Installation and Configuration Guide

Nymi Connect
v1.0
2025-04-24

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 guides contains information about how to install, configure and use the Nymi Connect application.

Audience

This guide provides information to CWP Administrators. A CWP the person in the enterprise that manages the CWP solution in their workplace.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	April 24, 2025	First release 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.

- **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, 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

Nymi Connect Deployment Overview

The Nymi Connect software extends the use of the Nymi Band to provide end-user authentication and e-signatures with various Nymi-Enabled Applications(NEAs).

You can deploy the Nymi Connect in two different configurations, where you install the Nymi Agent software on each user terminal or where you deploy a single instance of the Nymi Agent in a centralized location and configure the user terminals to use the centralized Nymi Agent.

Review the following information to decide which configuration to deploy.

Decentralized Nymi Agent	When the user terminals in your environment are thick clients and you install the MES application on the user terminal.
Centralized Nymi Agent	When the user terminals in your environments are thin clients that connect to an RDP or Citrix server to access the MES application.

Consider the following:

- Most deployments make use of a Centralized Nymi Agent configuration.
- You can deploy a configuration that uses a mixture of user terminals with centralized or decentralized Nymi Agent but for simplicity Nymi recommends that you choose one configuration, and then configure all user terminals to use a centralized or decentralized Nymi Agent.

The following figure provides a high level overview of the components in the Nymi solution with Nymi Connect.

Components in a Centralized Nymi Agent Configuration

The following figure provides a high-level overview of the Connected Worker Platform with a centralized Nymi Agent and the TCP ports that are used between the components for communication.

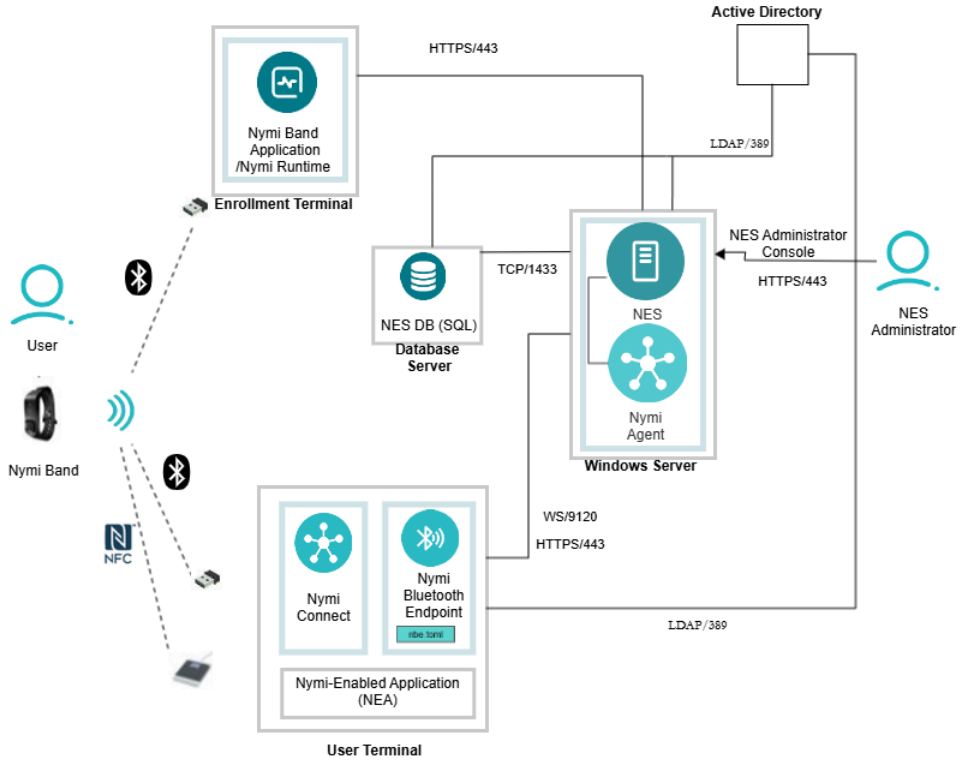


Figure 1: Connected Worker Platform with Nymi Connect components and connection ports in a Centralized Nymi Agent Configuration

The Nymi Connect Solution consists of the following components.

Table 2: Connected Worker Platform Components

Component	Description
Enrollment Terminal	Windows 10 or Windows 11 endpoint that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal that you use to enroll a new user and link them to their Nymi Band. The Nymi Band Application requires the Nymi Runtime application, which the Nymi Band Application automatically installs. The Nymi Band Application communicates with the Nymi Band through the Nymi-supplied Bluetooth adapter, which you plug into a USB port on the enrollment terminal.
Nymi Band	A wearable device that is associated with the biometrics of a single user. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled.

Component	Description
NES	Windows-based management server and collection of services that administrators access through a web-based application. NES coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates.
NES Administrator Console	A web application that provides NES Administrator with an interface to manage the NES configuration and users.
Domain Controller (DC)	Windows server with Active Directory.
User Terminal	Windows 10 or Windows 11 endpoint on which you install Nymi components that allow users to perform authentication tasks with a Nymi Band tap on the NFC reader or Bluetooth Adapter.
Nymi Bluetooth Endpoint	A component of the Nymi Runtime that you install on each user terminal. A component of the Nymi Runtime that provides an interface between the Bluetooth Adapter (BLE) and the Nymi Agent. You deploy Nymi Bluetooth Endpoint Daemon (NBEd) on individual workstations to provide Bluetooth communication with Nymi Bands. Nymi Bluetooth Endpoint communicates with the Nymi Bands through the Nymi-provided BLE Adapter, which you plug into a USB port on the user terminal.
nbe.toml	Configuration file that you create on each user terminal when the solution uses a centralized Nymi Agent. This file defines the hostname on which you installed the Nymi Agent and the connection port on which to communicate with the Nymi Agent.
Centralized Nymi Agent	Nymi Runtime component that you install in a central location on a single machine or a cluster of two or more machines that is accessible to all user terminals, for example on the server with the NES application. A component of the Nymi Runtime that provides BLE management, manages operations and message routing. Facilitates communication between a Nymi-Enabled Application(NEA) and the Nymi Band, and maintains knowledge of the Nymi Band presence and authenticated states. A component of the Nymi Runtime that provides BLE management, manages operations and message routing. Facilitates communication between a Nymi-Enabled Application(NEA) and the Nymi Band, and maintains knowledge of the Nymi Band presence and authenticated states.

Firewall Port Requirements

The following tables summarizes the TCP port requirements for the Nymi Connect Solution.

Table 3: Firewall Port Requirements

Component	Port Requirements
Enrollment Terminal	Port 389 to the Active Directory server for LDAP communication. Port 443 to the NES server for HTTPS communication.
User Terminal	Port 443 to the NES server for HTTPS communication. Port 9120 to the centralized Nymi Agent server for web socket communications, in configurations that install Nymi Bluetooth Endpoint on the user terminal and the Nymi Agent on a server.
SQL Server	Database server that contains tables that store information about the NES configuration and the Nymi Bands. For Proof of Concept (POC) and pre-production environments, you can use the Nymi-provided SQL Server Express software. For production environments Nymi recommends that you use SQL server. The same server or another server contains the eInfortree database.

Use Cases

A user can use their authenticated Nymi Band to log into POMSnet and e-signatures in POMSnet that you define and configure in the Nymi Connect *application.json* file.

Note: Nymi Connect does not support using the Nymi Band to log into POMSnet with Okta.

Preparing for an Nymi Connect Deployment

Review this section for information about the support application versions, prerequisite requirements and the steps that you must perform to prepare for the Nymi Connect deployment.

Supported User Terminals

You can install the Nymi Connect on the following operating systems:

- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows 2016
- Microsoft Windows 2019
- Microsoft Windows 2022

Note: Nymi Connect supports access to applications through a Citrix server and RDP session host.

Supported Browsers

This release of Nymi Connect supports Microsoft Edge 135.0.3179.66(64-bit) in Internet Explorer mode.

Supported Connected Worker Platform versions

This release requires Connected Worker Platform(CWP) 1.18.0 and later.

Pre-requisites

The user terminal on which you install Nymi Connect must:

- Have network connectivity to Nymi Enterprise Server(NES)
- Be joined to the same domain as NES.
- Have Nymi Runtime(Nymi Bluetooth Endpoint) installed.

Preparing Microsoft Edge Browser

Perform the following steps to configure the `Microsoft Edge` browser in Internet Explorer mode.

About this task

Procedure

1. Open `Microsoft Edge`, and open **`Settings`**.
2. In the **`Search settings`** field, type ***Compatibility***.
3. In the **`Allow sites to be reloaded in Internet Explorer mode (IE mode)`** section, from the drop list, select **`Allow`**, as shown in the following figure.

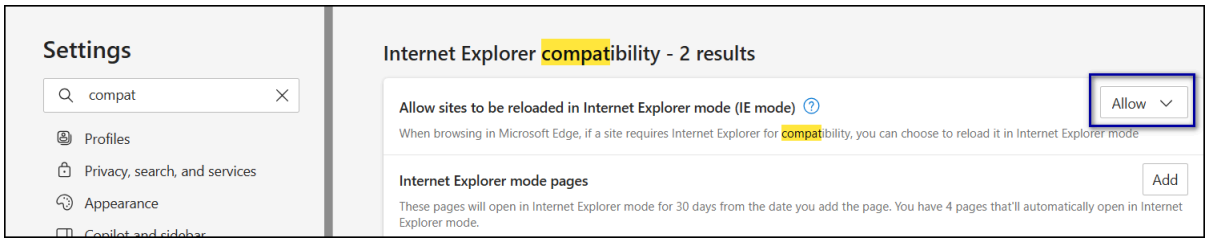


Figure 2: Allow option

4. In the `Internet Explorer mode pages` section, click **Add**,as shown in the following figure.

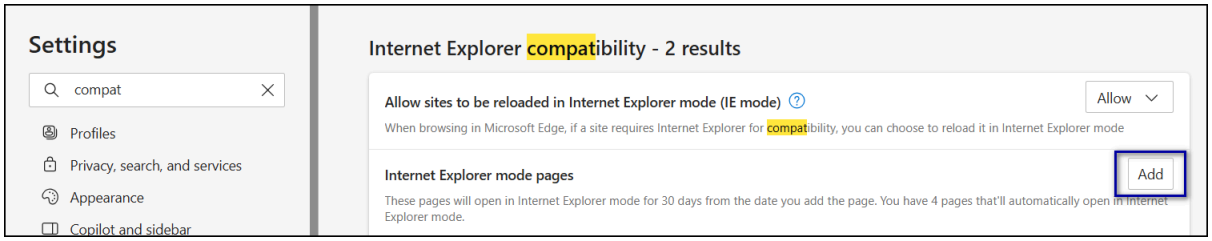


Figure 3: Allow option

5. In the `Add a Page` field, type the URL to your POMSnet instance, and then click **Add**.

   The following figure provide as an example of the `Add a Page` window.

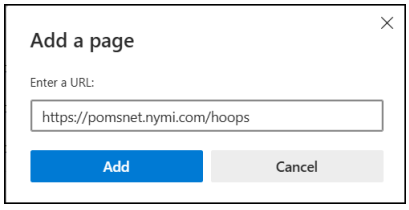


Figure 4: Add a Page

6. Click **`Internet options`**, as shown in the following figure.

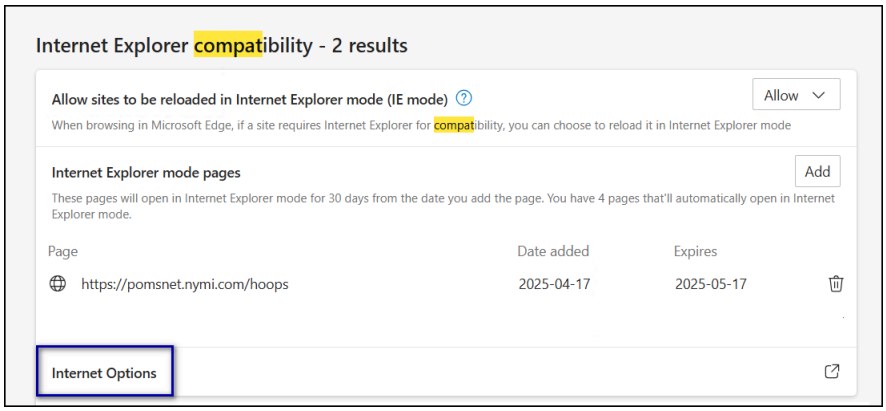


Figure 5: Internet Options

7. On the `Internet Options` window, select the **`Security`** tab, and then select **`Trusted Sites`**, as shown in the following figure.

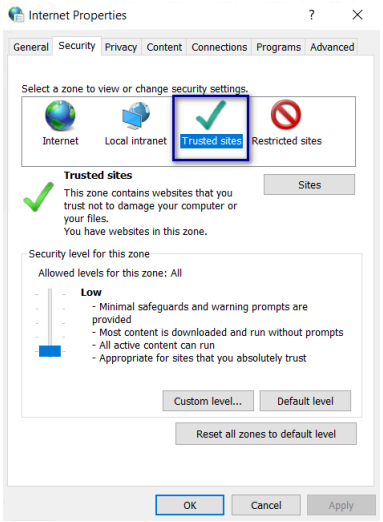


Figure 6: Trusted Sites

8. Click **`Sites`**, as shown in the following figure.

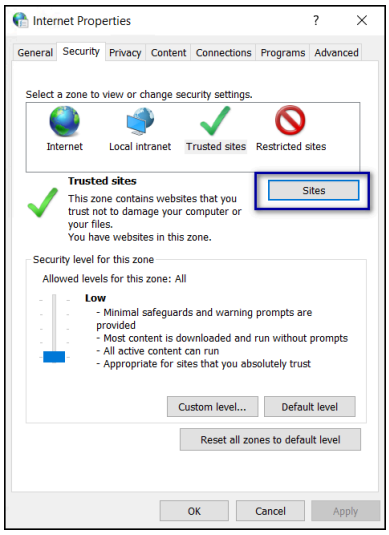


Figure 7: Sites

9. On the `Add this website to the zone` field, type the URL to POMSnet, and then click **Add**.

   The following figure provides an example of the `Trusted Sites` window.

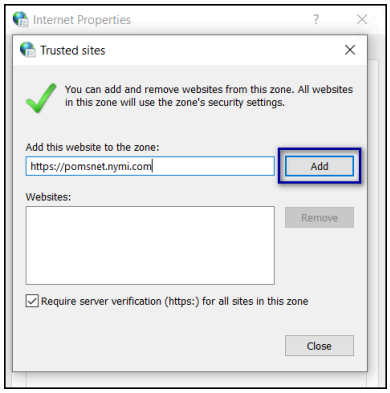


Figure 8: Trusted Sites

10. Click **`Close`**.
11. On the `Internet Properties` window, click **`OK`**.
12. In the browser, navigate to the POMSnet login page.
13. Click the **`Settings and more`** option, and then select **`Reload in IE mode`**, as shown in the following figure.

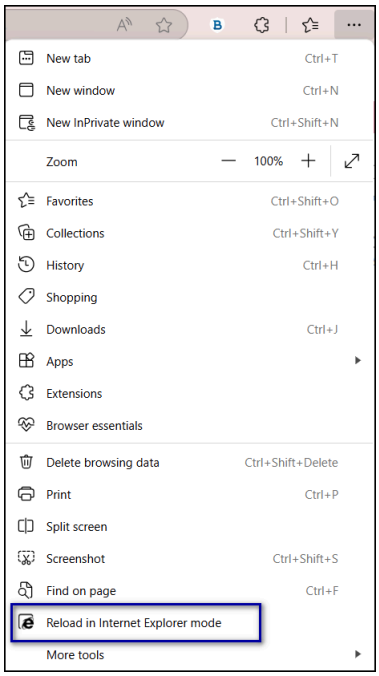


Figure 9: Reload in IE mode

The page reloads in Internet Explorer mode and a messages appears before below the navigation pane, as shown in the following figure.

