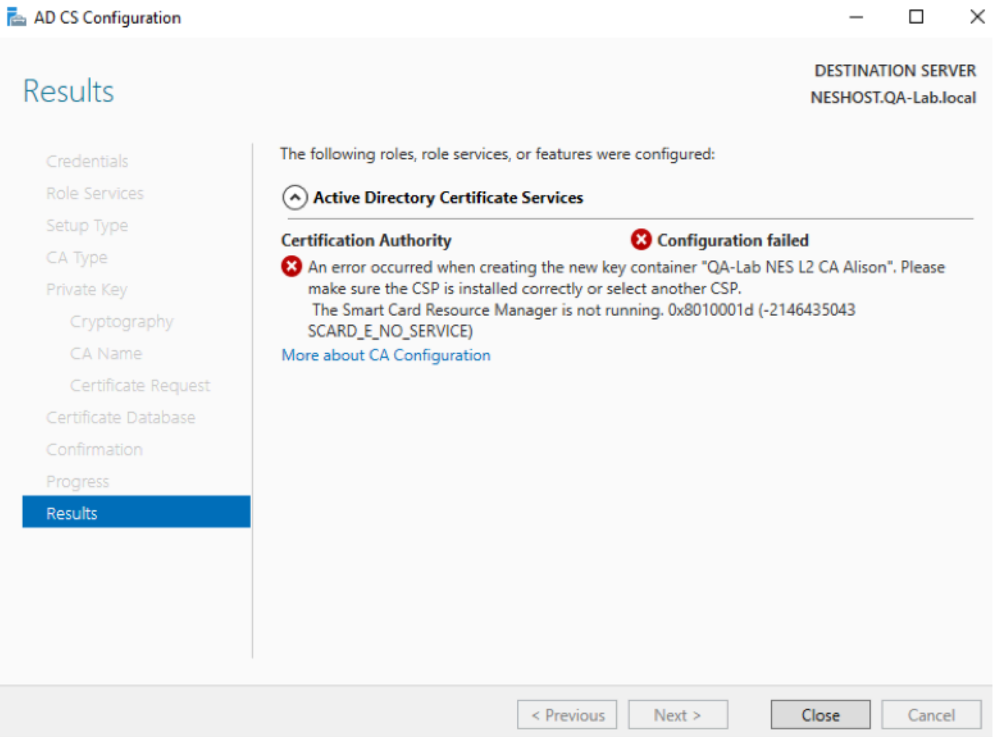
Install ASP.NET by performing the following steps:

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.

An error occurred when creating the new container *`L2_certificate_name`*. Please make sure that the CSP is installed correctly or select another CSP.

This error message appears during NDES configuration.

The following figure shows the complete error message.



The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority ☒ Configuration failed

☒ An error occurred when creating the new key container "QA-Lab NES L2 CA Alison". Please make sure the CSP is installed correctly or select another CSP.
The Smart Card Resource Manager is not running. 0x8010001d (-2146435043 SCARD_E_NO_SERVICE)

More about CA Configuration

Cause

An incorrect cryptography provider was selected during configuration.

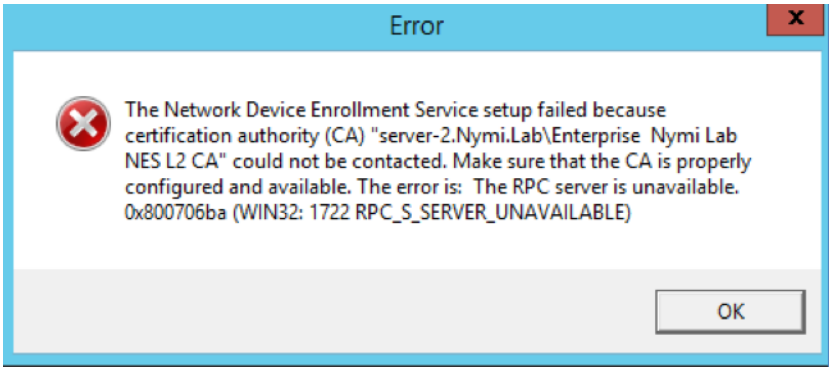
Resolution

Uninstall AD CS and then reinstall AD CS. On the `Cryptography for CA` window, from the **`Select a cryptographic provider`** list , choose **`ECDSA_P256#Microsoft Software Key Storage Provider`**.

The Network Device Enrollment Service setup failed because certification authority (CA) “servername”\L2 CN\ could not be contacted

This error message appears during the NDES configuration.

The following figure shows the complete error message.



The Network Device Enrollment Service setup failed because certification authority (CA) "server-2.Nymi.Lab\Enterprise Nymi Lab NES L2 CA" could not be contacted. Make sure that the CA is properly configured and available. The error is: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)

Cause

AD CS service is not running.

Resolution

Perform the following actions to start AD CS:

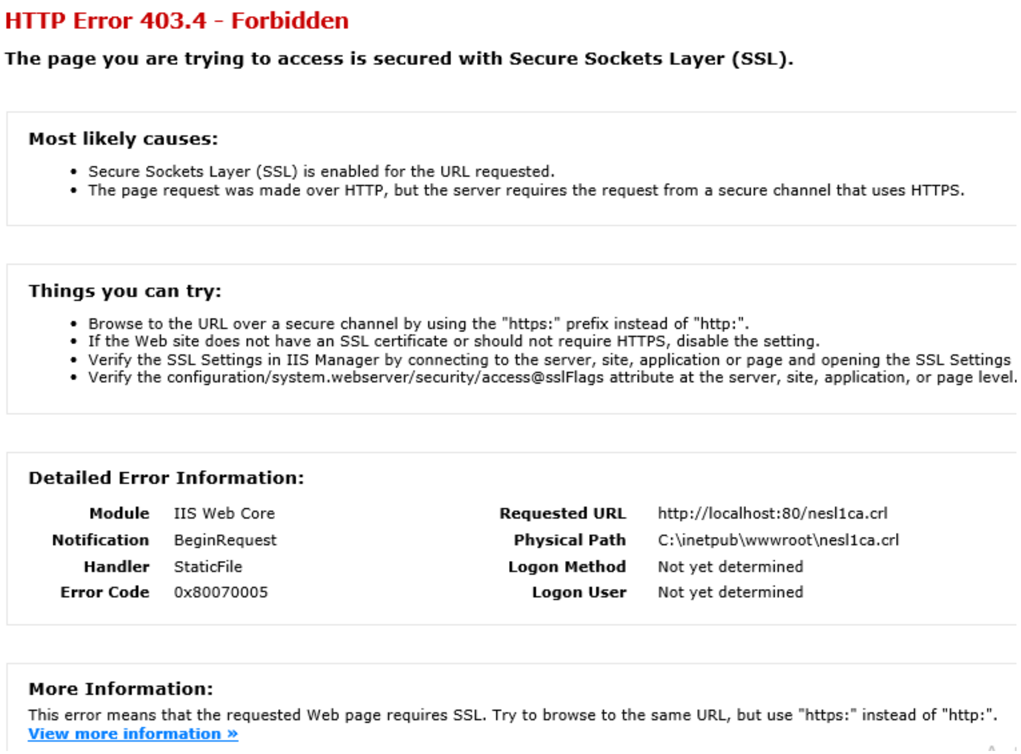
1. On the NES host, open `Server Manager` and from the **`Tools`** menu, select **`Certificate Authority`**.
2. On the **`Toolbar`**, click the green triangle.

