



# POMSnet Installation and Configuration Guide

**Nymi Connected Worker Platform**

**v4.0**

**2025-03-25**

# Contents

- Preface..... 3**
- Nymi-POMSnet Solution Overview..... 5**
  - Components in a Centralized Nymi Agent Configuration..... 5
- Use Cases..... 9**
- Install and Configure Nymi Components.....10**
  - NES Server Configuration..... 10
    - Configuring Check User Status..... 10
  - Set Up a Centralized Nymi Agent..... 11
    - Importing the Root CA certificate..... 12
    - Installing/Updating Centralized Nymi Agent.....14
    - Configuring the Nymi Agent For WSS..... 17
  - Set Up Enrollment Terminal..... 20
    - Set Up a Decentralized Enrollment Terminal..... 20
    - Set Up Centralized Enrollment..... 23
  - Set Up User Terminals.....30
    - Bluetooth Adapter Placement..... 30
    - Installing Nymi Bluetooth Endpoint.....30
    - Configuring the Nymi Enterprise Server URL.....33
    - Configuring the Connected Worker Platform Communication Protocol..... 33
- Configuring POMSnet..... 35**
- Using the Nymi Band with POMSnet..... 36**
- Troubleshooting POMSnet Issues.....38**
  - Disconnected from authentication service..... 38
  - Biometric authentication service is not configured to return user status..... 39

# 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.

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

## Audience

This guide provides information to NES and POMSnet Administrators. An NES and POMSnet Administrator is the person in the enterprise that manages the Connected Worker Platform with POMSnet 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	June 30, 2022	First release of this document.
2.0	March 6, 2023	Second release of this document. Updates include: <ul style="list-style-type: none"><li>• New <i>Use Cases</i> section</li><li>• Clarifications to the <i>Nymi Runtime Installation and Configuration</i> section.</li></ul>
3.0	January 15, 2024	Third release of this document to correct the Nymi Agent port from 9210 to 9120.
4.0	March 25, 2025	Fourth release of this document. Various updates to the <i>Overview</i> section.

### 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@nyimi.com](mailto:support@nyimi.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@nyimi.com](mailto:support@nyimi.com)

# Nymi-POMSnet Solution Overview

---

The Nymi-POMSnet Solution extends the use of the Nymi Band. The Nymi Band gives users passwordless access to POMSnet and the ability to apply their digital signature to process sign-offs.

## Components in a Centralized Nymi Agent Configuration

The following figure provides a high-level overview of the Nymi-POMSnet Solution with a centralized Nymi Agent, and the connection ports that are used between the components for communication.