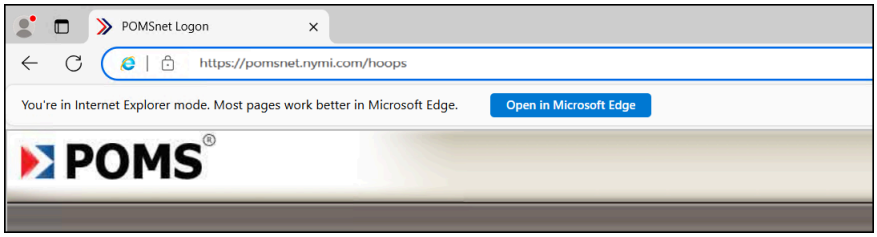


Figure 10: Trusted Sites

Deploy Nymi Components in a Centralized Nymi Agent Configuration

Install and configure the required software on the enrollment terminal and end user terminals.

Note: This guide assumes that you have deployed the NES in the environment. *Nymi Connected Worker Platform—Deployment Guide* describes how to deploy NES.

Configuring the Required NES Policies Options

To allow the Nymi Connect application to store encrypted passwords, enable the Nymi Lock Control option in the active NES policy.

About this task

Before users enroll their Nymi Bands, perform the following tasks from a Web Browser to enable the Nymi Lock Control.

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. In the **`Lock Control`** section, select the **`Enable Nymi Lock Control`** option.
   The following figure provides an example of the Lock Control policy settings.

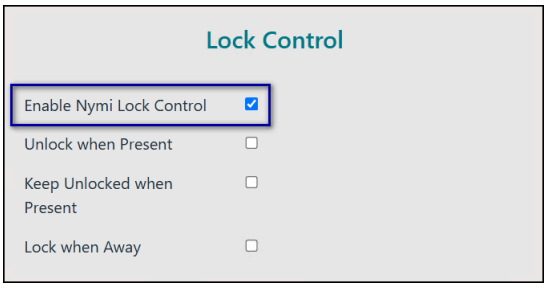


Figure 11: Enable Lock Control

Note: It is not necessary to select other Lock Control options.

5. Click **Save**.

Set Up a Centralized Nymi Agent

When your environment uses iOS devices, applications on RDP/Citrix session hosts, and web-based Nymi-Enabled Application(NEA)s, you must deploy a centralized Nymi Agent on a Windows server in the environment, such as the Nymi Enterprise Server(NES) server.

The Nymi Agent has two server interfaces:

- Standard Nymi Agent interface. By default, standard Nymi Agent interface connect over plain text websocket.
- Nymi WebAPI interface. By default Nymi WebAPI interface is disabled.

Nymi recommends that you configure the Nymi Agent to use secure websocket connections for both standard Nymi Agent interface, and if enabled, the Nymi WebAPI interface. This chapter provides more information.

Importing the Root CA certificate

Perform the following steps only if the Root CA issuing the TLS server certificate is not a Trusted Root CA. For example, when you use a self-signed TLS server certificate.

Before you begin

Install the Root CA on the following machines:

- All user terminals, including user terminals that run Nymi-Enabled Applications
- Enrollment terminal
- Centralized Nymi Agent

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.

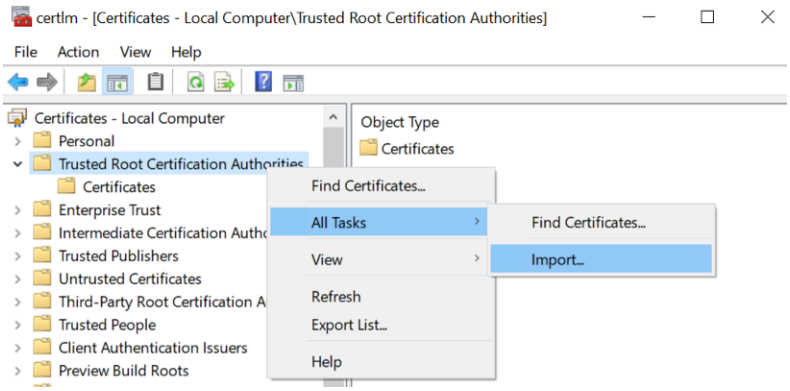


Figure 12: certlm application on Windows 10

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

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

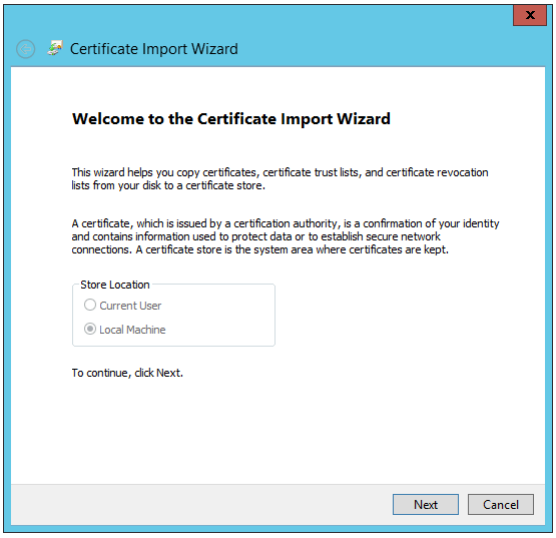


Figure 13: Welcome to the Certificate Import Wizard screen

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.

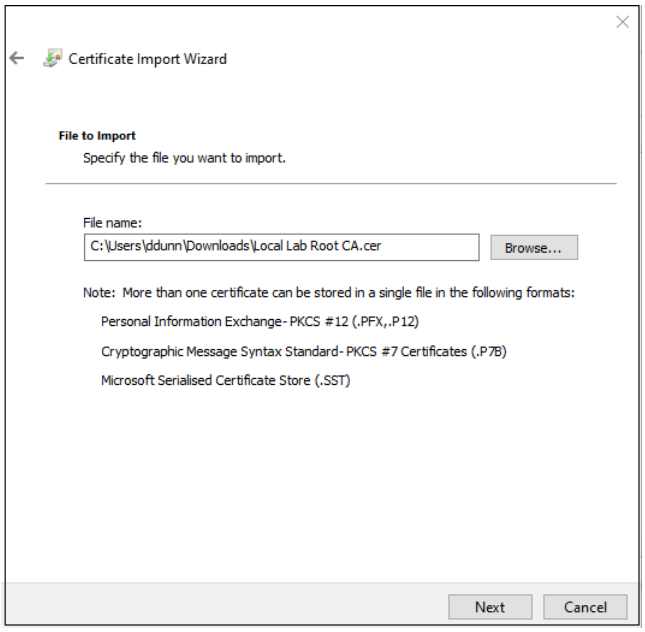


Figure 14: File to Import screen

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`**.

Installing/Updating Centralized Nymi Agent

Install or update the Nymi Agent application, which is included in the Nymi Runtime installation package, on a server in the environment.

About this task

When you install/update the Nymi Runtime software, you can choose to install the Nymi Agent application only.

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the *..\nymi-sdk\windows\setup* folder, right-click the *Nymi Runtime Installer version.exe* file, and select **`Run as administrator`**.
4. On the `Welcome` page, click **`Install`**.
5. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
7. On the `Nymi Runtime Setup` page, expand **`Nymi Runtime`**.

8. Select **`Nymi Bluetooth Endpoint`**, and then select **`Entire feature will be unavailable`**.

   The following figure provides an example of the `Nymi Runtime Setup` window with option to make **`Nymi Bluetooth Endpoint`** unavailable.

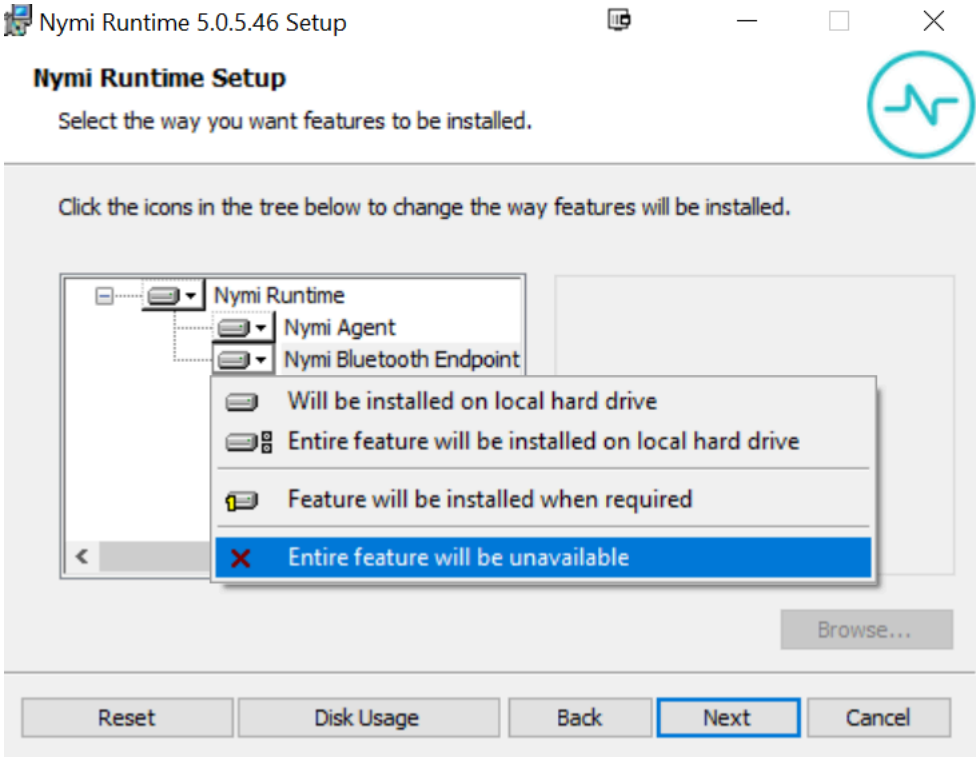


Figure 15: Nymi Bluetooth Endpoint feature will be unavailable

9. Observe that **`Nymi Bluetooth Endpoint`** is not available, as shown in the following figure, and then click **`Next`**.

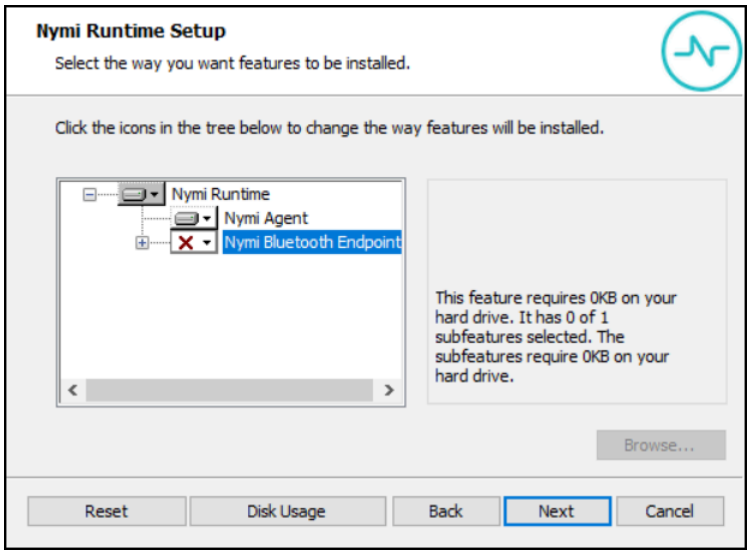


Figure 16: Nymi Bluetooth Endpoint feature is not available

10. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:

    - Accept the default service account NTAuthority\LocalService, click **`Next`**.
    - For non-English Windows Operating Systems and for Nymi WebAPI configurations where you install the centralized Nymi Agent on the NES server, choose the LocalSystem account from the drop list, and then click **`Next`**.

    Note: The service account must have permission to run as a service. Enable Service Log On provides more information about how to modify the local policy to enable this permission for the service account.

    The following figure shows the `Service Account` window.

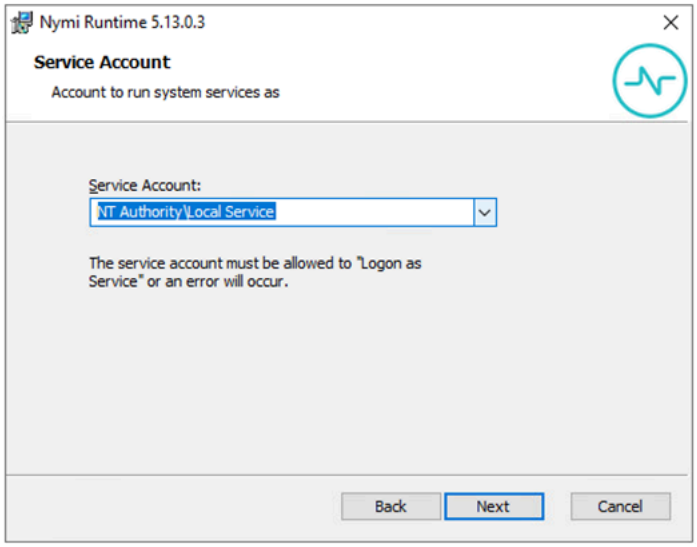


Figure 17: Nymi Runtime Service Account window

11. On the `(Optional) Nymi Infrastructure Service Account` window, specify the username and password of the Nymi Infrastructure Service Account. When you specify the username, include the domain name, for example *tw-lab\nymi_infra_service_acct*.

    The following figure shows the `Nymi Infrastructure Service Account` window.

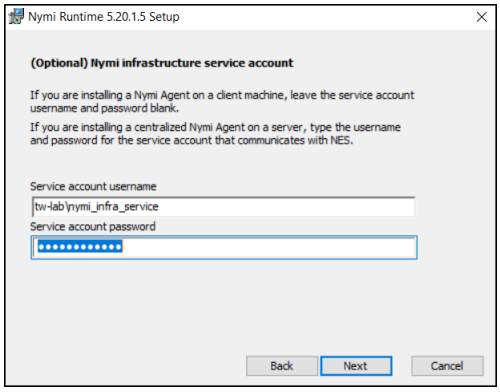


Figure 18: Nymi Infrastructure Service Account window

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

    - credentials-contains the encrypted credentials for the Nymi Infrastructure Service Account
    - Private key, which is used to encrypt the credentials.
    - Public key, which is used to encrypt the credentials.

12. On the `Ready to install` page, click **`Install`**.
13. Click **`Finish`**.
14. On the `Installation Completed Successfully` page, click **`Close`**.

Configuring the Nymi Agent

A centralized Nymi Agent uses a TOML formatted configuration file to set configuration parameters, such as defining the log level, enabling Nymi WebAPI, and enabling the use of secure websocket communications between the centralized Nymi Agent and other Nymi components.

About this task

Nymi provides a sample TOML file that you can rename and edit to define the configuration for your environment and use case. Perform the following steps on the Nymi Agent machine.

Procedure

1. Change to the *C:\Nymi\NymiAgent* directory.
2. Rename the *C:\Nymi\NymiAgent\nymi_agent_default.toml* file to *C:\Nymi\NymiAgent\nymi_agent.toml*
3. Edit the *C:\Nymi\NymiAgent\nymi_agent.toml*. The following table summarizes the available parameter setting and when to use each setting.

   Note: The TOML file has several sections and some sections contain parameter names that are the same. Ensure that you are in the correct section before you make updates.

Parameter and Sample Value	Section Name	Description
log_level = "warn"	[agent]	Required. Defines the debug logging level. Change the value when instructed by Nymi. Support values include: • error—to log only errors • warn—to log both errors and warnings • info—to log errors, warnings, and activity • debug—to log everything including debugging information The default value is *warn*.