Certificate Authority installation fails with the error "Revocation Server is offline"

The error message appears after you click **`Install`** during the Certificate Authority (CA) installation process.

Additionally, attempts to access the Certificate Revocation List (CRL) from a web browser fail with a 403 error.

For example, attempts to connect to http://localhost/crl/NESL1CA.crl or http://localhost/crl/NymiInfraRootCA.crl from a web browser display the following page:



HTTP Error 403.4 - Forbidden

The page you are trying to access is secured with Secure Sockets Layer (SSL).

Most likely causes:

- Secure Sockets Layer (SSL) is enabled for the URL requested.
- The page request was made over HTTP, but the server requires the request from a secure channel that uses HTTPS.

Things you can try:

- Browse to the URL over a secure channel by using the "https:" prefix instead of "http:".
- If the Web site does not have an SSL certificate or should not require HTTPS, disable the setting.
- Verify the SSL Settings in IIS Manager by connecting to the server, site, application or page and opening the SSL Settings
- Verify the configuration/system.webserver/security/access@sslFlags attribute at the server, site, application, or page level.

Detailed Error Information:

Module	IIS Web Core	Requested URL	http://localhost:80/nesl1ca.crl
Notification	BeginRequest	Physical Path	C:\inetpub\wwwroot\nesl1ca.crl
Handler	StaticFile	Logon Method	Not yet determined
Error Code	0x80070005	Logon User	Not yet determined

More Information:

This error means that the requested Web page requires SSL. Try to browse to the same URL, but use "https:" instead of "http:".

View more information »

Figure 8: HTTP Error 403.4 - Forbidden

Cause

The CRL distribution point configuration for the L1 and L2 certificates use an HTTP URL to fetch certificates but the CRL Virtual Directory setting in IIS is configured to require SSL.

Resolution

To resolve this issue disable the SSL required option for the default web page in IIS Manager on NES.

1. In IIS Manager, expand the ***NES server* > Sites > Default Web Site**.
2. In the Default Website pane, double-click **SSL Settings**, and then clear the **Require SSL** box.

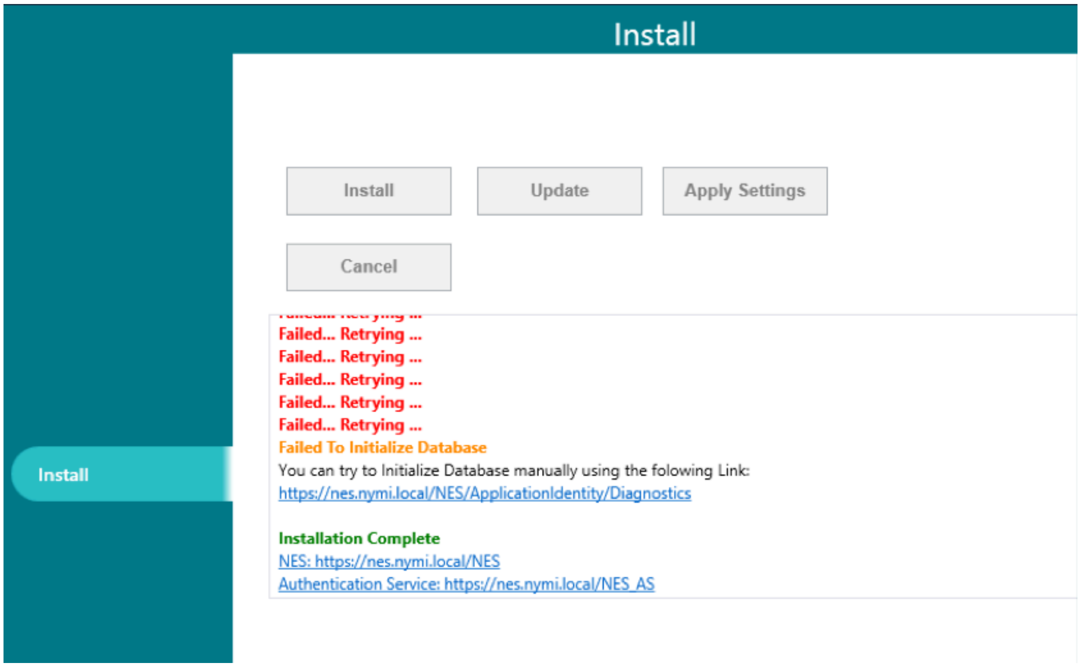
3. Remove NDES and the Certificate Authority:

   a. In `Server Manager`, select **`Manange > Remove Roles and Features`**. The `Remove Roles and Features` Wizard opens.
   b. Click **`Next`**.
   c. On the `Select destination server` page, click **`Next`**.
   d. On the `Remove server roles` page, expand **`Active Directory Certificate Services`** , clear **`Network Device Enrollment Service`**, and then click **`Next`**.
   e. On the `Remove features` page, click **`Next`**.
   f. On the `Confirmation removal selections` page, click **`Remove`**.
   g. When the removal completes, click **`Close`**.
   h. In `Server Manager`, select **`Manange > Remove Roles and Features`**.
   i. Click **`Next`**.
   j. On the `Select destination server` page, click **`Next`**.
   k. On the `Remove server roles` page, clear **`Actice Directory Certificate Services`**.
   l. On the `Remove features that require Active Directory Certificate Services`, click **`Remove Features`**
   m. On the `Remove server roles` page,ckick **`Next`**.
   n. On the `Remove Features` page, click **`Next`**.
   o. On the `Confirm removal selections` page, click **`Remove`**.
   p. When the removal completes, click **`Close`**.
   q. Restart the NES machine.
   r. Install AD CS, NDES, and the CA. The Nymi Connected Worker Platform NES Deployment Guide provides more information.

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.



Failed... Retrying ...
Failed... Retrying ...
Failed... Retrying ...
Failed... Retrying ...
Failed... Retrying ...
Failed To Initialize Database
You can try to Initialize Database manually using the folowing Link:
https://nes.nymi.local/NES/ApplicationIdentity/Diagnostics

Installation Complete
NES: https://nes.nymi.local/NES
Authentication Service: https://nes.nymi.local/NES_AS

Figure 9: 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 NES Deployment Guide* describes how to install ASP .NET.