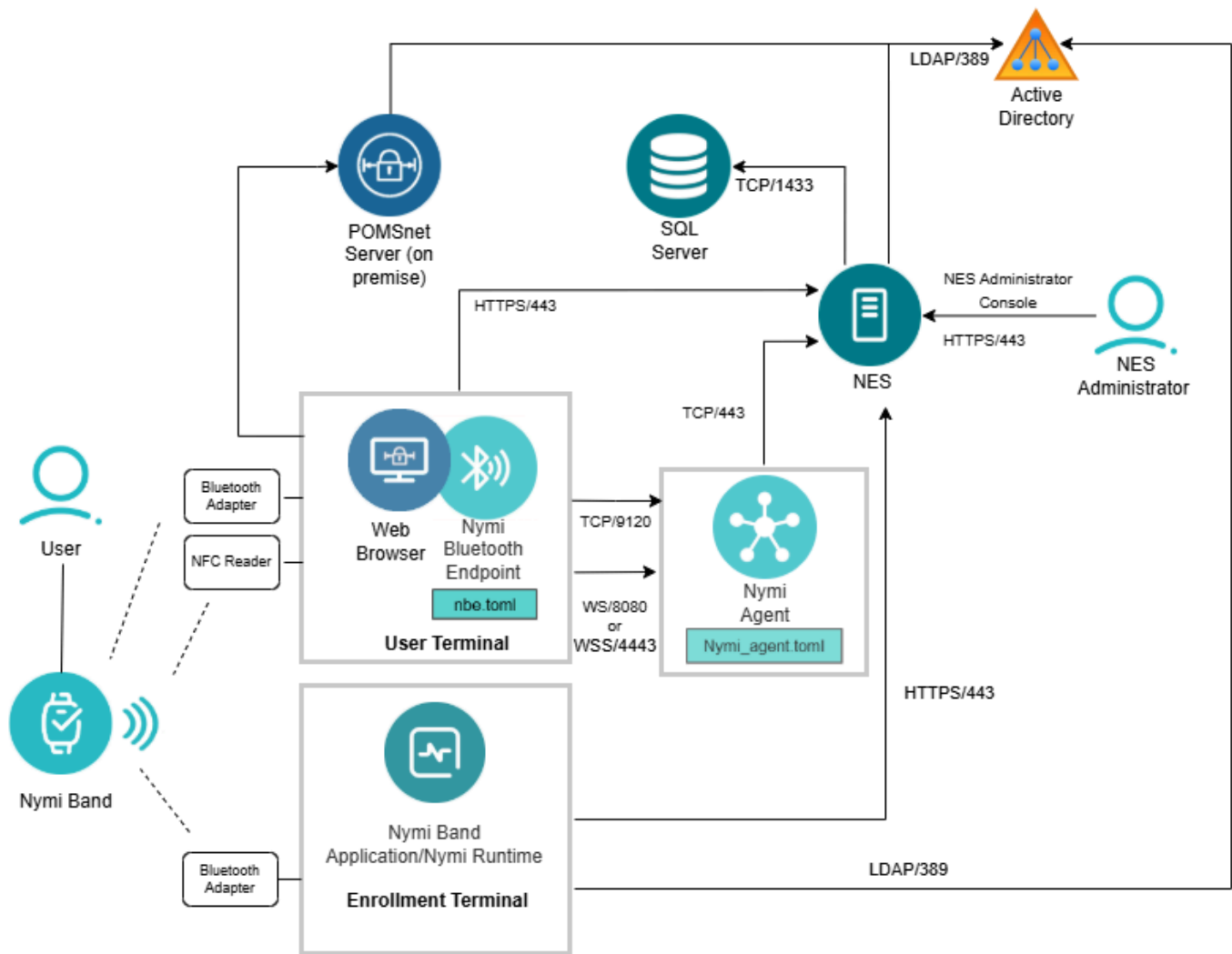


Figure 1: Nymi-POMSnet Solution in a Centralized Nymi Agent Configuration Overview

Table 2: Components in a Nymi-POMSnet Solution

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.

Component	Description
User Terminal	<p>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.</p> <p>Use a supported Web Browser to connect to the POMSnet interface. To support authentication operations with the Nymi Band, plug an NFC reader and Bluetooth adapter into available USB ports on the user terminal. Starting with POMSnet Aquila 2022.1.0, the Bluetooth adapter is optional.</p>
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 interface that provides NES Administrator the ability to manage the NES configuration and users.
Domain Controller (DC)	Windows server with Active Directory.
Nymi Agent	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.
Nymi Bluetooth Endpoint	A component of the Nymi Runtime that provides an interface between the Bluetooth Adapter (BLE) and the Nymi Agent. You deploy Nymi Bluetooth Endpoint 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.
<i>nbe.toml</i>	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.
<i>nyimi_agent.toml</i>	Configuration file that you create on the machines that run the Nymi Agent. This file defines the hostname of the NES server and the configuration parameters that support Nymi Band communications between the user terminals and the application server. If you do not use a centralized Nymi Agent, you must create this file on each user terminal.

Component	Description
POMSnet Server	A Nymi-Enabled Application(NEA) in which a user can perform authentication tasks with a Nymi Band tap.

### Firewall Port Requirements

The following tables summarizes the TCP port requirements for the Nymi-POMSnet Solution solution.