Parameter and Sample Value	Section Name	Description
protocol	[agent]	Optional. To enable the standard Nymi Agent to use secure websocket communications, uncomment protocol and change the value to wss. **Note:** Requires the configuration of the *cacertfile*, *cacert*, and *keyfile* parameters in the [agent] section. For example, protocol = "wss"
port	[agent]	Optional. Defines an alternate server port on which Nymi Agent communicates with the Nymi Bluetooth Endpoint and NEAs. The default port number is 9120. Nymi recommends that you use the default port number.
cacertfile	[agent]	Required when you want to use the wss protocol to secure communication between the centralized Nymi Agent and Nymi Bluetooth Endpoint, and Nymi Agent and native NEAs. Uncomment and specify the path to the PEM-formatted CA certificate bundle. The CA certificate bundle must start from the root CA and end in the subordinate CA issuing the server certificate. **Note:** Requires the configuration of *protocol= "wss"*, *certfile* and *keyfile* parameters in the [agent] section. For example: cacertfile = "certs/LocalLabRootCA3.pem"

Parameter and Sample Value	Section Name	Description
certfile	[agent]	Required when you want to use the wss protocol to secure communication between the centralized Nymi Agent and Nymi Bluetooth Endpoint, and Nymi Agent and native NEAs. Uncomment and specify the path to the TLS certificate file containing the Nymi Agent server certificate in PEM format. **Note:** Requires the configuration of *protocol= "wss"*, *cacertfile*, and *keyfile* parameters in the [agent] section. For example: "certfile = "certs/tw-srv1.tw-lab.local-cert.pem"
keyfile	[agent]	Required when you want to use the wss protocol to secure communication between the centralized Nymi Agent and Nymi Bluetooth Endpoint, and Nymi Agent and native NEAs. Uncomment and specify the path to the TLS certificate private key file, unencrypted and PEM formatted. **Note:** Requires the configuration of *protocol= "wss"*, *cacertfile*, and *certfile* parameters in the [agent] section. For example: "keyfile = "certs/tw-srv1.tw-lab.local-key.pem"
nea_name = "NymiWebAPI"	[nes]	Required for Nymi WebAPI. Uncomment this parameter to set the NEA name for the embedded NEA WebAPI server application.

Parameter and Sample Value	Section Name	Description
nes_url = "https://server.name.local.com" For example, https://myserver.name.local.com	[nes]	Required for Nymi WebAPI. Uncomment and specify the host URL for the NES server. Include only the protocol and hostname portion of the URI.
directory_service_id = "NES_DPS"	[nes]	Required for Nymi WebAPI. Uncomment and specify the instance name for NES. For example, if your NES URL is https://server.name.local.com/NES, the directory/instance name is NES. For example, *directory_service_id = "NES"*
credentials_location = certs/	[nes]	Required when you specified a Nymi Infrastructure Service Account during the Nymi Agent installation. Uncomment this line and leave the default value. The *credentials_location* parameter enables the use of the Nymi Infrastructure Service Account to complete authentication tasks with underlying functionality that improves the performance of Nymi Band taps in web-based NEAs and with BLE Taps. **Note:** The *certs* folder contains a file with the encrypted username and password for the Nymi Infrastructure Service Account.

Parameter and Sample Value	Section Name	Description
protocol = "wss" or *protocol = "ws"*	[webapi]	Required for Nymi WebAPI. Defines the connection protocol. If your deployment does not use Nymi WebAPI, leave both lines commented out. If your deployment uses Nymi WebAPI, uncomment one of the following lines: • *protocol = "wss"* To enable secure websocket connections. • *protocol = "ws"* To use plain text websocket connections. **Note:** Requires the configuration of the *cacertfile*, *certfile*, and *keyfile* parameters in the [webapi] section.
port = 443 or *port = 80*	[webapi]	Optional for Nymi WebAPI. Defines an alternate server port on which Nymi Agent listens for Nymi WebAPI client WebSocket connections. By default the *ws* protocol listens on 80 and the *wss* protocol listens on 443. To change the default port uncomment one of the following lines and specify the port number that applies to your configuration: • For the *ws* protocol, uncomment *port = 80*. • For the *wss* protocol, uncomment *port = 443*.

Parameter and Sample Value	Section Name	Description
cacertfile = "path/certfile.pem"	[webapi]	Required when the Nymi Agent uses the Nymi WebAPI with wss. Uncomment and specify the path to the PEM-formatted CA certificate bundle. The CA certificate bundle must start from the root CA and end in the subordinate CA issuing the server certificate **Note:** Requires the configuration of the *protocol = "wss"*, *certfile*, and *keyfile* parameters in the [webapi] section. For example: "certs/LocalLabRootCA3.pem"
certfile = "path/certfile.pem"	[webapi]	Required when the Nymi Agent uses the Nymi WebAPI with wss. Uncomment and specify the path to the TLS certificate in PEM format. **Note:** Requires the configuration of the *protocol = "wss"*, *cacertfile*, and *keyfile* parameters in the [webapi] section. For example: "certs/tw-srv1.tw-lab.local-cert.pem"
keyfile = "path/keyfile.pem"	[webapi]	Required when the Nymi Agent uses the Nymi WebAPI with wss. Uncomment and specify the path to the TLS certificate private key in unencrypted PEM format. **Note:** Requires the configuration of the *protocol = "wss"*, *cacertfile*, and *certfile* parameters in the [webapi] section. For example: "certs/tw-srv1.tw-lab.local-key.pem"

4. For secure Nymi Agent and secure WebSocket, copy the following files to the *C:\Nymi\NymiAgent\certs* directory:

- 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

Note: Secure Nymi Agent and secure WebSocket can share the CA root certificate bundle file, the server certificate file, and the server certificate private key file. Therefore, create only one copy of each file for both secure Nymi Agent and secure WebSocket.

5. Restart the **`Nymi Agent`** service.

Set Up Enrollment Terminal

There are two methods that you can use to configure the computer that users use to perform Nymi Band enrollments.

Decentralized Enrollment Terminal	You install the Nymi Band Application on one or more thick client user terminals. This method: • Organizations control when and where a user can perform an enrollment. • Supports a supervised enrollment process.
Centralized Enrollment Terminal	You install the Nymi Band Application on a Citrix session host and users can access the Nymi Band Application from the Citrix Storefront. This method: • Allows users to perform enrollments from any thin client. • Supports an unsupervised enrollment process.

Nymi recommends that you deploy a decentralized enrollment terminal.

Set Up a Decentralized Enrollment Terminal

Before a user can enroll and authenticate the Nymi Band, the NES Administrator must perform the following actions on at least one machine in the environment (the enrollment terminal). You cannot use a thin client as an enrollment terminal.

- Insert the Nymi-supplied Bluetooth adapter into an available USB port.
- Install the Nymi Band Application. The Nymi Band user requires physical access to the enrollment terminal.
- Set the NES_URL registry key.

Install the Nymi Band Application

Perform the following steps to install the Nymi Band Application on each enrollment terminal that you will use to enroll and authenticate users to their Nymi Bands.

You can perform a customizable installation or a silent installation.

Installing/Updating the Nymi Band Application

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Before you begin

For an update, uninstall the previous version of Nymi Runtime.

Procedure

1. Download the Nymi Band Application package.
2. Double-click the *Nymi-Band-App-installer-v_`version`.exe* file.
3. On the `User Account Control` window, click **`Yes`**.
4. On the `Prerequisites` window, click **`Next`**.
5. On the `Welcome` page, click **`Install`**.
6. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
7. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
8. On the `Nymi Runtime Setup` window, click **`Next`**.
9. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
   - Accept the default service account NTAuthority\LocalService, click **`Next`**.
   - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.

   Note: The service account must have permission to run as a service. Enable Service Log On provides more information about how to modify the local policy to enable this permission for the service account.

   The following figure shows the `Service Account` window.

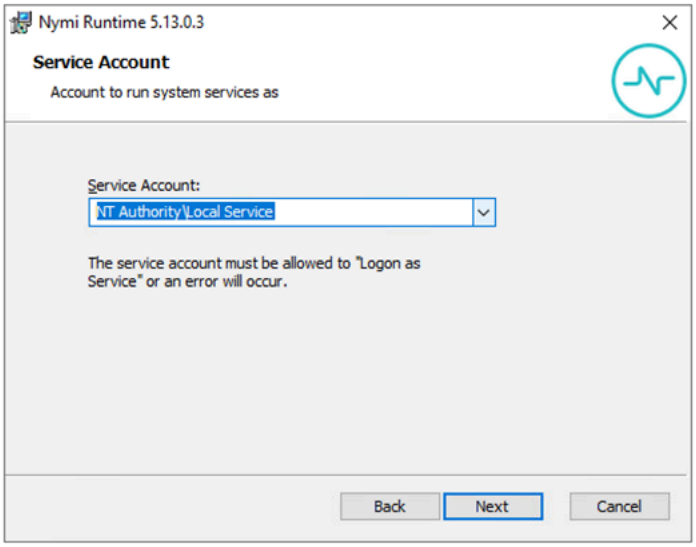


Figure 19: Nymi Runtime Service Account window

10. On the `(Optional) Nymi Infrastructure Service Account`, click **`Next`**.

    Only deployments that use web-based Nymi-enabled Applications(NEAs) with a centralized Nymi Agent require you to configure the Nymi Infrastructure Service Account.

11. On the `Ready to install` page, click **`Install`**.
12. Click **`Finish`**.
13. On the `Installation Completed Successfully` page, click **`Close`**.
14. On the `Welcome to Nymi Band Application Setup Wizard` window, click **`Next`**.
15. On the `Select Installation Folder` window, click **`Next`** to accept the default installation location.
16. In the `Ready to Install` window, click **`Install`**.
17. On the `Completing the Nymi Band Application Setup Wizard` window, click **`Finish`**.

What to do next

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

Installing the Nymi Band Application Silently

Perform the following steps to install or update the Nymi Band Application silently, for example, when you want to install the software remotely by using a software distribution application.

Before you begin

Before you install the Nymi Band Application, install the Nymi Runtime

Procedure

1. Save the Nymi Band Application package, provided to you by your Nymi Solution Consultant.

2. Launch the command prompt as administrator.
3. From the folder that contains the Nymi Band Application, type *Nymi-Band-App-installer-v_`version`.exe /exenoui /q*

   Where you replace *`version`* with the version of the Nymi installation file.

   The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, the Nymi Band Application and Nymi Runtime applications appear in the `Program and Features` applet.

   Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

Configuring the Nymi Enterprise Server URL

After you install the Nymi Band Application, perform the following steps to ensure that the enrollment process connect to the correct Nymi Enterprise Server(NES).

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software > Nymi`**.

   Note: If you installed the Nymi Band Application on a Citrix server, navigate to HKEY_CURRENT_USER instead of HKEY_LOCAL_MACHINE.
4. Right-click **`Nymi`**, and then select **`New > Key`**. Name the key **`NES`**.
5. Right-click **`NES`**, and then select **`New > String value`**.
6. In the **`Value`** field, type ***URL***.
7. Double-click **`URL`** and in the **`Value Data`** field, type ***https://nes_server/NES_service_name/*** or ***http://`nes_server`/`NES_service_name`*** depending on the NES configuration

   where:

   - *`nes_server`* is the FQDN of the NES host. The FQDN consists of the ***hostname.domain_name***. You can also find the FQDN by going to the server on which you deployed NES viewing the properties of the computer. The *`nes_server`* is the value that appears in the **`Full computer name`** field.
   - *`NES_service_name`* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
8. Click **`OK`**.

Set Up Centralized Enrollment

In this configuration, you perform the following steps:

- Install the Nymi Band Application on the Citrix/RDP server, without installing Nymi Runtime.

- Configure the Nymi Band Application to use the centralized Nymi Agent.
- Install the Nymi Bluetooth Endpoint on the thin client that users will use to access the Nymi Band Application.
- Configure the Nymi Bluetooth Endpoint on the thin client enrollment terminal to use the centralized Nymi Agent.

Installing the Centralized Nymi Band Application

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Procedure

1. Download the Nymi Band Application package.
2. Double-click the *Nymi-Band-App-installer-v_`version`.exe* file.
3. On the `User Account Control` window, click **`Yes`**.
4. On the `Welcome to Prerequisites` window, click **`Next`**.
5. On the `Prerequisites` window, clear the option to install Nymi Runtime, as shown in the following figure, and then click **`Next`**.

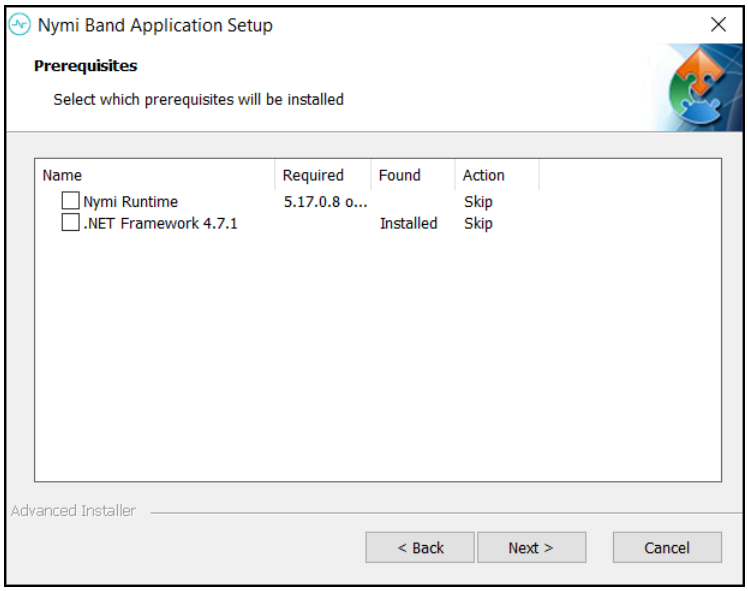


Figure 20: No Nymi Runtime Installation

6. On the `Welcome to Nymi Band Application Setup Wizard` window, click **`Next`**.
7. On the `Select Installation Folder` window, click **`Next`** to accept the default installation location.
8. In the `Ready to Install` window, click **`Install`**.
9. On the `Completing the Nymi Band Application Setup Wizard` window, click **`Finish`**.

Configuring Nymi Band Application to use a Centralized Nymi Agent

Perform the following steps on the enrollment terminal to configure the Nymi Band Application to use a centralized Nymi Agent.

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software > Nymi`**.

   Note: If you installed the Nymi Band Application on a Citrix server, navigate to HKEY_CURRENT_USER instead of HKEY_LOCAL_MACHINE.
4. Right-click **`NES`**, and then select **`New > String value`**.
5. In the **`Value`** field, type ***AgentURL***.
6. Edit the ***AgentURL*** key, and in the **`Value data`** field, type the URL to the Nymi Agent service, in the following format:

   `protocol://agent_server:agent_port/socket/websocket`

   where:

   - *`protocol`* is the websocket protocol to use to connect to the Nymi Agent:
     - ws for websocket.
     - wss for secure websocket.
   - *`agent_server`* is one of the following:
     - For WSS, the FQDN of the centralized Nymi Agent machine.
     - For WS, the IP address of the centralized Nymi Agent machine.
   - *`agent_port`* is the port on which to connect to the centralized Nymi Agent machine, for example 9120.

   For example, for WSS: "wss://agent.nymi.com:9120/socket/websocket"

Configuring the Nymi Enterprise Server URL

After you install the Nymi Band Application, perform the following steps to ensure that the enrollment process connect to the correct Nymi Enterprise Server(NES).

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software > Nymi`**.

   Note: If you installed the Nymi Band Application on a Citrix server, navigate to HKEY_CURRENT_USER instead of HKEY_LOCAL_MACHINE.
4. Right-click **`Nymi`**, and then select **`New > Key`**. Name the key **`NES`**.
5. Right-click **`NES`**, and then select **`New > String value`**.

6. In the **`Value`** field, type ***URL***.
7. Double-click **`URL`** and in the **`Value Data`** field, type ***https://nes_server/NES_service_name/*** or ***http://`nes_server`/`NES_service_name`*** depending on the NES configuration

   where:

   - *`nes_server`* is the FQDN of the NES host. The FQDN consists of the ***hostname.domain_name***. You can also find the FQDN by going to the server on which you deployed NES viewing the properties of the computer. The *`nes_server`* is the value that appears in the **`Full computer name`** field.
   - *`NES_service_name`* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
8. Click **`OK`**.

Install and Configure the Nymi Bluetooth Endpoint

Install the Nymi Bluetooth Endpoint on the thin client that users will access to connect to the Citrix/RDP centralized enrollment terminal. You can install the Nymi Bluetooth Endpoint silently or with the installation wizard.

After you install the Nymi Bluetooth Endpoint, you must update the *nbe.toml* file.

Installing the Nymi Bluetooth Endpoint

Install the Nymi Bluetooth Endpoint on the machine that accesses the Nymi Band Application on a Citrix/RPD session host.

About this task

When you install the Nymi Runtime software, you can choose to install the Nymi Bluetooth Endpoint only.