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

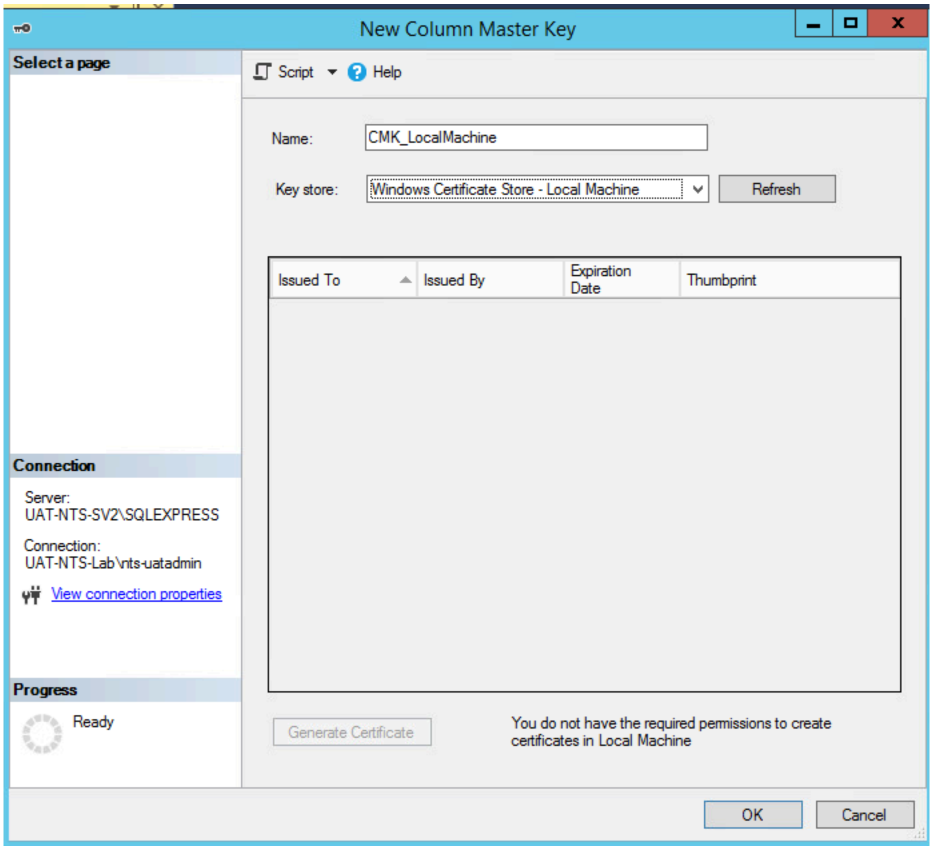
NES is deployed on a Domain Controller.

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.



Name: CMK_LocalMachine

Key store: Windows Certificate Store - Local Machine

Server: UAT-NTS-SV2\SQLEXPRESS

Connection: UAT-NTS-Lab\nts-uatadmin

You do not have the required permissions to create certificates in Local Machine

Figure 10: 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.

Troubleshooting NES Administrator Console connection issues

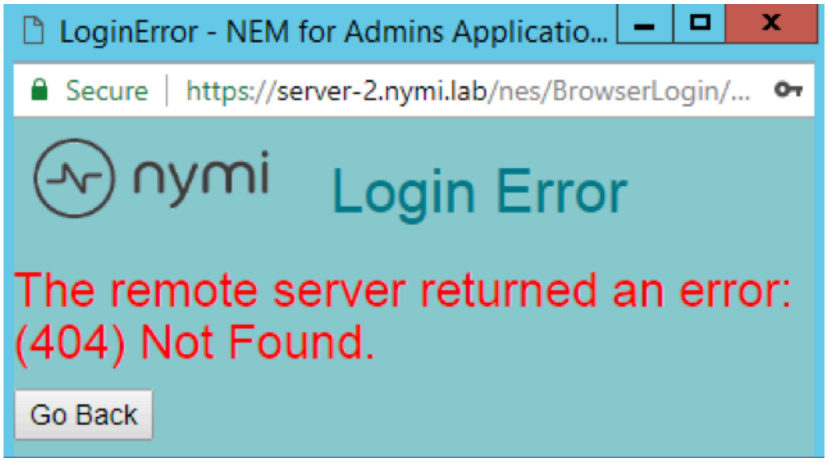
This section provides information about the error messages that might appear while you log in to the `NES Administrator Console`.

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.


LoginError - NEM for Admins Applicatio...
Secure
https://server-2.nymi.lab/nes/BrowserLogin/...
nymi
Login Error
Go Back

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

Figure 11: 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.

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 NES 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.

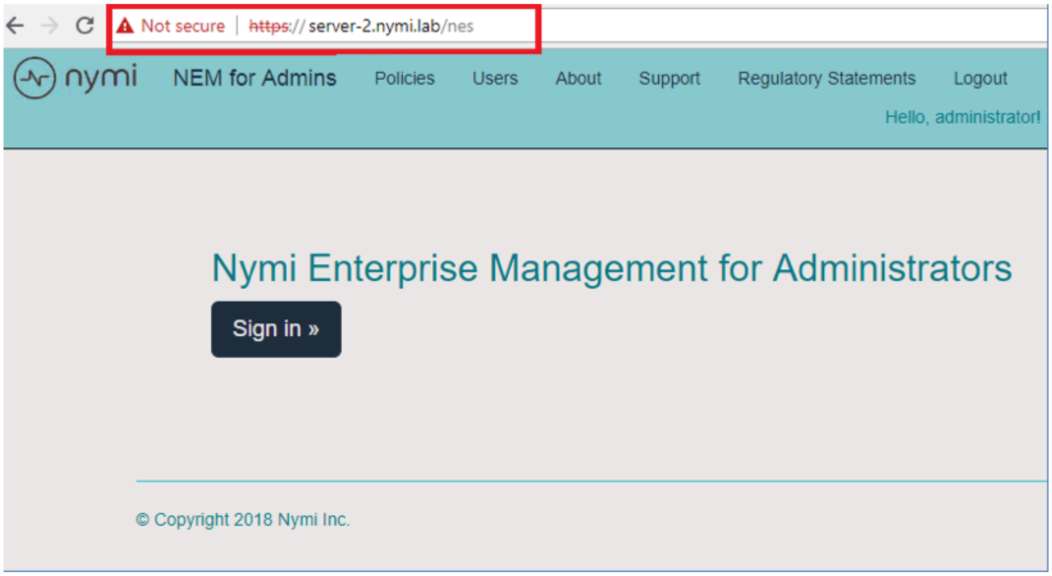
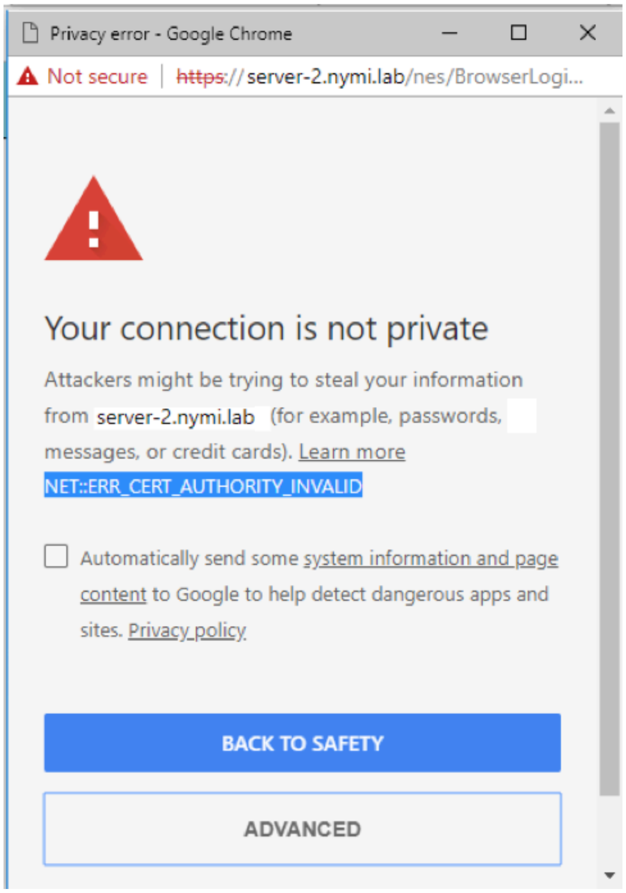


Figure 12: Cannot establish a secure connection to NES

- 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.