**Table 3: TCP 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 8080 to the NES server for web socket(ws) communications. Port 4443 to the NES server for secure web socket(wss) communications.  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.
Nymi Agent server	Port 443 to the NES server.
NES server	Port 1443 to the SQL server.



# Use Cases

---

A user can use their authenticated Nymi Band to perform the following POMSnet tasks:

- Sign in
- E-signatures

Users can tap authenticated Nymi Band near an NFC reader(NFC Tap) or the Nymi-supplied Bluetooth adapter(BLE Tap).

**Note:** NFC Taps do not require you to plug the Nymi-supplied Bluetooth adapter into a USB port on the user terminal.

# Install and Configure Nymi Components

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.

## NES Server Configuration

POMSnet 2022.1.0 and later responds to a request to perform an authentication task with the Nymi Band based on the status of the user account in Active Directory.

For example, if a user performs a Nymi Band tap to complete an e-signature, and the password for the user has expired, the attempted e-signature does not complete.

To support this requirement, configure Nymi Enterprise Server(NES) to check the status of the user in Active Directory(AD).

When a user uses their authenticated Nymi Band to perform an authentication task, POMSnet contacts the NES server for the user status. NES contacts AD for the information and returns the result to the POMSnet.

## Configuring Check User Status

Perform the following steps to configure Nymi Enterprise Server(NES) to provide the status of a user in active directory to a Nymi-Enabled Application(NEA).

### 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 **Active Directory** section, select the **Check User Status** option.

The following options appear to customize the active directory user check.

Option	Description
Cache User Status	<ul style="list-style-type: none"><li>Allows NES to cache the status of a user for the time defined in the <b>Cache Expiry</b> option.</li></ul>

Option	Description
	<ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• When this option is enabled, NES contacts AD on the first user status request and stores the results in cache. When an NEA request the status again, NES retrieves the status from cache.</li> <li>• When this option is disabled, NES does not cache the status of users and requires NES to check the status of users every time NES receives a request from the NEA.</li> </ul> <p>When you clear this option, the <b>Cache Expiry</b> option disappears.</p>
Cache Expiry	<ul style="list-style-type: none"> <li>• Defines the length of time that the status of the user remains valid in cache.</li> <li>• Default: 15 mins.</li> <li>• When NES receives a status request from an NEA, and the length of time that the user status has been stored in cache exceeds the cache expiry value, NES contacts AD for the user status and stores the results in cache again.</li> </ul> <p>Nymi suggests that you change this value to 30 seconds.</p>

## 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

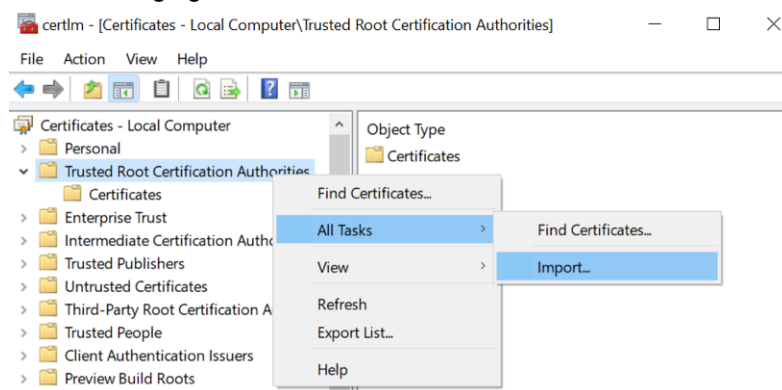
### About this task

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 2: certlm application on Windows 10**