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the *..\nymi-sdk\windows\setup* folder, right-click the *Nymi Runtime Installer version.exe* file, and select **`Run as administrator`**.
4. On the `Welcome` page, click **`Install`**.
5. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
7. On the `Nymi Runtime Setup` window, expand **`Nymi Runtime`**.
8. Select **`Nymi Agent`**, and then select **`Entire feature will be unavailable`**, as shown in the following figure, and then click **`Next`**.

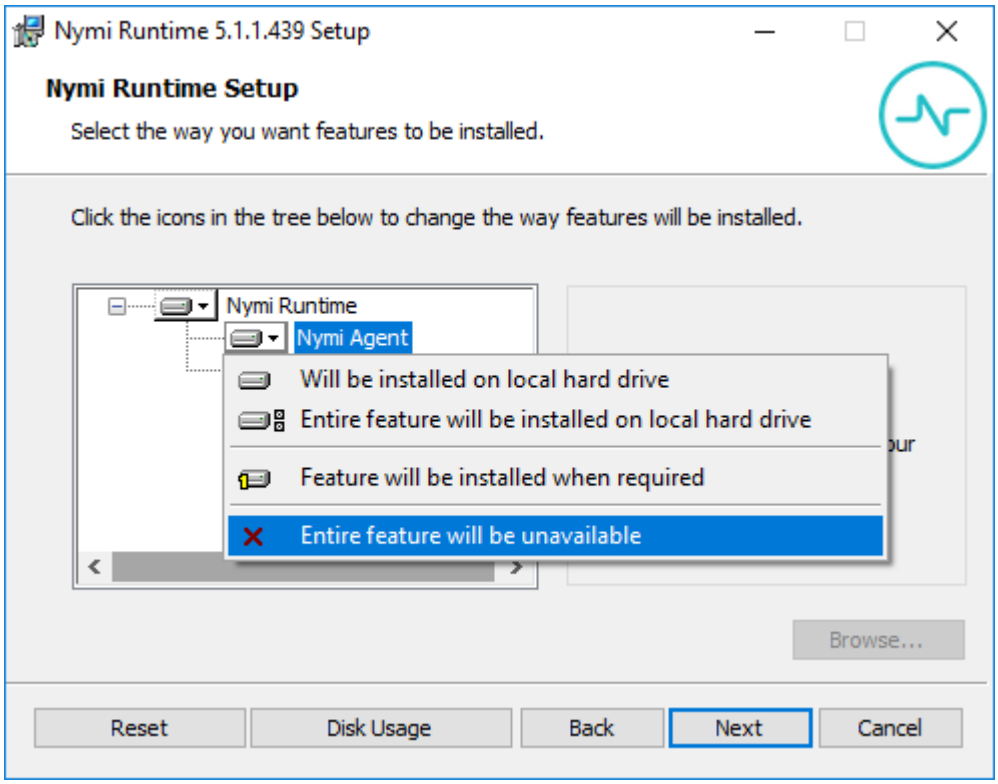


Figure 21: Nymi Agent feature will be unavailable

9. Observe that **`Nymi Agent`** is not available, as shown in the following figure, and then click **`Next`**.

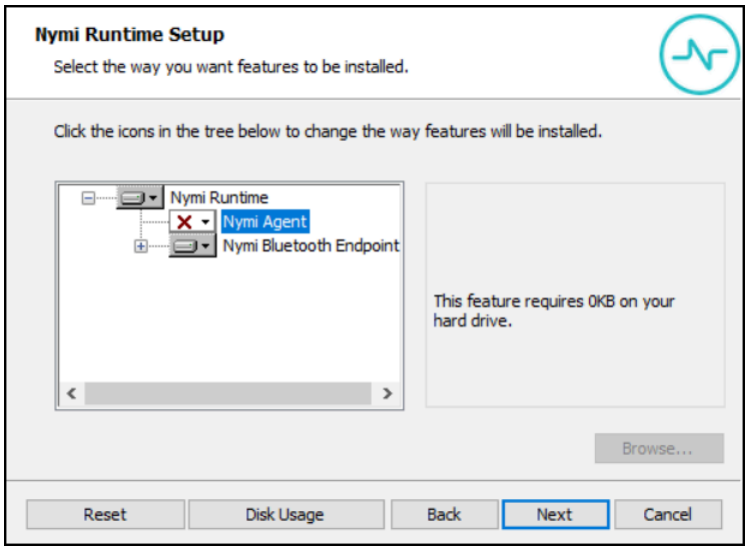


Figure 22: Nymi Agent feature is not available

10. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:

    - Accept the default service account NTAuthority\LocalService, click **`Next`**.

- For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **Next**.

Note: The service account must have permission to run as a service. Enable Service Log On provides more information about how to modify the local policy to enable this permission for the service account.

The following figure shows the Service Account window.

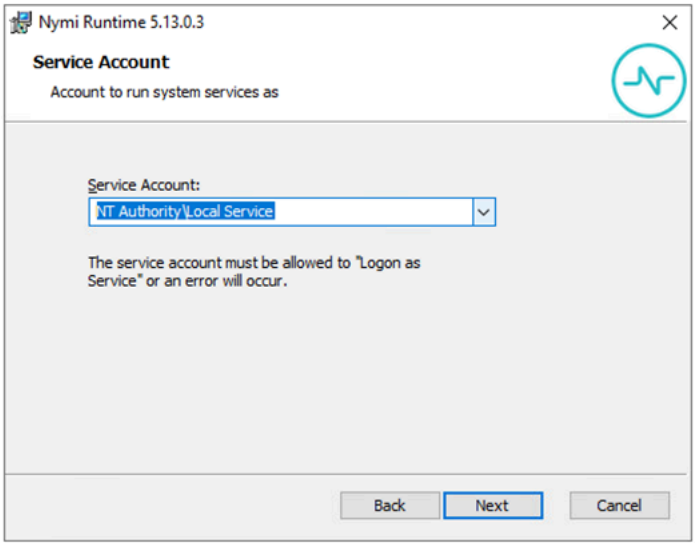


Figure 23: Nymi Runtime Service Account window

11. On the Ready to install page, click **Install**.
12. Click **Finish**.
13. On the Installation Completed Successfully page, click **Close**.

What to do next

Confirm that the status of the Nymi Bluetooth Endpoint service is running.

Installing Nymi Bluetooth Endpoint Silently

Procedure

Run a Command Prompt as administrator.

You can install the Nymi Bluetooth Endpoint silently by typing one of the following commands:

- "Nymi Runtime Installer *version*.exe" /exenoui InstallAgent=0 /q /log NymiRuntimeInstallation.log
- For installations on non-English operating systems,

  "Nymi Runtime Installer *version*.exe" ServiceAccount="LocalSystem" /exenoui InstallAgent=0 /q /log NymiRuntimeInstallation.log

Where you replace *version* with the version of the Nymi installation file.

Note: Ensure that you enclose the filename in double quotes.

The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, Nymi Runtime appears in the `Program and Features` applet and *NymiRuntimeInstallation.log* file contains information about the installation.

Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

What to do next

Confirm that the status of the Nymi Bluetooth Endpoint service is running.

Editing the Nymi Bluetooth Endpoint Configuration File

The Nymi Bluetooth Endpoint file uses the *nbe.toml* file to define the location of a remote Nymi Agent.

About this task

Perform the following steps to specify the URL to the remote Nymi Agent.

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 default agent_url parameter and perform the following changes:
   - For WSS:
     - Change the protocol from ws to wss
     - Replace `127.0.0.1` with the FQDN of the centralized Nymi Agent machine.
   - For WS, replace `127.0.0.1` with the IP address of centralized Nymi Agent machine.

   For example, for WSS:

   ```
   agent_url = "wss://agent.nymi.com:9120/socket/websocket"
   ```

   where ***agent.nymi.com*** is the FQDN of the centralized Nymi Agent machine.

   Note: Optionally, you can also change the communication port from the default value 9120.
4. Save the *nbe.toml* file.
5. Restart the `Nymi Bluetooth Endpoint` service.

What to do next

You can use Group Policies to push the modified *nbe.toml* file to the *C:\Nymi\Bluetooth_Endpoint* folder on each user terminal.

(Optional) Configuring the Communication Protocol

If you use the enrollment terminal to also access NEAs, perform the following steps to disable the legacy protocol.

About this task

Note: After you set this environment variable, user terminals cannot communicate with Nymi Bands that use pre-CWP 1.15.x firmware

Procedure

1. In the Windows search field, type ***env***, and then from the pop-up menu, select **`Edit the System Environment Variables`**.
2. Click **`Environment Variables`**.
3. In the **`System Variables`** section, click **`New`**, and the perform the following actions:
   a) In the **`Variable Name`** field, type *NYMI_NEA_SUPPORT_LEGACY_MODE*
   b) In the **`Variable Value`** field, type ***0***.
   The following figure provides an example of the new variable.

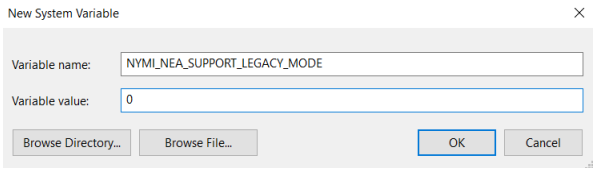


Figure 24: New System Variable window

   c) Click **OK**.

Set Up User Terminals

Bluetooth Adapter Placement

The enrollment terminal and each user terminal requires a Bluetooth adapter. The Bluetooth Low Energy (BLE) radio antenna in the Nymi-supplied BLED112 USB Adapter provides seamless Bluetooth capability between the Nymi Band and devices such as a laptop computer.

To ensure optimal system performance, place the Bluetooth adapter in a location that meets the following criteria:

- Is in clear line of sight to the Nymi Band.
- Is on the same side of the computer that you wear your Nymi Band.
- Is near the computer keyboard.

Note: The presence of liquids between the Nymi Band and Bluetooth adapter negatively affects the Bluetooth signal quality. This includes beverages and the human body. If Bluetooth (BLE) taps behave unexpectedly, consider another placement for the Bluetooth adapter, or edit the Nymi Bluetooth Endpoint configuration file to adjust the signal strength thresholds to perform a BLE tap.

Install and Configure the Nymi Bluetooth Endpoint

Install the Nymi Bluetooth Endpoint on the thin client that users will access to connect to the Citrix/RDP centralized enrollment terminal. You can install the Nymi Bluetooth Endpoint silently or with the installation wizard.

After you install the Nymi Bluetooth Endpoint, you must update the *nbe.toml* file.

Installing the Nymi Bluetooth Endpoint

Install the Nymi Bluetooth Endpoint on the machine that accesses the Nymi Band Application on a Citrix/RPD session host.

About this task

When you install the Nymi Runtime software, you can choose to install the Nymi Bluetooth Endpoint only.

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the *..\nymi-sdk\windows\setup* folder, right-click the *Nymi Runtime Installer version.exe* file, and select **`Run as administrator`**.
4. On the `Welcome` page, click **`Install`**.
5. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
7. On the `Nymi Runtime Setup` window, expand **`Nymi Runtime`**.
8. Select **`Nymi Agent`**, and then select **`Entire feature will be unavailable`**, as shown in the following figure, and then click **`Next`**.

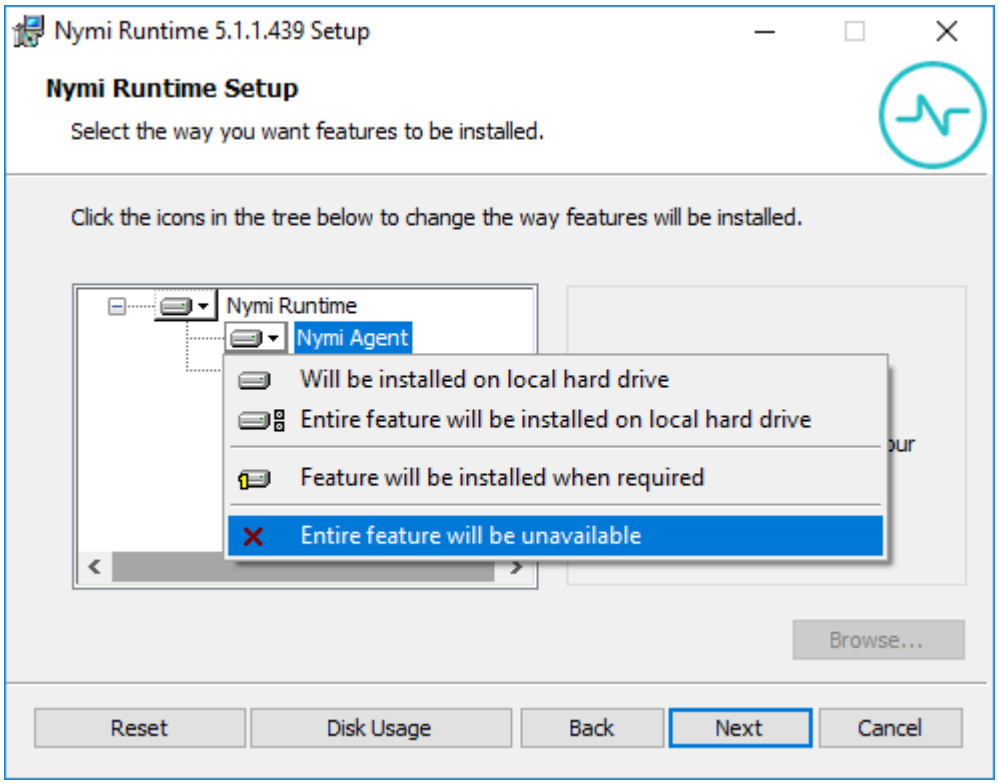


Figure 25: Nymi Agent feature will be unavailable

9. Observe that **`Nymi Agent`** is not available, as shown in the following figure, and then click **`Next`**.

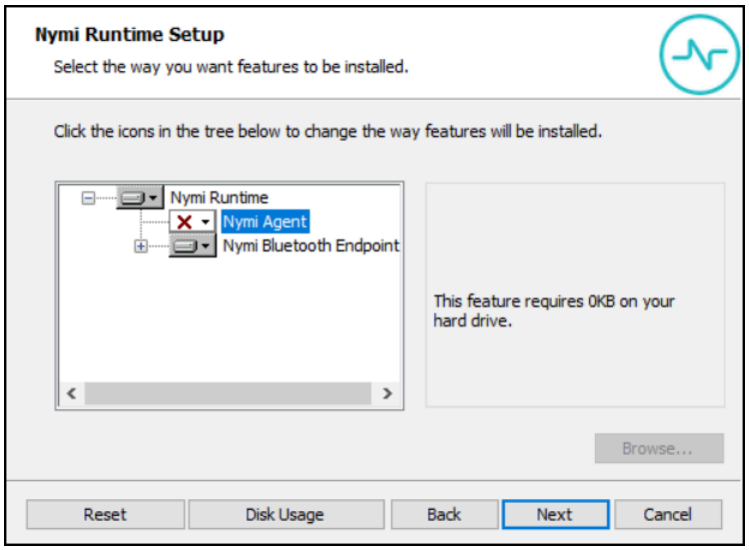


Figure 26: Nymi Agent feature is not available

10. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:

    - Accept the default service account NTAuthority\LocalService, click **`Next`**.

- For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **Next**.

Note: The service account must have permission to run as a service. Enable Service Log On provides more information about how to modify the local policy to enable this permission for the service account.

The following figure shows the Service Account window.

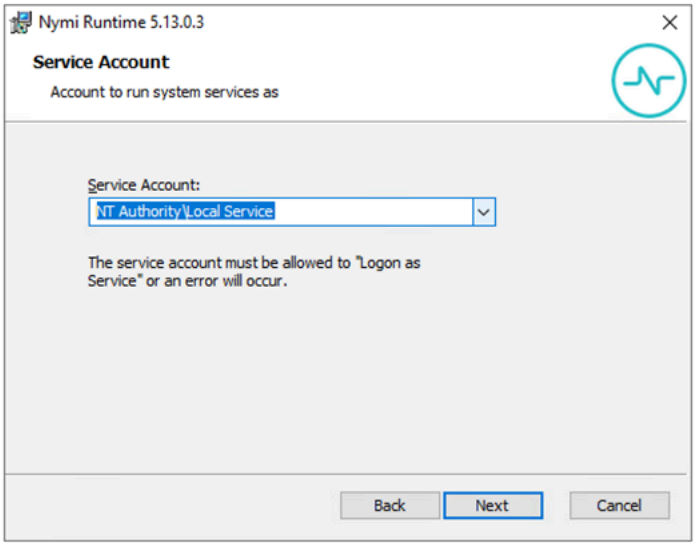


Figure 27: Nymi Runtime Service Account window

11. On the Ready to install page, click **Install**.
12. Click **Finish**.
13. On the Installation Completed Successfully page, click **Close**.