Privacy error - Google Chrome
Not secure
~~https~~://server-2.nymi.lab/nes/BrowserLogi...
BACK TO SAFETY
ADVANCED

Your connection is not private

Attackers might be trying to steal your information from server-2.nymi.lab (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

Figure 13: 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.

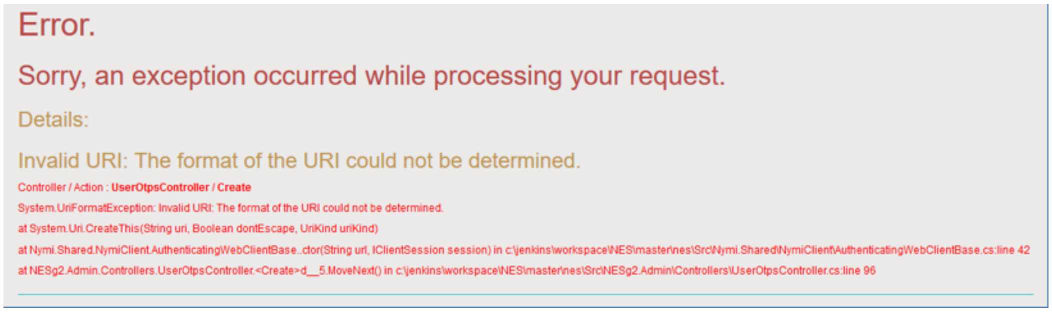
Resolution

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

Invalid URI: The format of the URI could not be determined

This error message appears when you attempt to create an OTP for a user.

The following figure shows the complete error message.



Error.

Sorry, an exception occurred while processing your request.

Details:

Invalid URI: The format of the URI could not be determined.

```
Controller / Action : UserOtpsController / Create
System.UriFormatException: Invalid URI: The format of the URI could not be determined.
at System.Uri.CreateThis(String uri, Boolean dontEscape, UriKind uriKind)
at Nymi.Shared.NymiClient.AuthenticatingWebClientBase..ctor(String url, IClientSession session) in c:\jenkins\workspace\NES\master\nes\Src\Nymi.Shared\NymiClient\AuthenticatingWebClientBase.cs:line 42
at NESg2.Admin.Controllers.UserOtpsController.<Create>d__5.MoveNext() in c:\jenkins\workspace\NES\master\nes\Src\NESg2.Admin\Controllers\UserOtpsController.cs:line 96
```

Figure 14: Invalid URI error

Cause

The enrollment URI that is specified in the active policy is not correct.

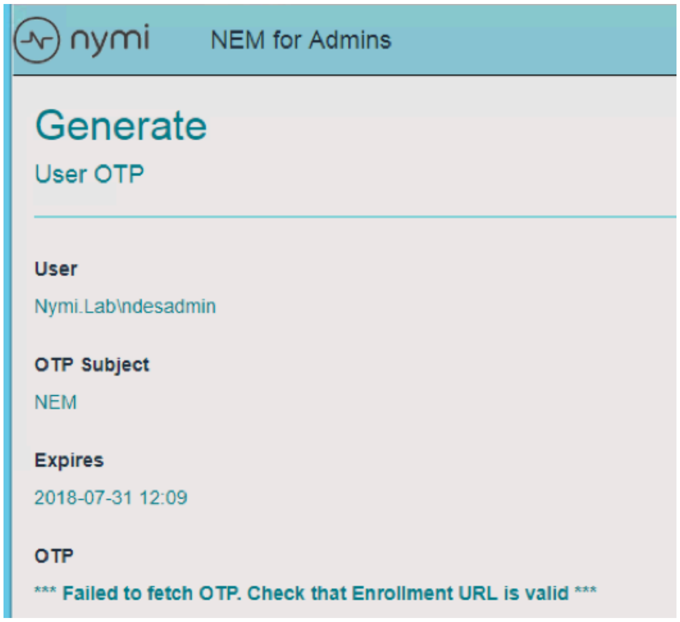
Resolution

Correct the enrollment URL in the active policy. The *Nymi Connected Worker Platform Administration Guide* describes how to edit the active policy.

Failed to fetch OTP. Check that Enrollment URL is valid

This error message appears when you try to generate an OTP for a user.

The following figure provides an example of the error message.



Generate

User OTP

User

Nymi.Lab\ndesadmin

OTP Subject

NEM

Expires

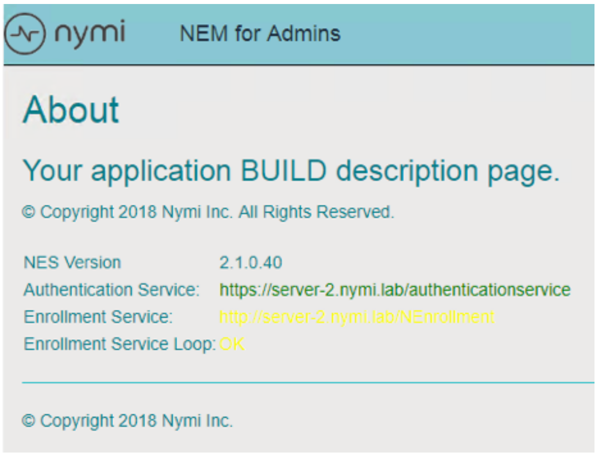
2018-07-31 12:09

OTP

*** Failed to fetch OTP. Check that Enrollment URL is valid ***

Figure 15: Failed to fetch OTP error

On the `About` page, the Enrollment Service and Enrollment Service Loop values are yellow, as shown in the following figure.



About

Your application BUILD description page.

© Copyright 2018 Nymi Inc. All Rights Reserved.

NES Version	2.1.0.40
Authentication Service:	https://server-2.nymi.lab/authenticationservice
Enrollment Service:	http://server-2.nymi.lab/NEnrollment
Enrollment Service Loop:	OK

© Copyright 2018 Nymi Inc.

Figure 16: About page showing Enrollment Service issues

Cause

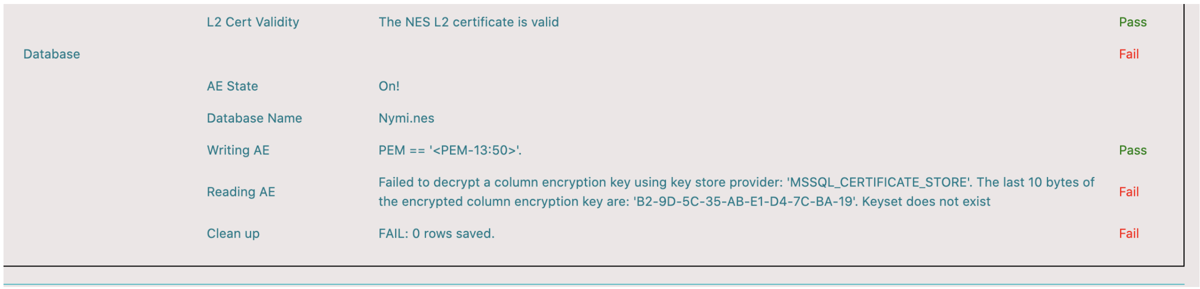
The Enrollment URL specified in the active group policy is not a secure URL (https).