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

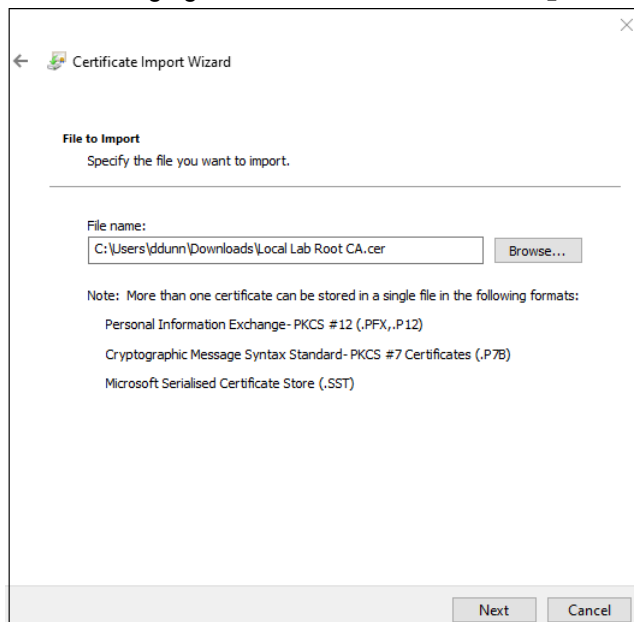
The following figure shows the Welcome to the Certificate Import Wizard screen.



**Figure 3: 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 4: 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.