What to do next

Confirm that the status of the Nymi Bluetooth Endpoint service is running.

Installing Nymi Bluetooth Endpoint Silently

Procedure

Run a Command Prompt as administrator.

You can install the Nymi Bluetooth Endpoint silently by typing one of the following commands:

- "Nymi Runtime Installer *version*.exe" /exenoui InstallAgent=0 /q /log NymiRuntimeInstallation.log
- For installations on non-English operating systems,

  "Nymi Runtime Installer *version*.exe" ServiceAccount="LocalSystem" /exenoui InstallAgent=0 /q /log NymiRuntimeInstallation.log

Where you replace *version* with the version of the Nymi installation file.

Note: Ensure that you enclose the filename in double quotes.

The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, Nymi Runtime appears in the `Program and Features` applet and *NymiRuntimeInstallation.log* file contains information about the installation.

Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

What to do next

Confirm that the status of the Nymi Bluetooth Endpoint service is running.

Editing the Nymi Bluetooth Endpoint Configuration File

The Nymi Bluetooth Endpoint file uses the *nbe.toml* file to define the location of a remote Nymi Agent.

About this task

Perform the following steps to specify the URL to the remote Nymi Agent.

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 default agent_url parameter and perform the following changes:
   - For WSS:
     - Change the protocol from ws to wss
     - Replace `127.0.0.1` with the FQDN of the centralized Nymi Agent machine.
   - For WS, replace `127.0.0.1` with the IP address of centralized Nymi Agent machine.

   For example, for WSS:

   ```
   agent_url = "wss://agent.nymi.com:9120/socket/websocket"
   ```

   where ***agent.nymi.com*** is the FQDN of the centralized Nymi Agent machine.

   Note: Optionally, you can also change the communication port from the default value 9120.
4. Save the *nbe.toml* file.
5. Restart the `Nymi Bluetooth Endpoint` service.

What to do next

You can use Group Policies to push the modified *nbe.toml* file to the *C:\Nymi\Bluetooth_Endpoint* folder on each user terminal.

Configuring the NES and Centralized Nymi Agent URLs

After you install Nymi Agent on the user terminal, define the NES and Nymi Agent URLs in the registry.

About this task

Perform the following steps with a local administrator account or run regedit as an administrator.

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software`**.
4. If required, create a new key named **`NES`**.
5. Right-click **`NES`**, and then select **`New > String value`**.
6. In the **`Value`** field, type ***URL***.
7. Double-click **`URL`** and in the **`Value Data`** field, type ***https://nes_server/NES_service_name/*** or ***http://nes_server/NES_service_name*** depending on the NES configuration

   where:

   - *`nes_server`* is the FQDN of the NES host. The FQDN consists of the ***hostname.domain_name***. You can also find the FQDN by going to the server on which you deployed NES viewing the properties of the computer. The *`nes_server`* is the value that appears in the **`Full computer name`** field.
   - *`NES_service_name`* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
8. Click **`OK`**.
9. Right-click **`NES`**, and then select **`New > String value`**.
10. In the **`Value`** field, type ***AgentURL***.
11. Edit the ***AgentURL*** key, and in the **`Value data`** field, type the URL to the Nymi Agent service, in the following format:

    `protocol://agent_server:agent_port/socket/websocket`

    where:

    - *`protocol`* is the websocket protocol to use to connect to the Nymi Agent:
      - ws for websocket.
      - wss for secure websocket.
    - *`agent_server`* is one of the following:

    - For WSS, the FQDN of the centralized Nymi Agent machine.
    - For WS, the IP address of the centralized Nymi Agent machine.
  - *agent_port* is the port on which to connect to the centralized Nymi Agent machine, for example 9120.

  For example, for WSS: "wss://agent.nymi.com:9120/socket/websocket"

12. Click **OK**.
13. Close Registry Editor.
14. Restart the Nymi Bluetooth Endpoint service.

Configuring Nymi Band Application to use a Centralized Nymi Agent

Perform the following steps on the enrollment terminal to configure the Nymi Band Application to use a centralized Nymi Agent.

Procedure

1. Run *regedit.exe*
2. On the User Account Control window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.

   Note: If you installed the Nymi Band Application on a Citrix server, navigate to HKEY_CURRENT_USER instead of HKEY_LOCAL_MACHINE.
4. Right-click **NES**, and then select **New > String value**.
5. In the **Value** field, type ***AgentURL***.
6. Edit the ***AgentURL*** key, and in the **Value data** field, type the URL to the Nymi Agent service, in the following format:

   protocol://agent_server:agent_port/socket/websocket

   where:

   - *protocol* is the websocket protocol to use to connect to the Nymi Agent:
     - ws for websocket.
     - wss for secure websocket.
   - *agent_server* is one of the following:
     - For WSS, the FQDN of the centralized Nymi Agent machine.
     - For WS, the IP address of the centralized Nymi Agent machine.
   - *agent_port* is the port on which to connect to the centralized Nymi Agent machine, for example 9120.

   For example, for WSS: "wss://agent.nymi.com:9120/socket/websocket"

Configuring the Connected Worker Platform Communication Protocol

Starting with Connected Worker Platform(CWP) 1.15, the Nymi solution supports a new, high performance protocol over Bluetooth between the Nymi Runtime and Nymi Bands.

About this task

Perform the following steps on all user terminals (for Evidian environments on Wearable user terminals only) where users access Nymi-enabled Applications(NEAs) to disable the legacy protocol. The enrollment terminal only requires the environment variable if users access NEAs on the enrollment terminal.

Note: After you set this environment variable, user terminals cannot communicate with Nymi Bands that use pre-CWP 1.15.x firmware

Procedure

1. In the Windows search field, type ***env***, and then from the pop-up menu, select **`Edit the System Environment Variables`**.
2. Click **`Environment Variables`**.
3. In the **`System Variables`** section, click **`New`**, and the perform the following actions:
   a) In the **`Variable Name`** field, type *NYMI_NEA_SUPPORT_LEGACY_MODE*
   b) In the **`Variable Value`** field, type ***0***.
   The following figure provides an example of the new variable.

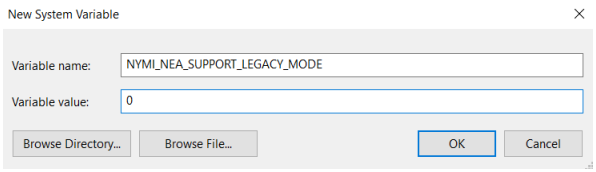


Figure 28: New System Variable window

   c) Click **OK**.

Install Nymi Connect

You can install Nymi Connect silently or with the installation wizard.

Installing Nymi Connect With the Installation Wizard

Perform the following step on each user terminal.

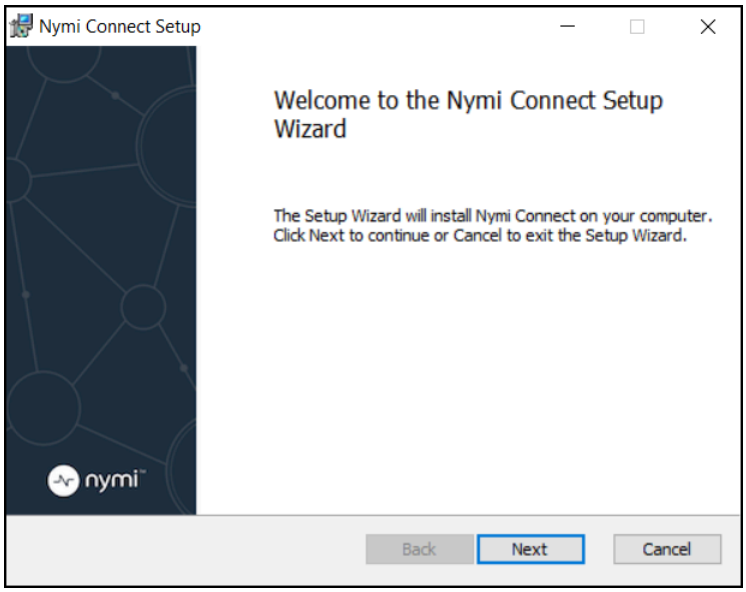
Before you begin

Install the Nymi Runtime software on the user terminal.

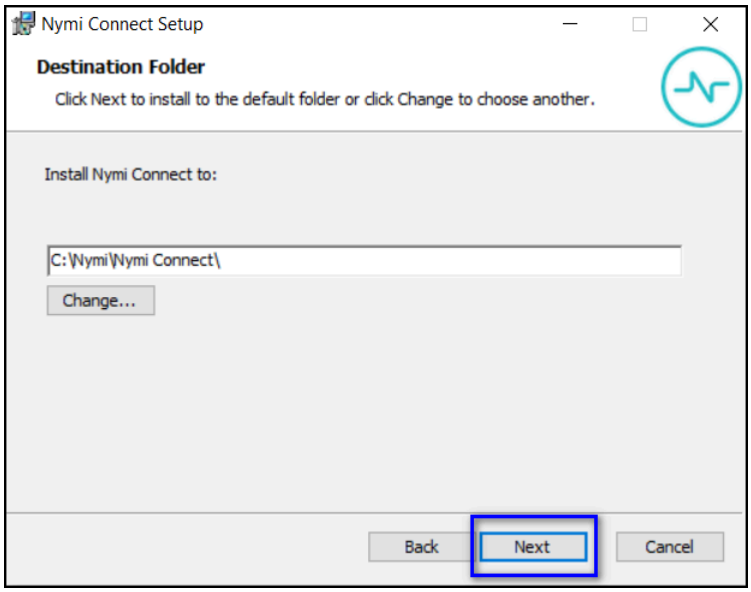
- For centralized Nymi Agent configurations, install Nymi Bluetooth Endpoint component.
- For decentralized Nymi Agent configurations, install the Nymi Agent and Nymi Bluetooth Endpoint components.

Procedure

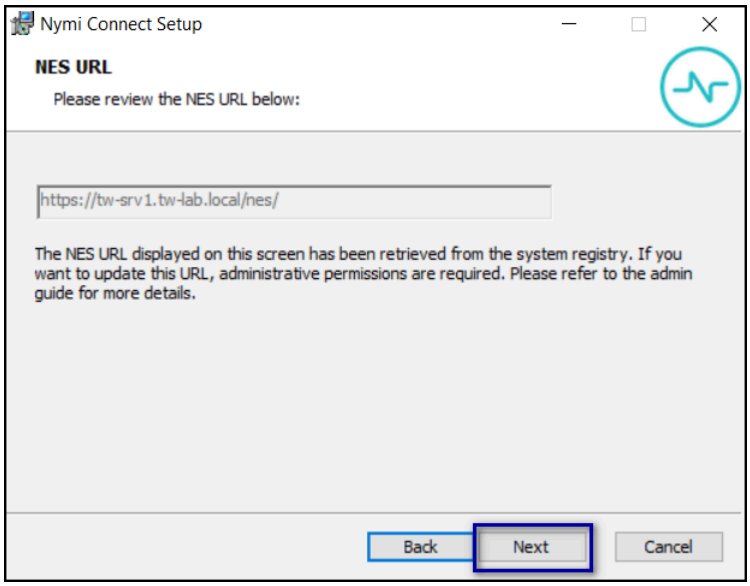
1. Double-click *Nymi Connect Installer-version.exe*
2. Click **`Install`**.
3. On the `User Account Control` pop-up, click **`Yes`**.
4. On the `Welcome to the Nymi Connect Setup Wizard` window, click **`Next`**.



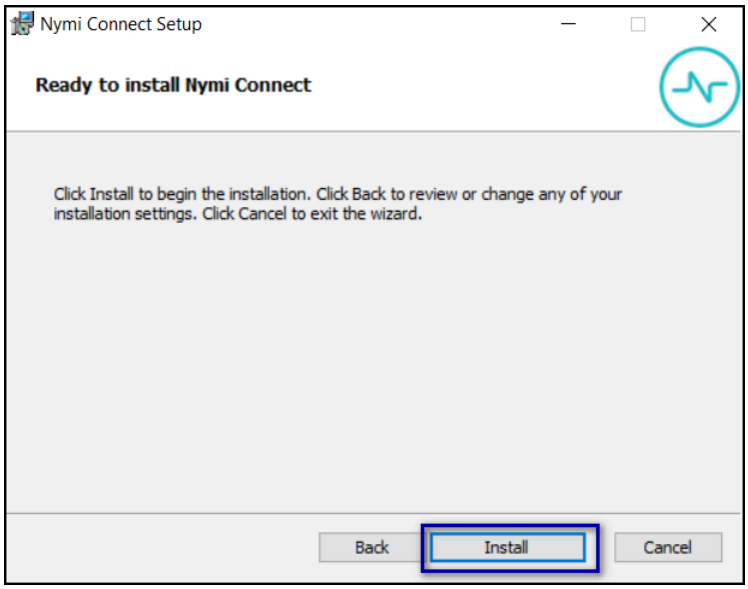
5. On the `Destination Folder` window, click **`Next`** to accept the default installation location, or click **`Change...`**, and then in the `Change destination folder` pop-up select a new installation location.



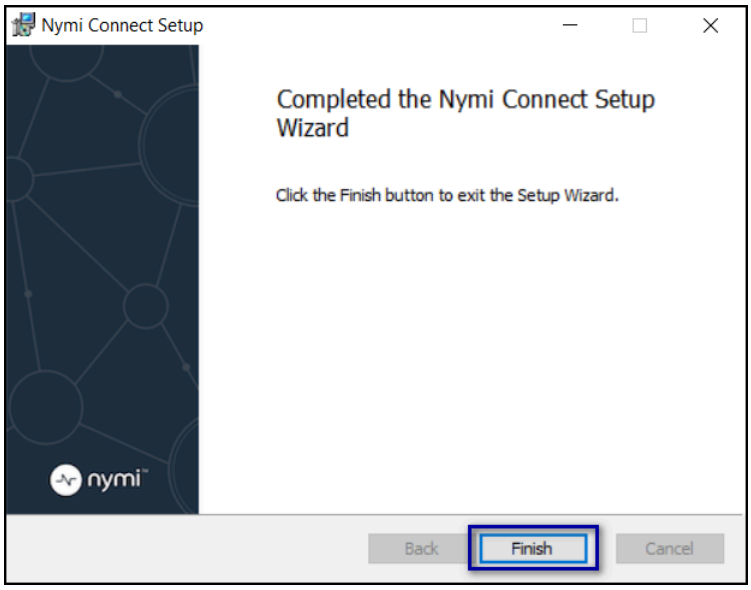
6. On the `NES URL` window, review the setting and then click **`Next`**.



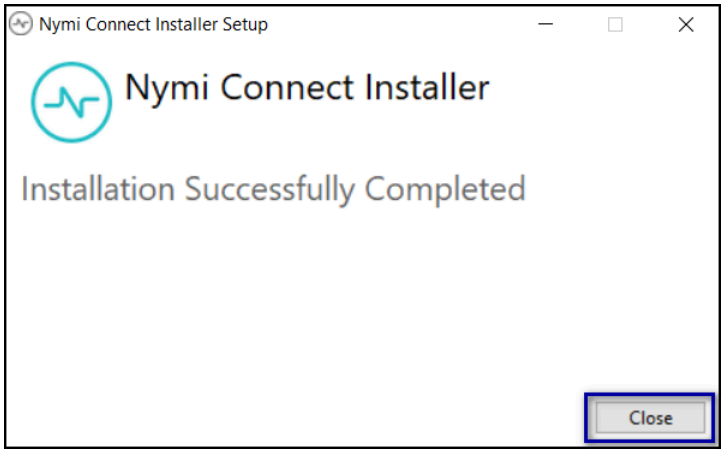
7. On the `Ready to install Nymi Connect` window, click **`Install`**.