Resolution

1. Edit the active group policy and update **`NEnrollment URL`** value to specify https and not http.
2. Save the group policy.
3. Log out and log back into the NES Administrator Console.

Failed to decrypt a column encyrption 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 hardended but the Application Pool Identity that was defined during the NES deployment was not set to LocalSystem.

Resolution

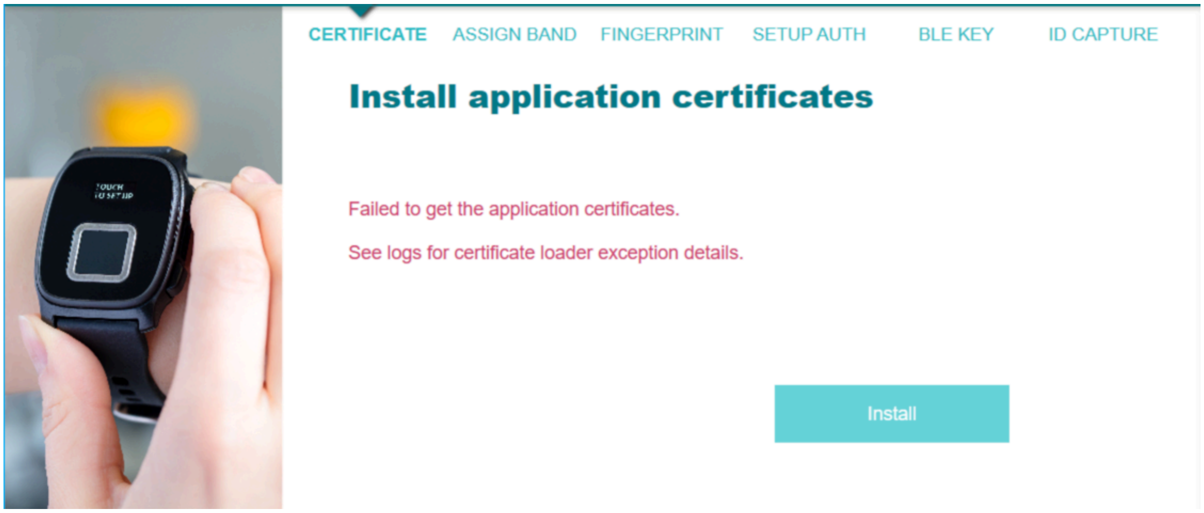
1. Run the NES installaton wizard.
2. On the **`IIS`** tab, from the **`Application Pool Identity`** list, select **`LocalSystem`**.
3. On the **`Install`** tab, select **`Apply Settings`**.
4. Connect to the console and click **`About`**
5. Click **`View Full System Diagnostics`**, and confirm that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

Troubleshooting Nymi Band Application Errors

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

Self Signed Certificate Expiry

On the **`Install Certificates`** screen of the Nymi Band Application, a **`Failed to get the application certificates`** error appears.



Failed to get the application certificates.

See logs for certificate loader exception details.

Figure 17: Failed application certificate

Cause

The Self-signed certificate has expired on NES. The problem occurred while the Nymi Band Application was communicating with the NES.

Resolution

Ensure that the certificates have not expired and that the certificates are correctly installed.

For more information, see **`Importing the Root CA certificate`** in the *Nymi Connected Worker Platform Administration Guide*.

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.

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

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 NES 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.

Enrollment URL is not set. Contact your administrator.

This error message appears when an employee 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.

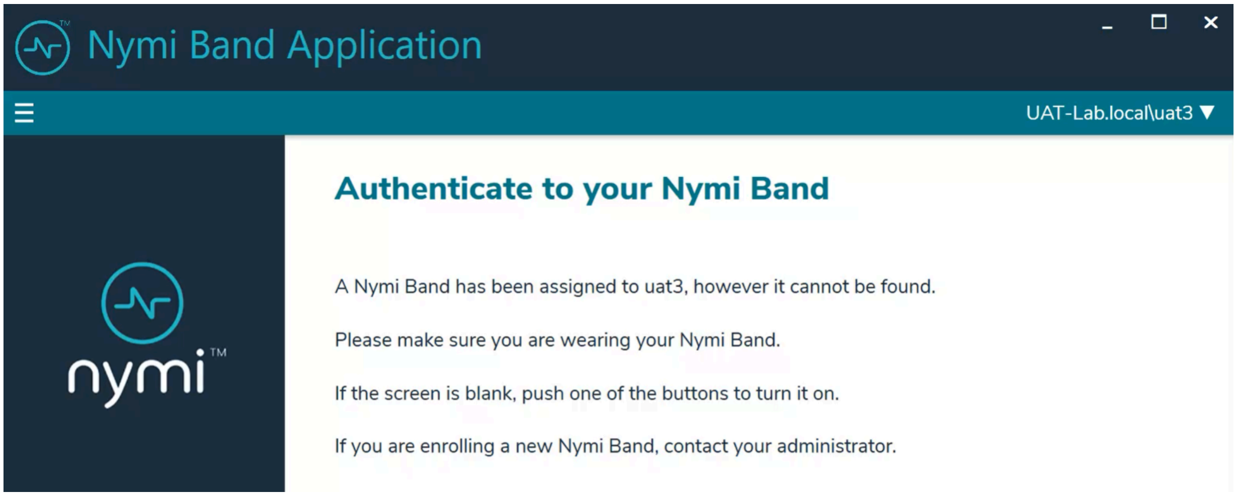
Resolution

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.

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.



Authenticate to your Nymi Band

A Nymi Band has been assigned to uat3, however it cannot be found.

Please make sure you are wearing your Nymi Band.

If the screen is blank, push one of the buttons to turn it on.

If you are enrolling a new Nymi Band, contact your administrator.

Figure 18: 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.

Troubleshooting Enrollment Service Connection Issues

When errors appear in the `Nymi Band Application` during enrollment or when an employee specifies the OTP, check the Enrollment Service status in the `NES Administrator Console` System Diagnostics.

To access the System Diagnostics information, from the `About` page, navigate to the `System Diagnostics` page by clicking **`View Full Diagnostics`**

This section provides information about errors that you might encounter during the enrollment process.

Failed to get application certificates

This error message appears when you type the OTP, and then click **`Install`**.

The *nem.log* file contains the following error messages:

```
Band message read error, status: 2200: Problem occurred while
communicating with server. Could not get NEA certificate from server.
```

Cause

The OTP typed by the employee has already been used to install application certificates.

Resolution

Generate a new OTP for the user account or log in to `Nymi Band Application` the with a user account that has an unused OTP.

Failed to get NEM certificate

This error messages appears when you type the OTP in the `Nymi Band Application`, and then click **`Install`**.

Cause

There is an issue with the specified OTP.