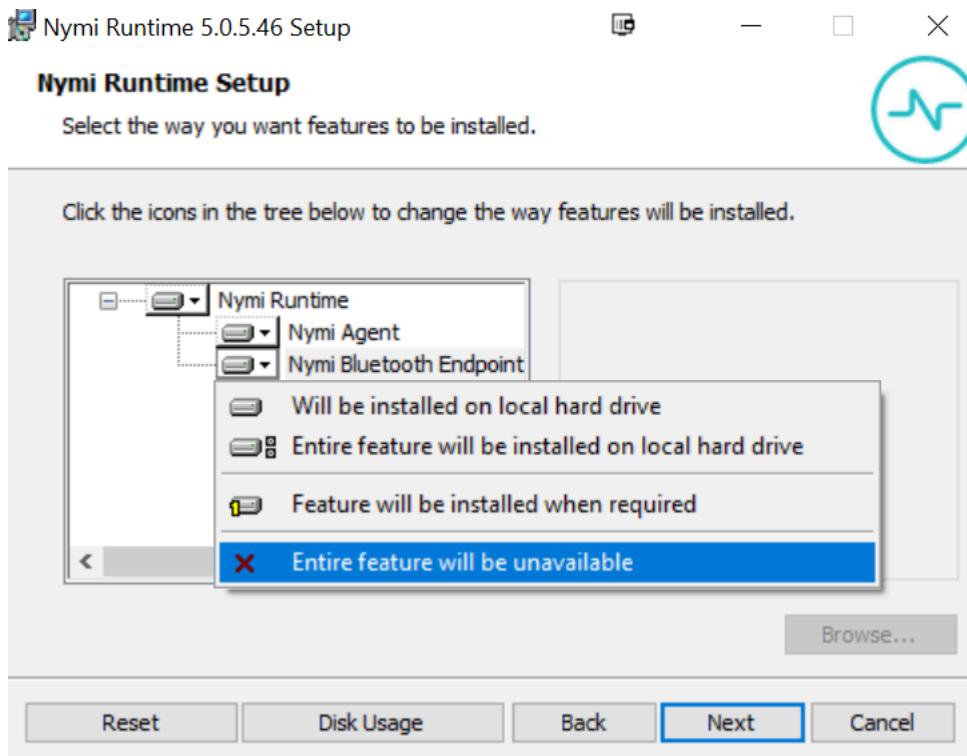
### About this task

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

### Procedure

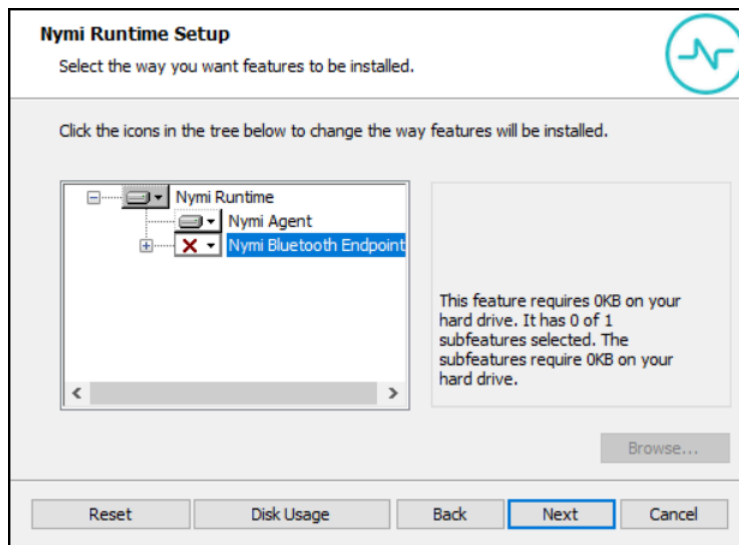
1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the `..nymy-sdk\windows\setup` folder, right-click the *Nymi Runtime Installer version.exe* file, and select **Run as administrator**.
4. On the Welcome page, click **Install**.
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 5: 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**.



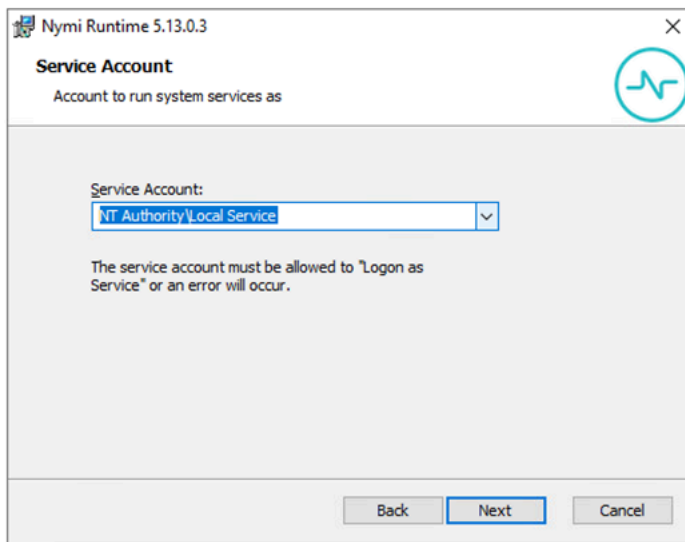
**Figure 6: Nymi Bluetooth Endpoint feature is not available**

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.

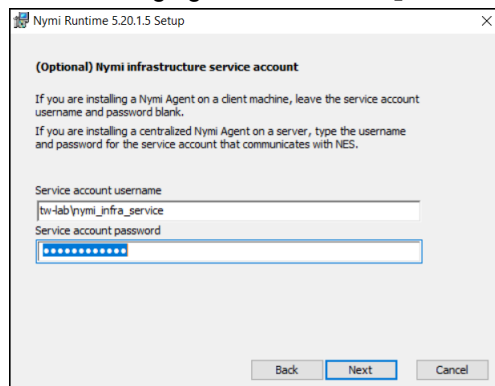
The following figure shows the Service Account window.



**Figure 7: 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 8: 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 For WSS

The Nymi-POMSnet Solution requires that you configure the Nymi Agent to use secure websocket communications between Nymi WebAPI and other Nymi components.