8. On the `Completed the Nymi Connect Setup Wizard` window, click **`Finish`**.



9. On the `Installation Successfully Completed` window, click **`Close`**.



Installing Nymi Connect Silently

About this task

Perform the following steps on each user terminal.

Procedure

1. Run a Command Prompt as administrator.
2. Type the following command: ***"Nymi Connect Installer-vversion.exe" /exenoui /q***
   For example, ***"Nymi Connect Installer-v1.0.0.0.exe" /exenoui /q***

What to do next

If you use management software to push the Nymi Connect installation to user terminals or you run the installer as an administrator, you will need to restart the user terminal to ensure that all components initialize correctly and the Nymi Connect application runs under the user context.

Configuring Nymi Connect

Configure Nymi Connect to access you POMSnet server.

About this task

After you install Nymi Connect and hover over the Desktop System Tray icon, the status of Nymi Connect appears as *Nymi Connect - App Setting file is invalid.*

Procedure

1. Open a web browser and navigate to your POMSnet server.
2. Edit the *C:\Nymi\Nymi Connect\appsettings.json* file with an application such as Notepad++ in administrator mode, and the perform the following actions:
   a) In the *applicationHostName* parameter, specify the URL to your POMSnet server in between the quotes.

      For example, the parameter definition appears as follows:

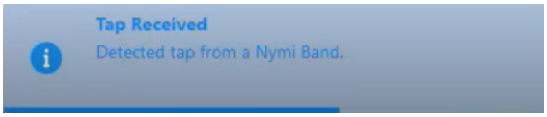
      "applicationHostName": "https://poms.nymi.com",
3. Save the file.
4. Right-click the *Nymi Connect* desktop system tray icon, and then click **`Restart`**.

Using Nymi Connect

The following work flow describes the use case where a user uses their Nymi Band to complete authentication tasks in a login or e-signature window.

1. Nymi Connect appears in the system tray. The follow table displays the icon that can appear.

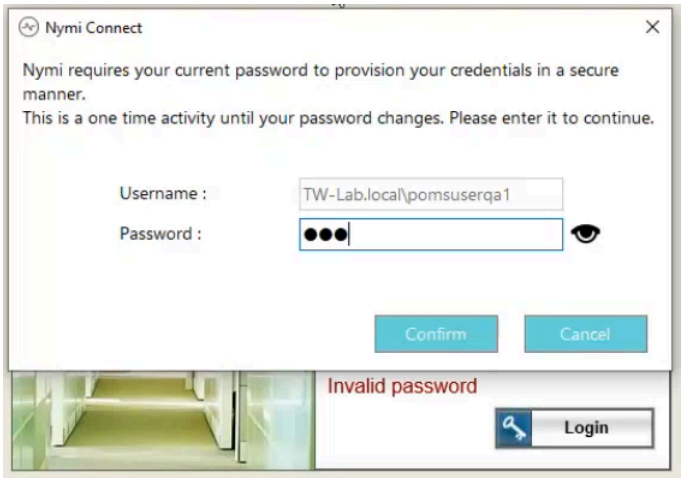
	When Nymi Connect successfully established a connection with all the required components. When you hover over the icon, the message pop-up displays *Nymi Connect*.
	When Nymi Connect cannot establish a connection with one or more required components. Hover over the icon to display the error message. *Troubleshooting Nymi Connect Status Messages* provides more information.

   Note: Upon start-up, Nymi Connect initializes components and establishes a connection to the Nymi Agent. When you hover over the Nymi Connect Desktop System Tray icon, the status appears as *Nymi Connect - initializing*. If a user performs a Nymi Band tap in Nymi Connect immediately after installation or a restart, Nymi Connect might not detect the tap until initialization completes.
2. User starts the Nymi-Enabled Application(NEA) and navigates to a screen that requires their user credentials.
3. User performs a left mouse click on the **`Username`** field.
4. User performs an NFC Tap or BLE Tap with their authenticated Nymi Band. A messages appears above the Desktop system tray that displays Tap Received - Detected tap from a Nymi Band, as shown in the following figure. 

5. Nymi Connect verifies the configuration and criteria settings in the JSON file match the application that is in focus.
   - When the verification succeeds, Nymi Connect retrieves the credentials of the Nymi Band user and populates the values in the credentials window, and then completes the login or e-signature.
   - When verification fails, a pop-up appears that displays an error message. *Troubleshooting Nymi Connect Usage Errors* provides more information.
6. When verification succeeds, the NEA authenticates the user credentials and completes the authentication or rejects the authentication.

Managing Password Changes

When a user password changes, the first time the user performs a Nymi Band tap to complete an authentication task, the authentication task fails with the error, and Nymi Connect displays a window that prompts the user to manually type their new password once.



After the user clicks **`Confirm`**, ensure that the cursor is in the **`Username`** field and instruct the user can perform another Nymi Band tap.

Performing Tasks that Require Two E-Signatures

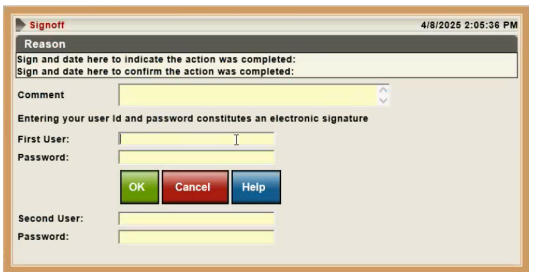
Some tasks require a sign off from two different users.

About this task

Procedure

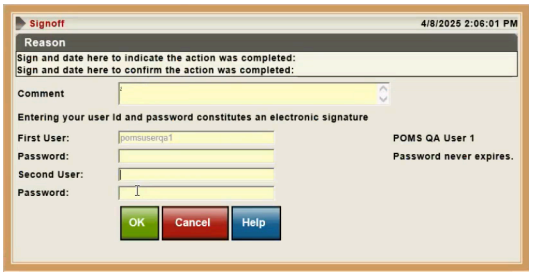
1. Perform an operation that requires two e-signatures.
2. Left-mouse click in the **`First user`** username field.

   The following figure provides an example of a dual e-signature window where the cursor is active in the first username field.



3. Instruct the first user to perform a Nymi Band tap with their authenticated Nymi Band.
   The Nymi Connect injects the username and password of the user into the first set of credential fields, and clicks **OK**.
4. Left-mouse click in the **`First user`** username field.

   The following figure provides an example of a dual e-signature window where the cursor is active in the second username field.



5. Instruct the second user to perform a Nymi Band tap with their authenticated Nymi Band.
   The Nymi Connect injects the username and password of the user into the second set of credential fields, clicks **OK**, and the window closes.

Log Files

Nymi Connect stores audit and application log files in the *C:\Users\username\AppData\Roaming\Nymi\Nymi Connect* folder.

The following table summarizes the available log files and the content of each log file:

Log file	Location	Purpose
Application Log files	*%AppData%\Nymi\Nymi Connect\Logs\App*	Contains information that is related to general application behavior and operational activities. These logs provide insights into normal functions, process flow, and application events and can assist you in troubleshooting issues.
Audit log files	*%AppData%\Nymi\Nymi Connect\Logs\Audit*	Contains information about critical user events, which Nymi Connect records on a daily basis. Events include: • Injection Started—Indicates the start of the credential injection process. • Injection Failed—Indicates a failure in the credential injection process and includes the reasons if the reasons are identifiable. For example, network issues. • Failure Reasons—Provides information about why a credential injection attempt failed. • Target Application—Indicates the specific application that was in use for each injection attempt.
Profile	*%AppData%\Nymi\Nymi Connect\Logs\Profiles*	Contains performance information that identifies the length of time each function spends to complete any operation.

Log file	Location	Purpose
Nymi API Log File	*%AppData%\Nymi\Nymi Connect\Logs\nymi_api.log*	Contains API-specific errors that can occur when the user starts Nymi Connect or perform a Nymi Band tap.

To save log files in a single file that you can send to Nymi Support, perform the following actions:

1. Right-click the Nymi Connect Desktop System Tray icon, and then select **`Export Logs`**.
2. In the `Save Logs` window, type a name for the *ZIP* file, and then click **`Save`**. The default location for the files is the *Documents* directory of the currently logged on user.

Troubleshooting Nymi Connect Usage Errors

This section provides information about how to troubleshoot and resolve error messages that can appear when you use Nymi Connect and the Nymi Band to complete authentication tasks.

Nymi Connect Does Not Start

When a user manually restarts the Nymi Connect service or after a reboot, the Nymi Connect application does not appear in the Desktop System Tray.

The following error message appears in the *C:\Users\username\AppData\Roaming\Nymi\Nymi Connect\App\log\ncw_date.log* file.

```
An error has occured.  Failed to load the configuration file from C:\Nymi\NymiConnect\appsettings.json
```

Cause

There is a configuration error in the *appsettings.json*.

Resolution

Correct the *appsettings.json*, and then start Nymi Connect service again.

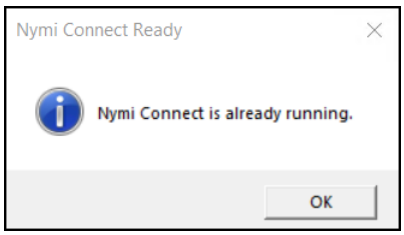
Common configuration considerations include:

- Start each commented line with //
- Each uncommented line should end with a comma (,) except for the last line before a closing }

Nymi Connect is already running

This error message appears when a user starts Nymi Connect.

The following image displays the error message.



Cause

Only one instance of Nymi Connect can run on a user terminal.

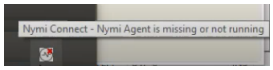
Resolution

Click **OK**. Before attempting to start Nymi Connect, view the System Tray and confirm that Nymi Connect is not already started.

Nymi Connect Agent is missing

This error message appears when a user starts Nymi Connect.

The following image displays the error message.



Cause 1

Nymi Connect cannot connect to the centralized Nymi Agent server.

Resolution 1

To resolve this issue, perform the following actions:

1. Confirm that the status of the Nymi Agent service is **Running** on the centralized Nymi Agent server. If you start the Nymi Agent service, on the user terminal, right click the Nymi Connect icon and select **`Restart`**.
2. On the user terminal, edit the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file and ensure that the *AGENT_URL* parameter correctly defines the Nymi Agent server.

   Note: If you update the *nbe.toml* file, restart the Nymi Bluetooth Endpoint service.

Cause 2

In a decentralized Nymi Agent configuration, the Nymi Agent service is not running.

Resolution 2

To resolve this issue, and start the Nymi Agent service on the user terminal.

Cause 3

The Nymi Runtime software was not installed on the user terminal.

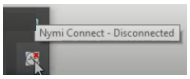
Resolution 3

Install the Nymi Runtime software on the user terminal. For a decentralized Nymi Agent configuration, after installation, configure the *nbe.toml* file.

Nymi Connect - Disconnected

This error message appears when a user hovers over the Nymi Connect Desktop System Tray icon.

The following image displays the error message.



The Nymi Connect log file (*NC_date.log*) in *%AppData%\Nymi\Nymi Connect\Logs\App* folder displays the following error:

```
ERROR Token retrieval failed: Nymi Connect - Disconnected
```

Cause

Nymi Connect cannot communicate with the Nymi Enterprise Server(NES).

Resolution

Resolve connectivity issues, right-click the Nymi Connect Desktop System Tray icon, and then click **`Restart`**.

Nymi Connect Does not Detect Nymi Band Tap

A user performs a Nymi Band tap in the username and password window, but Nymi Connect does not detect the tap operation.

Situation 1

The Nymi Connect log file (*nc_data.log*) in *%AppData%\Nymi\Nymi Connect\Logs\App* directory displays the following error messages:

```
Band service disconnected, error code: 4000
```

Cause 1

The *AgentURL* registry key is not correctly configured.

Resolution 1

To resolve this issue, perform the following actions on the user terminal:

1. Run *regedit.exe*.
2. Navigate to **`HKLM > Software > Nymi > NES`**.
3. Confirm that the *AgentURL* registry key is defined for the centralized Nymi Agent server.
4. Click **`OK`**.
5. Restart the Nymi Connect process, by right-clicking the **`Nymi Connect`** icon on the system tray and selecting **`Restart`**.

Situation 2

The Nymi Connect log file (*nc_date.log*) in *%AppData%\Nymi\Nymi Connect\Logs\App* directory does not display messages related to the failed Nymi Band tap but the *%AppData%\Nymi\Nymi Connect\nymi_api.log* file reports the following error messages:

```
NES query responded with status 404 not found
        NES query failed:  The requested query was not found on the NES server
```

Cause 2

This error can appear because the Nymi Band that the user uses to perform the Nymi Band tap is not identified as their active Nymi Band in the NES database. This can occur for the following reasons:

- NES supports self re-enrollment and the user has performed an enrollment on another Nymi Band, which is their active Nymi Band.
- A CWP Administrator has disconnected the Nymi Band to user association but the user has not performed the delete user data operation and performed a new enrollment.
- The user completed their enrollment on a different NES server.

Resolution 2

Perform one of the following actions:

- Instruct the user to re-enroll the Nymi Band. If NES does not support self service re-enrollment, disassociate the Nymi Band from the user in the NES Administrator Console.
- Instruct the user to use their new active Nymi Band and perform a delete user data operation on the inactive NES.

Credentials for your Nymi Band have not been found

This error message appears when a user performs a Nymi Band tap in the Nymi Connect username and password window.

The following image displays the error message.

Cause

At the time that the user enrolled their Nymi Band, the Lock Control settings was not enabled in the Nymi Enterprise Server(NES) policy.

Resolution

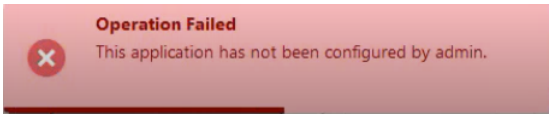
To resolve this issue, perform the following actions:

1. Log into the NES Administrator Console, and click **`Policies`**.
2. Edit the active policy, and then ensure that **`Enable Lock Control`** is selected.
3. If you enabled Lock Control, click **`Save`**.
4. From the menu, click **`Search`**.
5. In the **`Search`** field, type the name of the user.
6. In the `Nymi Bands` section, click the link for the active Nymi Band.
7. On the `Nymi Band Properties` page, observe that the **`Encrypted Password`** value is undefined.
8. Instruct the user to log in to the Nymi Band Application while they wear their authenticated Nymi Band and allow the application to apply settings.
9. `Nymi Band Properties` page, observe that the**`Encrypted Password`** value is Stored.
10. Close the NES Administrator Console and then instruct the user to perform the Nymi Band tap again.

This application has not been configured by admin

This error message appears when a user performs a Nymi Band tap in the Nymi Connect username and password window.

The following image displays the error message.



Cause 1

The application that is active at the time that the user performs the Nymi Band tap is not supported.

Resolution 1

Before you perform the Nymi Band tap, ensure that the browser window that is connected to the POMSnet server is the active window.

Cause 2

The *appsettings.json* file defines a value for the *ProcessName* or *windowsTitle* parameter, but does not define the *applicationHostName* parameter.

Resolution 1

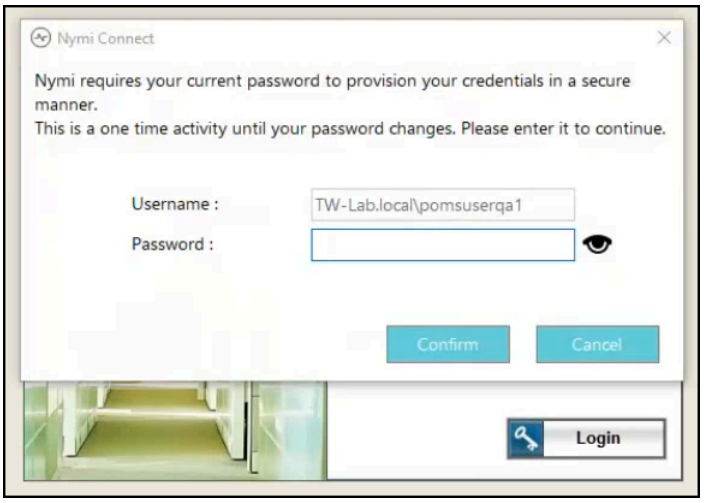
To resolve this issue, perform the following actions:

- Edit the *C:\Nymi\NymiConnect\appsettings.json* and specify the POMSnet URL for the *applicationHostName* value.
- Right-click the Nymi Connect application in the Desktop System Tray, and the select **`Restart`**.
- Perform the Nymi Band tap again.