Resolution

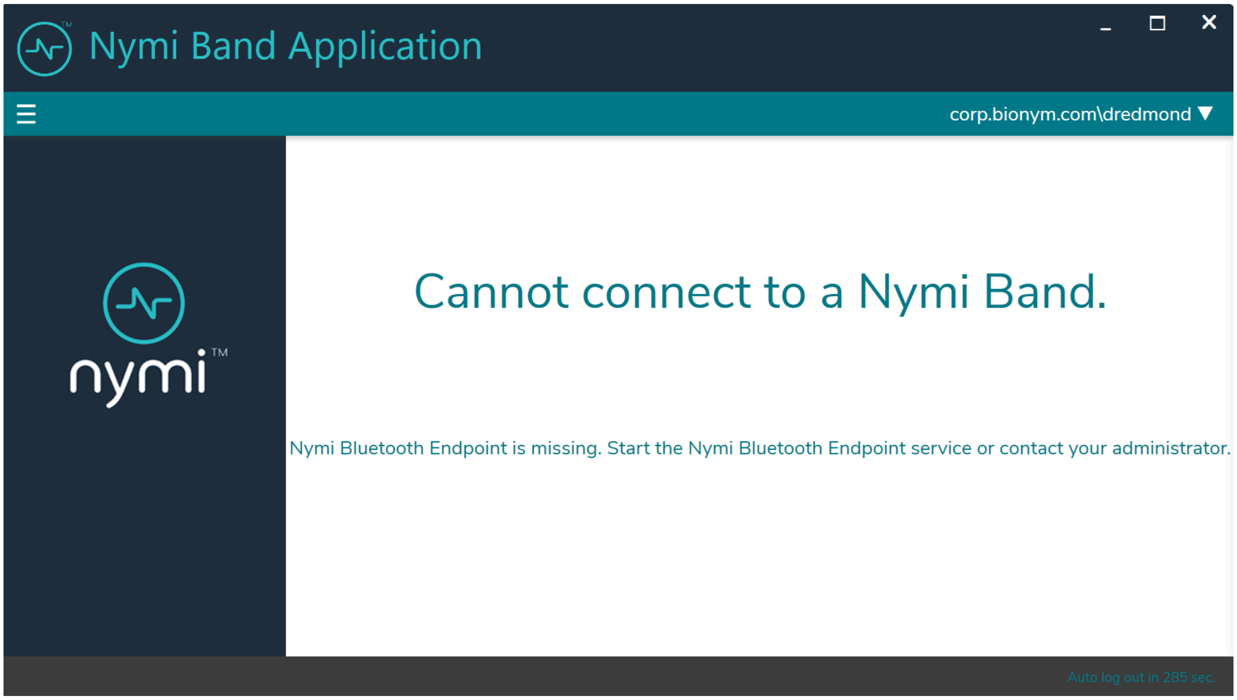
Perform each of the following actions, until the issue is resolved:

- Type the correct OTP. If you copied the OTP from the `NES Administrator Console` window, and then pasted the OTP into the `Nymi Band Application`, ensure that spaces are not present at the end of the OTP.
- Ensure that the OTP is for the account that is logged into the `Nymi Band Application`.

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.



Cannot connect to a Nymi Band.

Nymi Bluetooth Endpoint is missing. Start the Nymi Bluetooth Endpoint service or contact your administrator.

Auto log out in 285 sec.

Figure 19: Cannot Connect to a Nymi Band

Cause

This error message can appear for the following reasons:

- The `Nymi Bluetooth Endpoint` service is not running or needs to be reset.
- The Bluetooth adapter is not plugged into the terminal.

Resolution

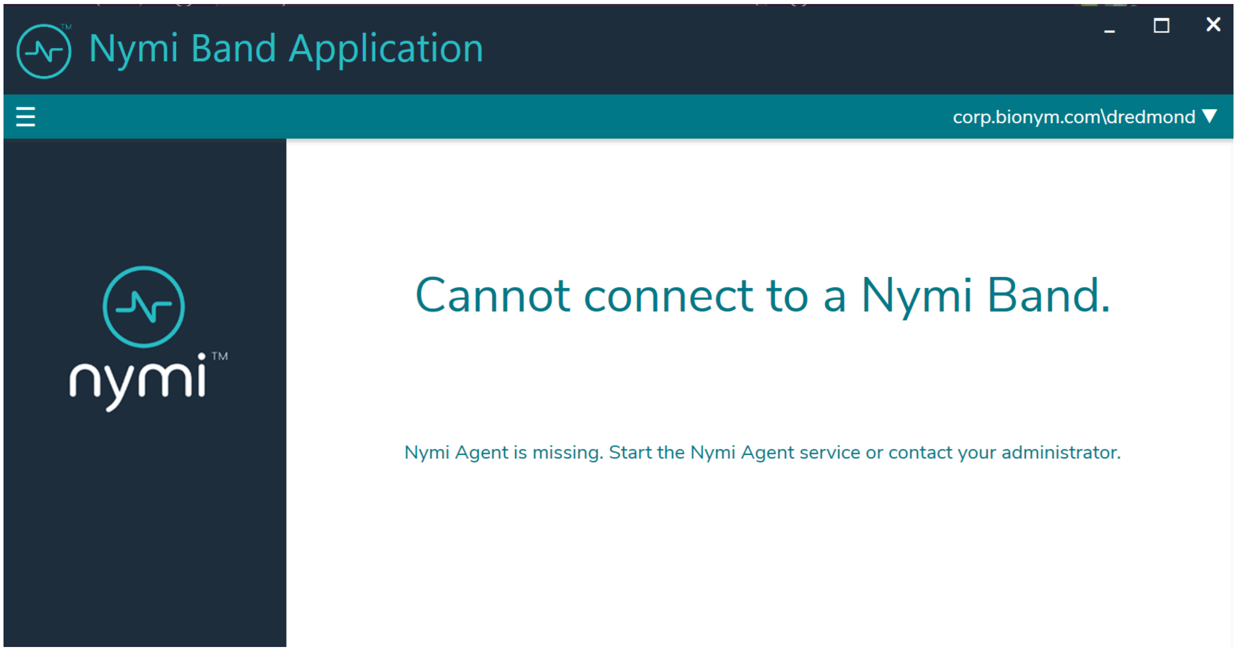
To resolve this issue, perform one of the following actions:

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

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.



Cannot connect to a Nymi Band.

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

Figure 20: Nymi Agent is missing error

Cause

The `Nymi Agent` service is not running on the network device.

Resolution

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`.

Band error: (2000) Request made with invalid parameters

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

Cause

This error can appear for the following reasons:

- Employee typed an incorrect setup code.
- Setup code on the Nymi Band changed before the employee completed typing the setup code in the `Nymi Band Application`.

Resolution

Check the setup code on the Nymi Band, type the correct setup code, and then click **`Begin`**. The setup code is time-sensitive and changes over time.

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.

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 9000: An error occurred in the system.

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

Cause

The situations in which this error can appear include:

- An incorrect setup code was provided.
- Another Nymi Band that has not been enrolled is near the terminal while the employee is enrolling their Nymi Band.

Resolution

- If another unenrolled Nymi Band was nearby, remove the Nymi Band that you want to enroll from the wrist, and then put the Nymi Band back on the wrist.
- Attempt the enrollment again.
- Retype the setup code.