### About this task

A centralized Nymi Agent uses a TOML formatted configuration file to set configuration parameters. 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	Description
[agent] section—Defines configuration parameters for the Nymi Agent service. Most options are optional for the Nymi-POMSnet Solution.	
<i>log_level</i>	<p>Required. Defines the debug logging level. Change the value when instructed by Nymi. Support values include:</p> <ul style="list-style-type: none"> <li>• error—to log only errors</li> <li>• warn—to log both errors and warnings</li> <li>• info—to log errors, warnings, and activity</li> <li>• debug—to log everything including debugging information</li> </ul> <p>The default value is <i>warn</i>.</p>
<i>protocol</i>	<p>Optional. To enable the standard Nymi Agent to use secure websocket communications, uncomment protocol and change the value to <i>wss</i>.</p> <p><b>Note:</b> Requires the configuration of the <i>cacertfile</i>, <i>cacert</i>, and <i>keyfile</i> parameters in the [agent] section.</p> <p>For example, protocol = "wss"</p>

Parameter	Description
<i>port</i>	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.
<i>cacertfile</i>	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.  <b>Note:</b> Requires the configuration of <i>protocol= "wss"</i> , <i>certfile</i> and <i>keyfile</i> parameters in the [agent] section.  For example: <i>cacertfile</i> = "certs/LocalLabRootCA3.pem"
<i>certfile</i>	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.  <b>Note:</b> Requires the configuration of <i>protocol= "wss"</i> , <i>cacertfile</i> , and <i>keyfile</i> parameters in the [agent] section.  For example: <i>certfile</i> = "certs/tw-srv1.tw-lab.local-cert.pem"
<i>keyfile</i>	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.  <b>Note:</b> Requires the configuration of <i>protocol= "wss"</i> , <i>cacertfile</i> , and <i>certfile</i> parameters in the [agent] section.  For example: <i>keyfile</i> = "certs/tw-srv1.tw-lab.local-key.pem"
[nes] section—Defines how the Nymi Agent connects to Nymi components.	
<i>nea_name</i>	Required. Uncomment this parameter and leave the default value.
<i>nes_url "</i>	Required. Uncomment and specify the host URL for the NES server. Include only the protocol and hostname portion of the URI.  For example, https://myserver.name.local.com
<i>directory_service_id</i>	Required. 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, <i>directory_service_id</i> = "NES"

Parameter	Description
<i>credentials_location</i>	<p>Required. Uncomment this line and leave the default value.</p> <p>The <i>credentials_location</i> 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.</p> <p><b>Note:</b> The <i>certs</i> folder contains a file with the encrypted username and password for the Nymi Infrastructure Service Account.</p>
[webapi]—Defines the parameter to enable secure websocket communications between components.	
<i>protocol</i>	<p>Required. Defines the connection protocol. Uncomment <i>protocol = "wss"</i>, which enables secure websocket connections.</p> <p><b>Note:</b> This option requires the configuration of the <i>cacertfile</i>, <i>certfile</i>, and <i>keyfile</i> parameters in the [webapi] section.</p>
<i>port</i>	<p>Required. Defines an alternate server port on which Nymi Agent listens for Nymi WebAPI client WebSocket connections. Uncomment <i>port = 4443</i>.</p>
<i>cacertfile</i>	<p>Required. 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</p> <p><b>Note:</b> Requires the configuration of the <i>protocol = "wss"</i>, <i>certfile</i>, and <i>keyfile</i> parameters in the [webapi] section.</p> <p>For example: "certs/LocalLabRootCA3.pem"</p>
<i>certfile</i>	<p>Required. Uncomment and specify the path to the TLS certificate in PEM format.</p> <p><b>Note:</b> Requires the configuration of the <i>protocol = "wss"</i>, <i>cacertfile</i>, and <i>keyfile</i> parameters in the [webapi] section.</p> <p>For example: "certs/tw-srv1.tw-lab.local-cert.pem"</p>
<i>keyfile</i>	<p>Required. Uncomment and specify the path to the TLS certificate private key in unencrypted PEM format.</p> <p><b>Note:</b> Requires the configuration of the <i>protocol = "wss"</i>, <i>cacertfile</i>, and <i>certfile</i> parameters in the [webapi] section.</p> <p>For example: "certs/tw-srv1.tw-lab.local-key.pem"</p>