Nymi Band Tap in a Nymi Connect-Enabled Application Prompts for Password

When a user performs a Nymi Band tap to complete an authentication task, the credentials are not injected. A pop-up window appears that prompts the user to type their password .

The following image displays the error message.



Cause 1

The user enrolled their Nymi Band at a time when the Lock Control option was not enabled in the active Nymi Enterprise Server(NES) policy.

Resolution 1

To resolve this issue, perform the following actions:

1. In the **`Password`** field of the pop-up window, type the password, and then click **`Confirm`**.
2. In the `Login` window with the cursor in the **`Username`** field, perform a Nymi Band tap.

Cause 2

The user removed the Nymi Band immediately after the Nymi Band tap and before Nymi Connect completed the verification of the user.

The *%appdata%\Nymi\NymiConnect\Logs\App\NC_date.log* file reports the following errors:

```
Failed to decrypt using symmetric key. Exception: Band error 3010:
Operation interrupted.
```

Resolution 2

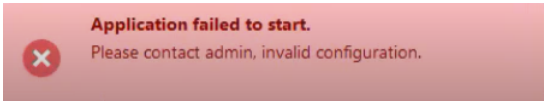
To resolve this issue, perform the following actions:

1. Instruct the user to click **`Cancel`**.
2. Instruct the user to authenticate to their Nymi Band.
3. With the cursor in the **`Username`** field, perform a Nymi Band tap.

Please Contact Admin, Invalid Configuration

This error message appears when a user attempts to start or restart the Nymi Connect application.

The following image displays the error message.



When the user hovers over the Nymi Connect application in the Desktop System Tray, the following message appears:

```
Nymi Connect - App setting file is missing
```

The following error message appears in the *C:\Users\username\AppData\Roaming\Nymi\Nymi Connect\App\log\ncw_date.log* file.

```
ERROR:  Application configuration file not found.
```

Cause

The *C:\Nymi\Nymi Connect* folder does not contain the *appsettings.json* file.

Resolution

Restore the file from backup.

User credential validation interrupted due to user cancellation or timeout

This error message appears when a user performs an activity in the application that displays in the Nymi Connect username and password window.

The following image displays the error message.

Cause

The user pressed a key on the keyboard or the user does not tap their Nymi Band within the tap detection expiration period.

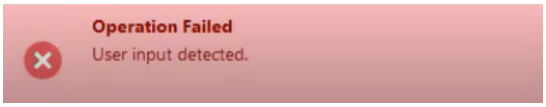
Resolution

To resolve this issue, instruct the user to click **OK** and with the cursor in the **Username** field, perform a Nymi Band tap.

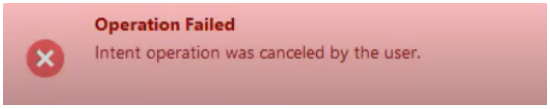
User Input Detected

This error message appears above the Desktop System Tray after a user performs a Nymi Band tap in the username and password window.

The following image displays the error message.



Additionally, the message Operation Failed - Intent operation cancelled by user appears above the Desktop System Tray, as shown in the following figure.



Cause

The user pressed a key on the keyboard while Nymi Connect was processing the Nymi Band tap. or the user does not tap their Nymi Band within the tap detection expiration period.

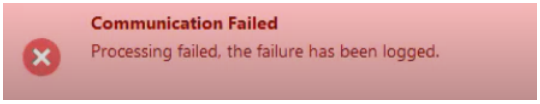
Resolution

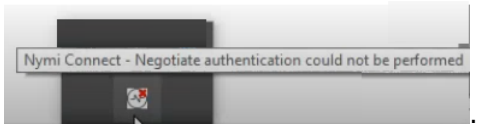
To resolve this issue, instruct the user to click **OK** and perform the Nymi Band.

Nymi Connect - Negotiate Authenication Could Not Be Performed

This error message appears above the Desktop System Tray after the user starts Nymi Connect.

The following image displays the error message.



The error message Nymi Connect - Negotiate Authentication could not be performed appears when you hover over the Nymi Connect Desktop System Tray icon, as shown in the following error. 

The following error message appears in the *C:\Users\username\AppData\Roaming\Nymi\Nymi Connect\App\log\ncw_date.log* file.

```
Token retrieval failed: Nymi Connect - Negotiate Authentication could not be performed
```

Cause 1

The root certificate is missing on the user terminal.

Resolution 1

To resolve this issue, perform the following actions:

1. Import the Root CA certificate on the user terminal.
2. Restart Nymi Connect.

Cause 2

Expired TLS certificate on the Nymi Enterprise Server(NES) server or IIS configuration issues.

Resolution 2

- Confirm the expiration date of the TLS certificate and replace as required. The *Nymi Connected Worker Platform—Troubleshooting Guide* provides more information.
- Review the IIS configuration. The *Nymi Connected Worker Platform—Deployment Guide* provides more information.
- Restart Nymi Connect.

Cause 3

Connectivity issues with NES.

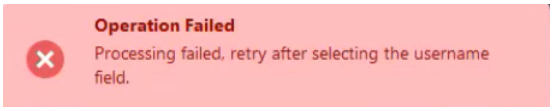
Resolution 3

Resolve connectivity issues.

Operation Failed - Processing failed, retry after selecting the username field

This error message appears above the desktop system tray when a user performs a Nymi Band tap in a username and password window.

The following image provides an example of the error message.



Cause

The user tapped their Nymi Band when the cursor focus was not in the **`Username`** field. For example, the cursor was in the **`Password`** field.

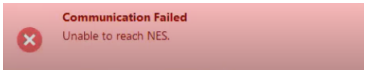
Resolution

To resolve this issue, instruct the user to click their mouse in the **`username`** field, and then perform the Nymi Band tap.

Communication Failed - Unable to reach NES

This error message appears when a user starts Nymi Connect.

The following image displays the error message.



Cause

Nymi Connect cannot connect to the Nymi Enterprise Server(NES)

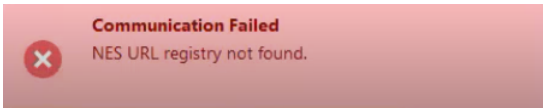
Resolution

Resolve connectivity issues.

Communication Failed - NES URL Registry Not Found

This error message appears when a user starts Nymi Connect.

The following image displays the error message.



Cause

The URL Registry key is not defined on the user terminal.

Resolution

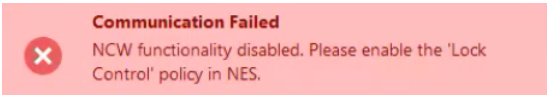
To resolve this issue, perform the following steps on the user terminal.

1. Run *regedit.exe*.
2. Confirm that the *URL* registry key is defined in **`HKLM > Software > Nymi > NES`**.

NCW functionality disabled. Please enable the 'Lock Control' policy in NES

This error message appears when a user starts Nymi Connect.

The following image displays the error message.



Cause

The active NES policy does not allow the use of the Lock Control feature.

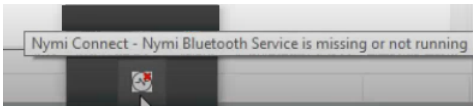
Resolution

To resolve this issue, in the NES Administrator Console, edit the active policy. In the **`Lock Control`** section, select the **`Enable Nymi Lock Control`** option.

Nymi Connect - Nymi Bluetooth Service is Missing or Not Running

This error message appears when a user starts Nymi Connect.

The following image displays the error message.



Cause

The state of the Nymi Bluetooth Endpoint service is not Running or the Bluetooth adapter is missing.

Resolution

To resolve this issue, perform the following steps on the user terminal.

1. In the `Services` applet, start the **`Nymi Bluetooth Endpoint`** service. If the service does not appear, Start Nymi Runtime installer and choose to install the Nymi Bluetooth Endpoint component only.
2. Plug a Nymi-provided Bluetooth Adapter into a USB port on the user terminal.

An Error Occurred Getting User Information

This error message appears when a user performs a Nymi Band tap to complete an e-signature in POMSnet.

The following image displays the error message.

Additionally, the contents of the **`Comments`** field are replaced with the username of the Nymi Band user.

Cause

The user perform the Nymi Band tap when the cursor focus is in the **`Comments`** field.

Resolution

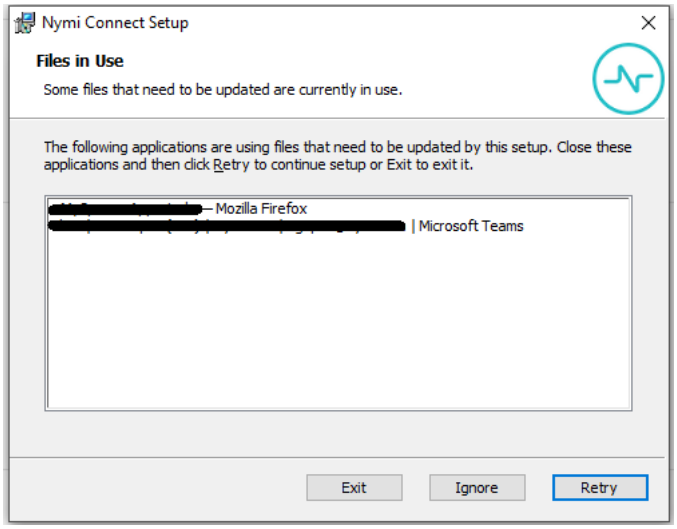
To resolve this issue, perform the following actions.

1. In the **`Comments`** field, re-enter the comment text.
2. Left mouse click in the **`Username`** field.
3. With the cursor in the **`Username`** field, perform a Nymi Band tap.

Nymi Connect Uninstall Reports Files in Use

This error message appears when a user uninstalls the Nymi Connect software.

The following image displays the error message.



Cause

The Nymi Connect application is running in the background.

Resolution

To resolve this issue, click **`Ignore`**.

The section *Uninstalling Nymi Connect* provides more information about how to uninstall the Nymi Connect software.

Nymi Band Injects Old Password

This issue appears the first time a user performs a Nymi Band tap after a password change. When the user taps, Nymi Connect injects the old password into the password field, and then prompts the user to provide the new password.

Cause

By default, Nymi Connect injects cached the username and password into the credentials fields first, and then validates that the cached credentials match the credentials that are stored in Nymi Enterprise Server(NES).

Resolution

To prevent Nymi Connect from injecting the old password before validating the credentials in NES, perform the following steps to change the default behaviour and to force Nymi Connect to validate the user credentials before injecting the username and password into the credential fields.

1. Edit the *C:\Nymi\NymiConnect\appsettings.json* file as an administrator.
2. Change the value in for the *executionOrder* parameter from **`InjectFirst`** to **`ValidationFirst`**
3. Save the file.
4. Right-click the Nymi Connect Desktop System Tray icon, and then click **`Restart`**.
5. Perform the Nymi Band tap on the authentication window. Nymi Connect does not inject the credentials into the credential window and prompts the user to type their new password.

Nymi Connect Prompts for Password

A user updates their password in AD, but when they perform a Nymi Band tap, Nymi Connect injects the old password, and then displays a prompt for the user to type their new password. After they type their new password, the authentication task completes.

Cause

By default, Nymi Connect uses cached credentials to complete authentication tasks. Nymi Connect will continue to inject the cached credentials until the cache expires. By default, the cached values remain valid for 15 minutes. When the cache expires and the Nymi Band user performs a tap, Nymi Connect prompts the user to provide their new password, and then updates the cache.

Credentials caching improves Nymi Band tap performance by avoiding repeated calls to retrieve Nymi Band details from NES.

Resolution

To resolve this issue, after a user changes their password, restart Nymi Connect, which forces Nymi Connect to refresh the cache.

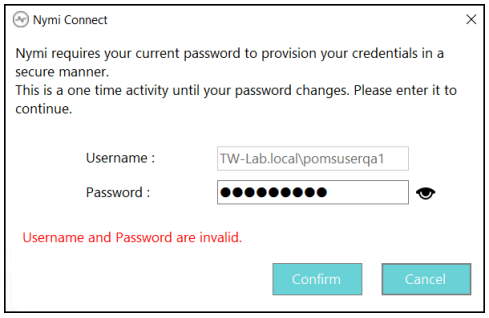
To decrease the cache expiration time, perform the following steps:

1. Edit the *C:\Nymi\NymiConnect\appsettings.json* file as an administrator.
2. Change the value in for the *cacheExpiration* parameter from fifteen minutes (**`00:15:00`**) to a lower value, such as 2 (**`00:02:00`**) or 3 minutes (**`00:03:00`**) .
3. Save the file.
4. Right-click the Nymi Connect Desktop System Tray icon, and then click **`Restart`**.

Username and Password are Invalid

This message appears on the Nymi Connect password prompt window after a user types types their username and password, and then click **`Confirm`**.

The following figure shows the error.



Cause

This error can appear for several reasons:

- Password is not correct or has expired
- User account is disabled or locked in Active Directory.

Resolution

To resolve this issue, review the user account in AD and make changes as required. If the password has expired, instruct the user to update their password and then specify the new password in the Nymi Connect prompt.

Note: The user might see the prompt on subsequent Nymi Band taps until the cached credentials expire. By default, cached credentials expire every 15 minutes. When the user provides their new password at the prompt and the cache has expired, Nymi Connect updates the cache with the new password, and subsequent Nymi Band taps do not prompt the user for the new password.

Uninstalling Nymi Connect

Perform the following actions to remove the Nymi Connect application.

Procedure

1. From `Add or Remove Programs`, select **`Nymi Connect Installer`**, and then click **`Uninstall`**.
2. When prompted, click **`Uninstall`**.
3. On the `Modify Setup` window, click **`Uninstall`**.
4. On the `User Account Control` window, click **`Yes`**.
5. On the **`Uninstall Successfully Completed`** window, click **`Close`**.

Appendix A—Install and Configure Nymi Components in a Decentralized Nymi Agent Configuration

Review this section for information about how to deploy the solution with a decentralized Nymi Agent.

In this configuration, you install the following components:

- Nymi Band Application and the Nymi Runtime software on a thick client enrollment terminal.
- Nymi Runtime application on each thick client user terminal.

Components in a Local Nymi Agent Configuration

The following figure provides a high-level overview of the Connected Worker Platform solution that uses a local Nymi Agent and the TCP ports that are used between the components for communication.

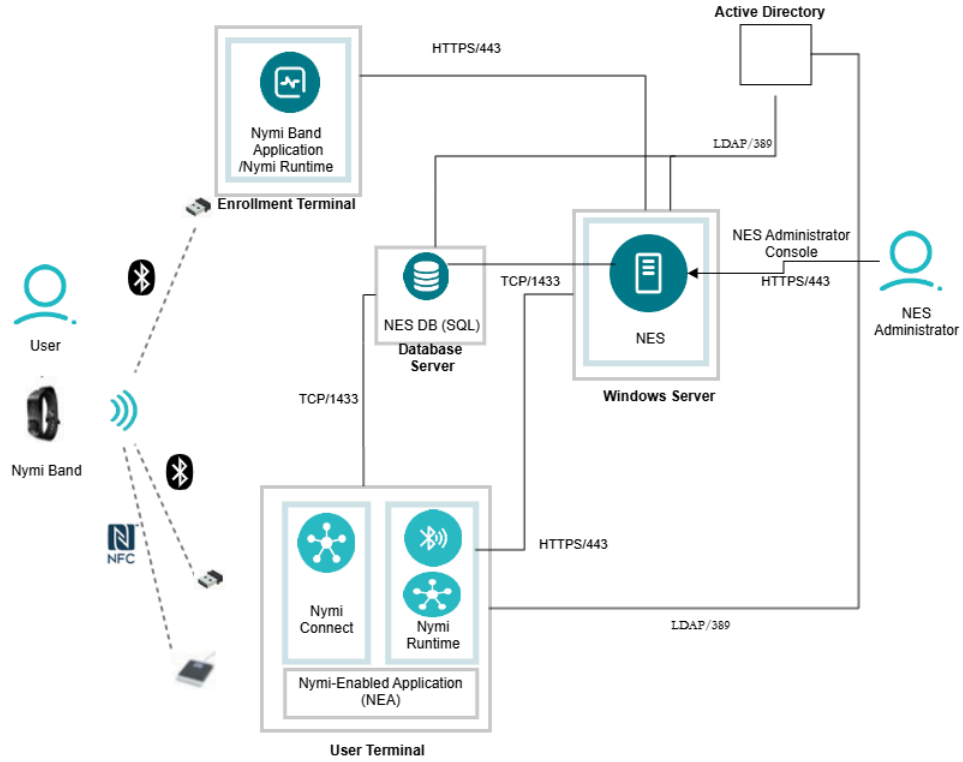


Figure 29: Connected Worker Platform with Nymi Connect components and connection ports

The Connected Worker Platform consists of the following components.