Setup codes do not match or Error 9000

During enrollment, this error message might appear after you type the setup code and click **`Begin`**. If you encounter this error, perform the following actions.

Cause

The situations in which this error can appear include:

- An incorrect setup code was provided.
- Another Nymi Band that has not been enrolled is near the terminal while the employee is enrolling their Nymi Band.

Resolution

- If another unenrolled Nymi Band was nearby, remove the Nymi Band that you want to enroll from the wrist, and then put the Nymi Band back on the wrist.
- Attempt the enrollment again.
- Ensure that the setup code on the Nymi Band is the same as the setup code that you typed in the Nymi Band application. Pay special attention to “O”, “0”, “U”, “V”, “B”, and “8”, as they might look similar.
- If the problem persists:

1. Go to **`Start`** and type `Services`, and then press **`Enter`**.
2. In the Services window, right—click **`Nymi Bluetooth Endpoint`**, and then click **`Restart`**.
3. Relaunch the `Nymi Band Application`.

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.

Troubleshooting Lock Control

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

Log Files

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

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 `Submit a Request` page, in the drop-down, select **`Nymi Customer - Technical Support`**.
4. On the next page, fill in the appropriate details, and in the **`Attachments`** section, click **`Add file`**.
5. Navigate to the *C:\Users\[username]\AppData\Roaming\Nymi\unlock\ZipLog* folder, and then select the zip file.

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.

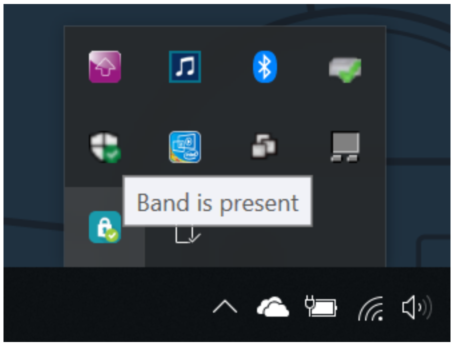


Figure 21: Nymi Lock Control Band is Present status

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
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

Message	Cause	Resolution
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
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

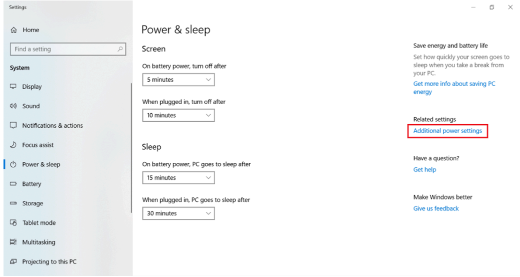
To resolve this issue, perform one of the following actions:

- 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.

     Power & sleep

     Screen

     On battery power, turn off after: 5 minutes

     When plugged in, turn off after: 10 minutes

     Sleep

     On battery power, PC goes to sleep after: 15 minutes

     When plugged in, PC goes to sleep after: 30 minutes

     Save energy and battery life

     Set how quickly your screen goes to sleep when you take a break from your PC.

     Get more info about saving PC energy

     Related settings

     Additional power settings

     Have a question?

     Get help

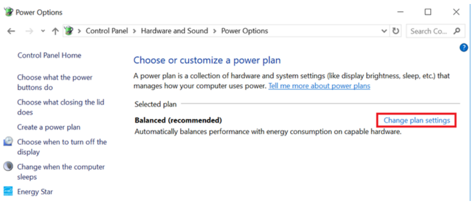
     Make Windows better

     Give us feedback

     Figure 22: 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.

     Power Options
Control Panel > Hardware and Sound > Power Options
Search Co...
Control Panel Home
Choose what the power buttons do
Choose what closing the lid does
Create a power plan
Choose when to turn off the display
Change when the computer sleeps
Energy Star

     Choose or customize a power plan

     A power plan is a collection of hardware and system settings (like display brightness, sleep, etc.) that manages how your computer uses power. Tell me more about power plans

     Selected plan

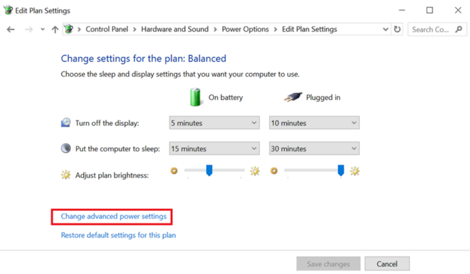
     Balanced (recommended) — Change plan settings

     Automatically balances performance with energy consumption on capable hardware.

     Figure 23: 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.

     Edit Plan Settings
Control Panel > Hardware and Sound > Power Options > Edit Plan Settings
Search Co...
Save changes
Cancel

     Change settings for the plan: Balanced

     Choose the sleep and display settings that you want your computer to use.

	On battery	Plugged in
Turn off the display:	5 minutes	10 minutes
Put the computer to sleep:	15 minutes	30 minutes
Adjust plan brightness:		

     Change advanced power settings

     Restore default settings for this plan

     Figure 24: Edit Plan Settings screen

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

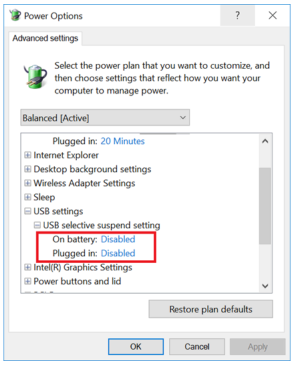
     a. Expand **USB settings > USB selective suspend setting**

     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.



Select the power plan that you want to customize, and then choose settings that reflect how you want your computer to manage power.

Balanced [Active]

- Plugged in: 20 Minutes
- ⊞ Internet Explorer
- ⊞ Desktop background settings
- ⊞ Wireless Adapter Settings
- ⊞ Sleep
- ⊟ USB settings
  - ⊟ USB selective suspend setting
    - On battery: Disabled
    - Plugged in: Disabled
- ⊞ Intel(R) Graphics Settings
- ⊞ Power buttons and lid

`Figure 25: 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.

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.

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.

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.

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

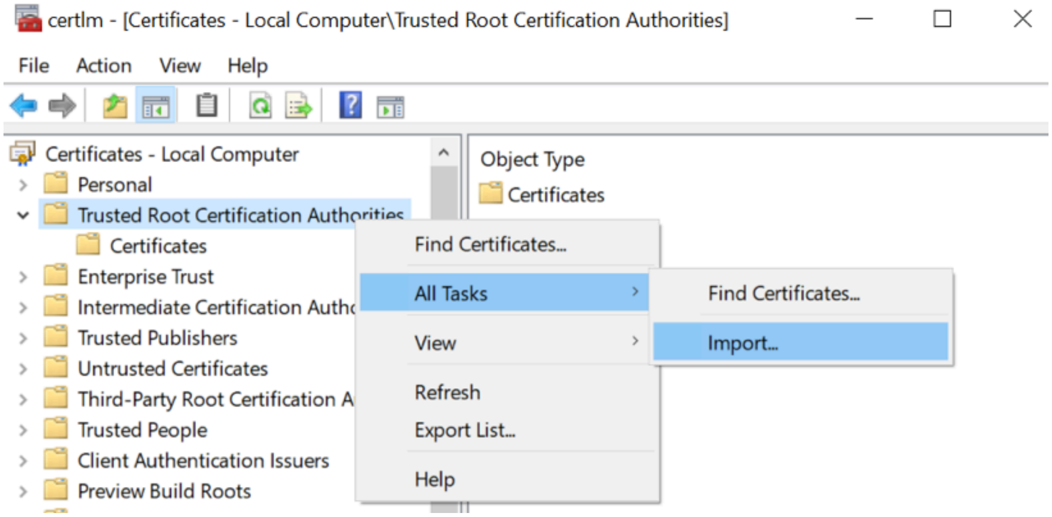
Before a network device can access the `NES Administrator Console`and the `Nymi Band Application`, a valid root CA certificate must exist in the Trusted Root Certification Authorities store.