4. 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: <ul style="list-style-type: none"><li>• Organizations control when and where a user can perform an enrollment.</li><li>• Supports a supervised enrollment process.</li></ul>
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: <ul style="list-style-type: none"><li>• Allow users to perform enrollments from any thin client.</li><li>• Support an unsupervised enrollment process.</li></ul>

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

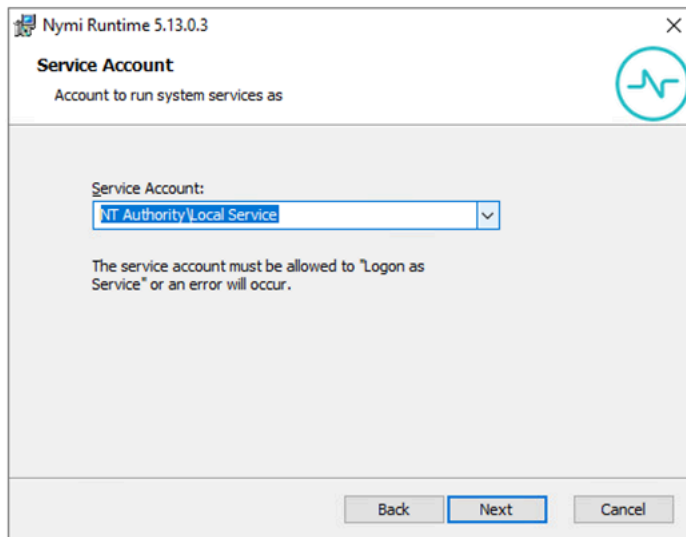
For an update, uninstall the previous version of Nymi Runtime.

## 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 NT Authority\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 9: 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 **NES**, and then select **New > String value**.
5. In the **value** field, type **URL**.
6. 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.
7. Click **OK**.

## Set Up Centralized Enrollment

In this configuration, you perform the following steps:

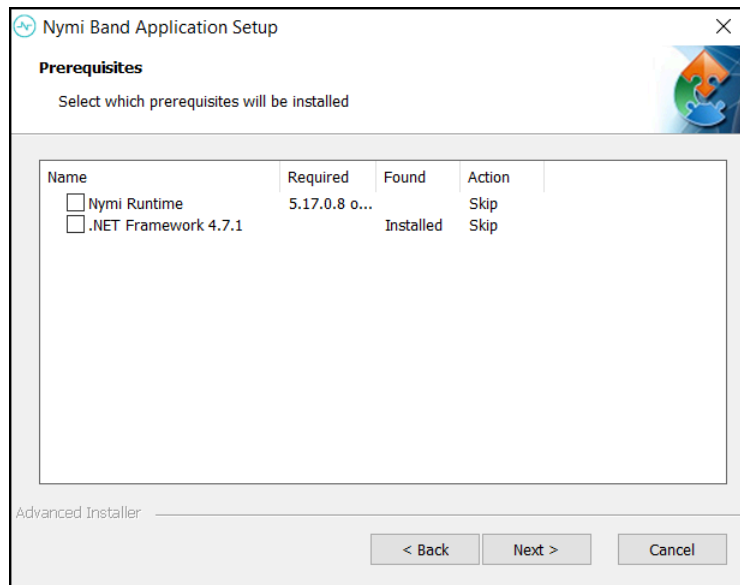
- Install the Nymi Band Application on the Citrix/RDP server, without installing Nymi Runtime.
- Configure the Nymi Band Application to use the centralized Nymi Agent.
- Install the Nymi Bluetooth Endpoint on the thin client that users will use to access the Nymi Band Application.
- Configure the Nymi 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 10: 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 **NES**, and then select **New > String value**.
5. In the **value** field, type **URL**.
6. 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.