Table 4: Connected Worker Platform Components

Component	Description
Enrollment Terminal	Windows 10 or Windows 11 endpoint that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal that you use to enroll a new user and link them to their Nymi Band. The Nymi Band Application requires the Nymi Runtime application, which the Nymi Band Application automatically installs. The Nymi Band Application communicates with the Nymi Band through the Nymi-supplied Bluetooth adapter, which you plug into a USB port on the enrollment terminal.
User Terminal	Windows 10 or Windows 11 endpoint on which you install Nymi components that allow users to perform authentication tasks with a Nymi Band tap on the NFC reader or Bluetooth Adapter.

Component	Description
Nymi Band	A wearable device that is associated with the biometrics of a single user. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled.
NES	Windows-based management server and collection of services that administrators access through a web-based application. NES coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates.
NES Administrator Console	A web application that provides NES Administrator with an interface to manage the NES configuration and users.
Domain Controller (DC)	Windows server with Active Directory.
Nymi Runtime	A Windows application that you install on the enrollment terminal and user terminals. Nymi Runtime includes the Nymi Agent and Nymi Bluetooth Endpoint components.

Firewall Port Requirements

The following tables summarizes the TCP port requirements for the Connected Worker Platform.

Component	Port Requirements
Enrollment Terminal	Port 389 to the Active Directory server for LDAP communication. Port 443 to the NES server for HTTPS communication.
User Terminal	Port 443 to the NES server for HTTPS communication.
NES server	Port 1443 to the SQL server.

Configuring the Required NES Policies Options

To allow the Nymi Connect application to store encrypted passwords, enable the Nymi Lock Control option in the active NES policy.

About this task

Before users enroll their Nymi Bands, perform the following tasks from a Web Browser to enable the Nymi Lock Control.

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. In the **`Lock Control`** section, select the **`Enable Nymi Lock Control`** option.
   The following figure provides an example of the Lock Control policy settings.

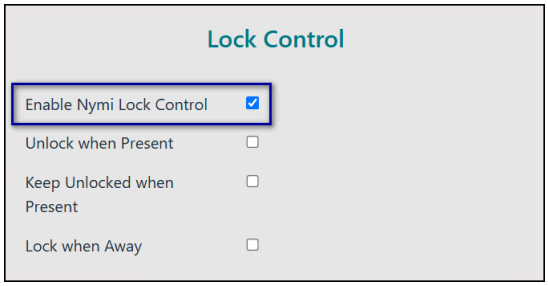


Figure 30: Enable Lock Control

Note: It is not necessary to select other Lock Control options.

5. Click **`Save`**.

Set Up Thick Client Enrollment Terminal

Install the Nymi Band Application, which also installs the Nymi Runtime software on a thick client.

Install the Nymi Band Application

Perform the following steps to install the Nymi Band Application on each enrollment terminal that you will use to enroll and authenticate users to their Nymi Bands.

You can perform a customizable installation or a silent installation.

Installing/Updating the Nymi Band Application

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Before you begin

For an update, uninstall the previous version of Nymi Runtime.

Procedure

1. Download the Nymi Band Application package.
2. Double-click the *Nymi-Band-App-installer-v_`version`.exe* file.
3. On the `User Account Control` window, click **`Yes`**.

4. On the `Prerequisites` window, click **`Next`**.
5. On the `Welcome` page, click **`Install`**.
6. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
7. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
8. On the `Nymi Runtime Setup` window, click **`Next`**.
9. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
   - Accept the default service account NTAuthority\LocalService, click **`Next`**.
   - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.

   Note: The service account must have permission to run as a service. Enable Service Log On provides more information about how to modify the local policy to enable this permission for the service account.

   The following figure shows the `Service Account` window.

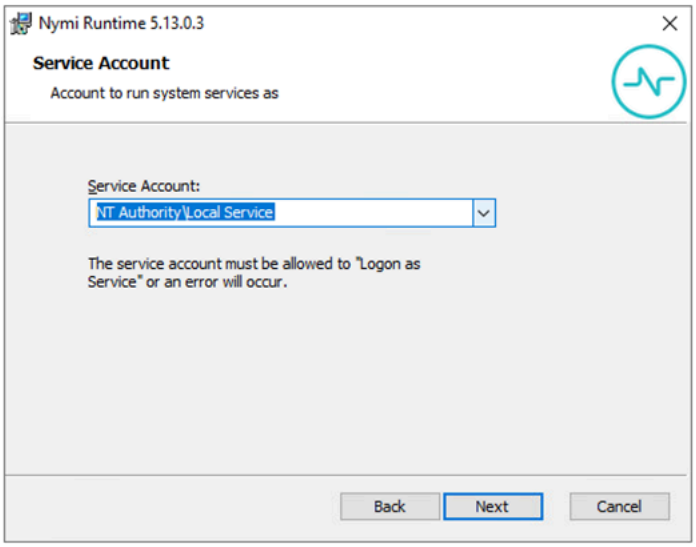


Figure 31: Nymi Runtime Service Account window

10. On the `(Optional) Nymi Infrastructure Service Account`, click **`Next`**.
    Only deployments that use web-based Nymi-enabled Applications(NEAs) with a centralized Nymi Agent require you to configure the Nymi Infrastructure Service Account.
11. On the `Ready to install` page, click **`Install`**.
12. Click **`Finish`**.
13. On the `Installation Completed Successfully` page, click **`Close`**.
14. On the `Welcome to Nymi Band Application Setup Wizard` window, click **`Next`**.
15. On the `Select Installation Folder` window, click **`Next`** to accept the default installation location.

16. In the `Ready to Install` window, click **`Install`**.
17. On the `Completing the Nymi Band Application Setup Wizard` window, click **`Finish`**.

What to do next

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

Installing the Nymi Band Application Silently

Perform the following steps to install or update the Nymi Band Application silently, for example, when you want to install the software remotely by using a software distribution application.

Before you begin

Before you install the Nymi Band Application, install the Nymi Runtime

Procedure

1. Save the Nymi Band Application package, provided to you by your Nymi Solution Consultant.
2. Launch the command prompt as administrator.
3. From the folder that contains the Nymi Band Application, type *Nymi-Band-App-installer-v_`version`.exe /exenoui /q*

   Where you replace *`version`* with the version of the Nymi installation file.

   The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, the Nymi Band Application and Nymi Runtime applications appear in the `Program and Features` applet.

   Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

Configuring the Nymi Enterprise Server URL

After you install the Nymi Band Application, perform the following steps to ensure that the enrollment process connect to the correct Nymi Enterprise Server(NES).

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software > Nymi`**.

   Note: If you installed the Nymi Band Application on a Citrix server, navigate to HKEY_CURRENT_USER instead of HKEY_LOCAL_MACHINE.
4. Right-click **`Nymi`**, and then select **`New > Key`**. Name the key **`NES`**.
5. Right-click **`NES`**, and then select **`New > String value`**.
6. In the **`Value`** field, type ***`URL`***.

7. Double-click **URL** and in the **Value Data** field, type ***https://nes_server/NES_service_name/*** or ***http://nes_server/NES_service_name*** depending on the NES configuration

   where:

   - *nes_server* is the FQDN of the NES host. The FQDN consists of the ***hostname.domain_name***. You can also find the FQDN by going to the server on which you deployed NES viewing the properties of the computer. The *nes_server* is the value that appears in the **Full computer name** field.
   - *NES_service_name* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
8. Click **OK**.

(Optional) Configuring the Communication Protocol

If you use the enrollment terminal to also access NEAs, perform the following steps to disable the legacy protocol.

About this task

Note: After you set this environment variable, user terminals cannot communicate with Nymi Bands that use pre-CWP 1.15.x firmware

Procedure

1. In the Windows search field, type ***env***, and then from the pop-up menu, select **Edit the System Environment Variables**.
2. Click **Environment Variables**.
3. In the **System Variables** section, click **New**, and the perform the following actions:
   a) In the **Variable Name** field, type *NYMI_NEA_SUPPORT_LEGACY_MODE*
   b) In the **Variable Value** field, type ***0***.

      The following figure provides an example of the new variable.

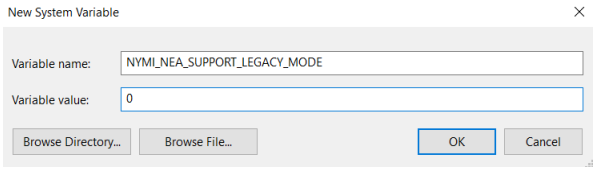


Figure 32: New System Variable window

   c) Click **OK**.

Set Up Thick Client User Terminals

You can use the Nymi Band to perform daily authentication tasks that would normally require a username and password in an MES application that reside on VMware Horizon thin clients a remote session host .

- Import the Root CA certificate for NES (when the Root CA that issued the certificate is not a trusted CA).

  Apple recommends deploying certificates with a Mobile Device Management (MDM) system. Certificate payloads are automatically trusted for SSL when installed with Configurator, MDM, or as part of an MDM enrollment profile.

  Apple Support provides more information.

  Note: If you manually import a device profile, you must enable trust for SSL/TLS. Apple Support provides more information.
- Install the Nymi Bluetooth Endpoint service.
- Insert the Nymi-supplied Bluetooth adapter into an available USB port.
- Optionally, insert a Nymi-verified NFC reader into an available USB port.

Bluetooth Adapter Placement

The enrollment terminal and each user terminal requires a Bluetooth adapter. The Bluetooth Low Energy (BLE) radio antenna in the Nymi-supplied BLED112 USB Adapter provides seamless Bluetooth capability between the Nymi Band and devices such as a laptop computer.

To ensure optimal system performance, place the Bluetooth adapter in a location that meets the following criteria:

- Is in clear line of sight to the Nymi Band.
- Is on the same side of the computer that you wear your Nymi Band.
- Is near the computer keyboard.

Note: The presence of liquids between the Nymi Band and Bluetooth adapter negatively affects the Bluetooth signal quality. This includes beverages and the human body. If Bluetooth (BLE) taps behave unexpectedly, consider another placement for the Bluetooth adapter, or edit the Nymi Bluetooth Endpoint configuration file to adjust the signal strength thresholds to perform a BLE tap.

Install the Nymi Runtime

Perform the following steps to install the Nymi Runtime on each enrollment terminal that you will use to enroll and authenticate users to their Nymi Bands.

You can perform a customizable installation or a silent installation.

Installing/Updating Nymi Runtime

Perform the following steps to install or update Nymi Runtime on a user terminal, on which you want to install a Nymi-enabled Application.

About this task

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the *..\nymi-sdk\windows\setup* folder, right-click the *Nymi Runtime Installer version.exe* file, and select **`Run as administrator`**.
4. On the `Welcome` page, click **`Install`**.
5. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
7. On the `Nymi Runtime Setup` page, click **`Next`**.
8. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
   - Accept the default service account NTAuthority\LocalService, click **`Next`**.
   - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.

   Note: The service account must have permission to run as a service. Enable Service Log On provides more information about how to modify the local policy to enable this permission for the service account.

   The following figure shows the `Service Account` window.

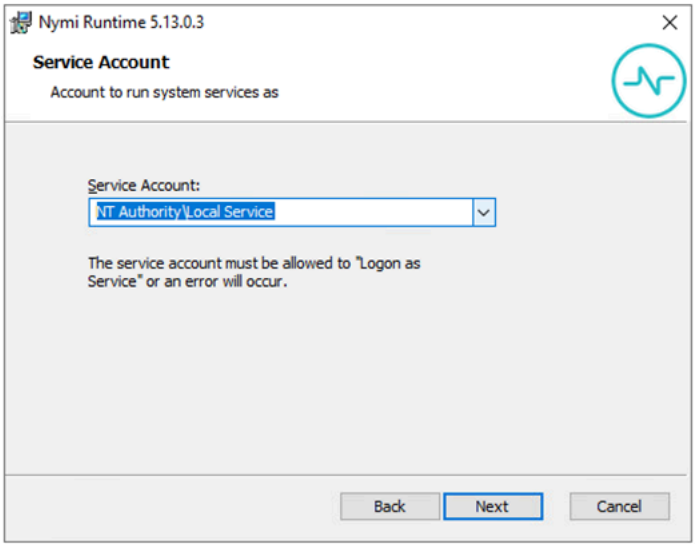


Figure 33: Nymi Runtime Service Account window

9. On the `(Optional) Nymi Infrastructure Service Account`, click **`Next`**.

   Only deployments that use web-based Nymi-enabled Applications(NEAs) with a centralized Nymi Agent require you to configure the Nymi Infrastructure Service Account.

10. On the `Ready to install` page, click **`Install`**.
11. Click **`Finish`**.
12. On the `Installation Completed Successfully` page, click **`Close`**.

What to do next

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

Installing the Nymi Runtime Silently

Perform the following steps to install or update the Nymi Runtime and the BLE adapter drivers silently, without user intervention.

Procedure

1. Log in to the network terminal with an account that has administrator privileges.
2. Download and extract the Nymi SDK package.
3. Launch the command prompt as administrator.
4. Change to the *..\nymi-sdk\windows\runtime* folder, and then type one of the following commands:

   - ```
     "Nymi Runtime Installer version.exe" /exenoui /q /log NymiRuntimeInstallation.log
     ```
   - For installations on non-English operating systems,

     ```
     "Nymi Runtime Installer version.exe" ServiceAccount="LocalSystem" /exenoui /q /log
     NymiRuntimeInstallation.log
     ```
     ```

Where you replace *version* with the version of the Nymi installation file.

Note: Ensure that you enclose the filename in double quotes.

The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, Nymi Runtime appears in the `Program and Features` applet and *NymiRuntimeInstallation.log* file contains information about the installation.

Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

What to do next

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

Configuring the Connected Worker Platform Communication Protocol

Starting with Connected Worker Platform(CWP) 1.15, the Nymi solution supports a new, high performance protocol over Bluetooth between the Nymi Runtime and Nymi Bands.

About this task

Perform the following steps on all user terminals (for Evidian environments on Wearable user terminals only) where users access Nymi-enabled Applications(NEAs) to disable the legacy protocol. The enrollment terminal only requires the environment variable if users access NEAs on the enrollment terminal.

Note: After you set this environment variable, user terminals cannot communicate with Nymi Bands that use pre-CWP 1.15.x firmware

Procedure

1. In the Windows search field, type ***env***, and then from the pop-up menu, select **`Edit the System Environment Variables`**.
2. Click **`Environment Variables`**.
3. In the **`System Variables`** section, click **`New`**, and the perform the following actions:
   a) In the **`Variable Name`** field, type *NYMI_NEA_SUPPORT_LEGACY_MODE*
   b) In the **`Variable Value`** field, type ***0***.
   The following figure provides an example of the new variable.

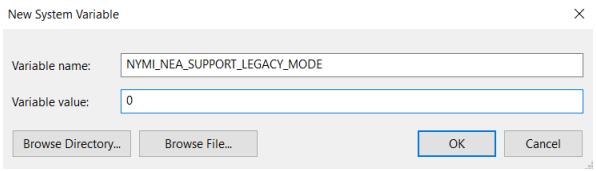


Figure 34: New System Variable window

   c) Click **OK**.

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