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:

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`**.

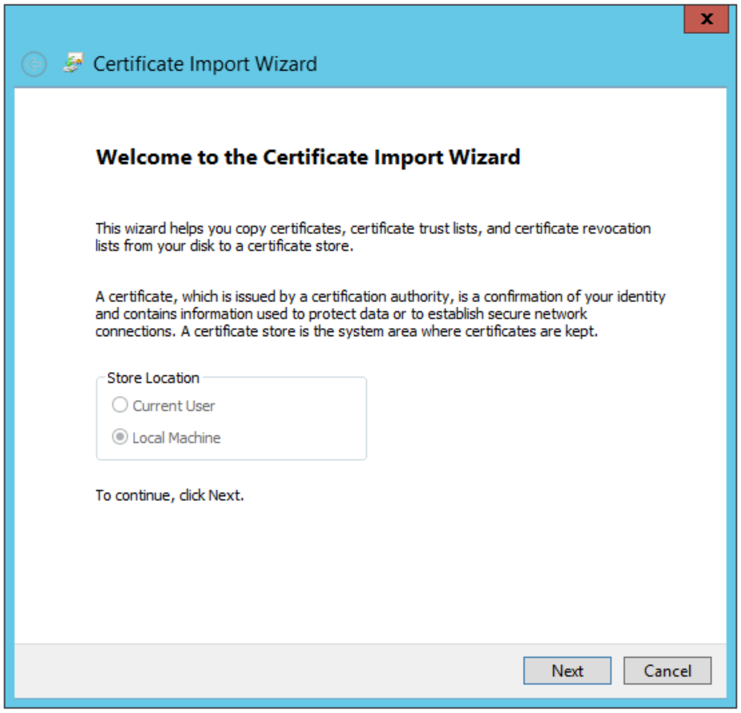
   The following figure shows the `certlm` window.


certlm - [Certificates - Local Computer\Trusted Root Certification Authorities]
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification A
Trusted People
Client Authentication Issuers
Preview Build Roots
Object Type
Certificates
Find Certificates...
All Tasks
View
Refresh
Export List...
Help
Find Certificates...
Import...

`Figure 26: 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.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

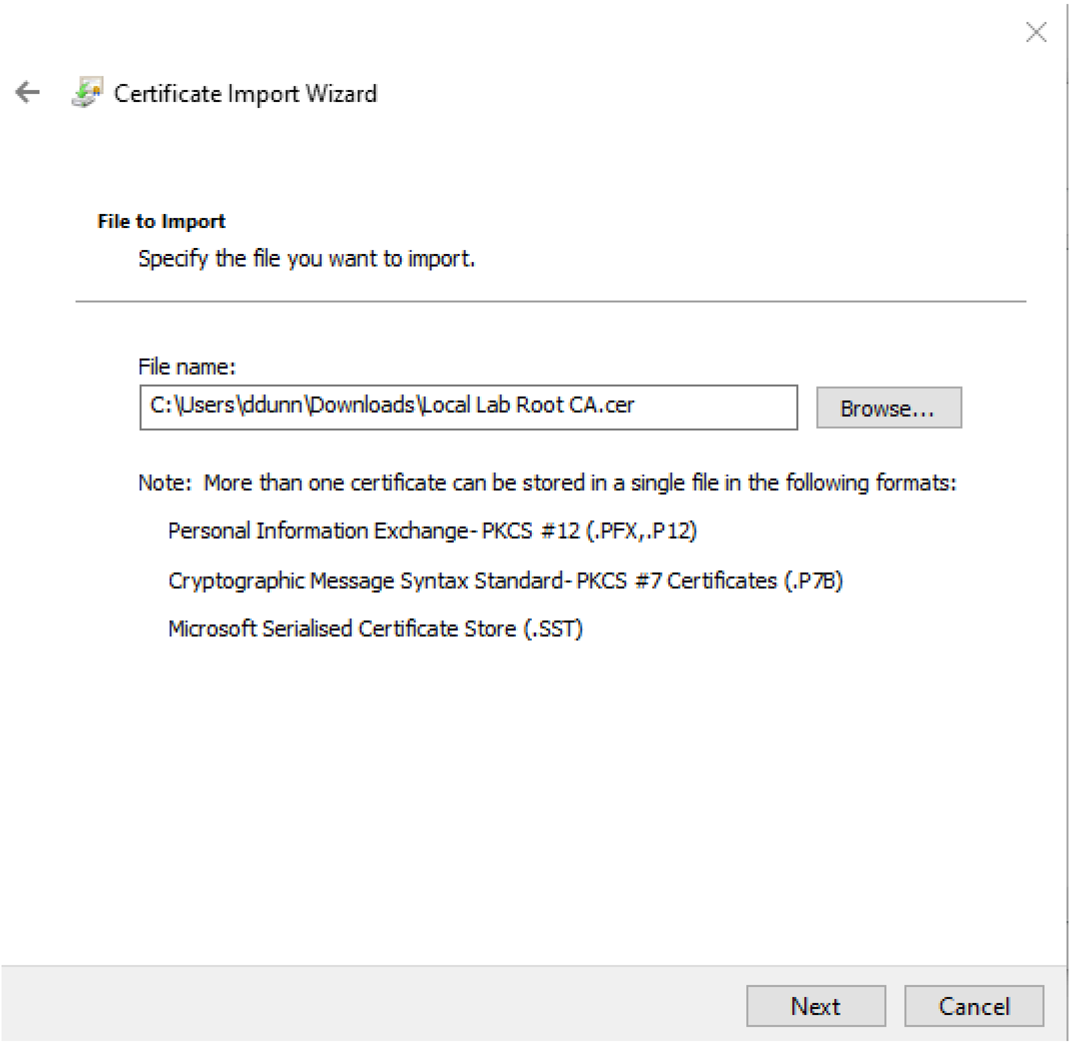
To continue, click Next.

`Figure 27: 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.



File to Import

Specify the file you want to import.

File name:

C:\Users\ddunn\Downloads\Local Lab Root CA.cer

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialised Certificate Store (.SST)

`Figure 28: 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`**.

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**.

Submitting a support request

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

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.

Nymi Inc. (Nymi) believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

The information in this document is provided as-is and Nymi makes no representations or warranties of any kind. This document does not provide you with any legal rights to any intellectual property in any Nymi product. You may copy and use this document for your referential purposes.

This software or hardware is developed for general use in a variety of industries and Nymi assumes no liability as a result of their use or application.Nymi, Nymi Band, and other trademarks are the property of Nymi Inc. Other trademarks may be the property of their respective owners.

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