7. Click **OK**.

## Install and Configure the Nymi Bluetooth Endpoint on the Enrollment User Terminal

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

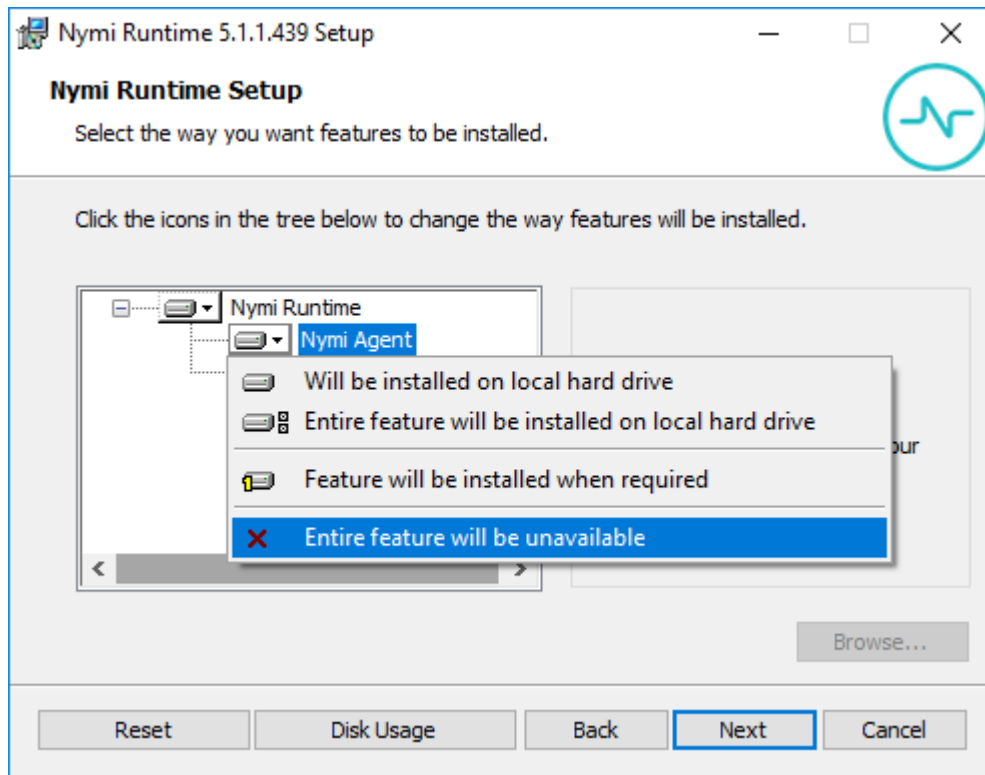
Install the Nymi Bluetooth Endpoint on the machine that accesses the Nymi Band Application on a Citrix/RPD session host.

#### About this task

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

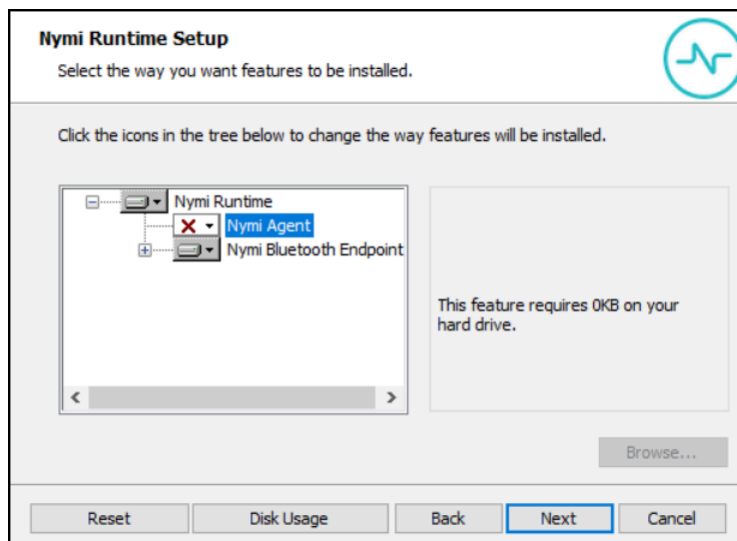
#### Procedure

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 11: 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 12: Nymi Agent feature is not available**

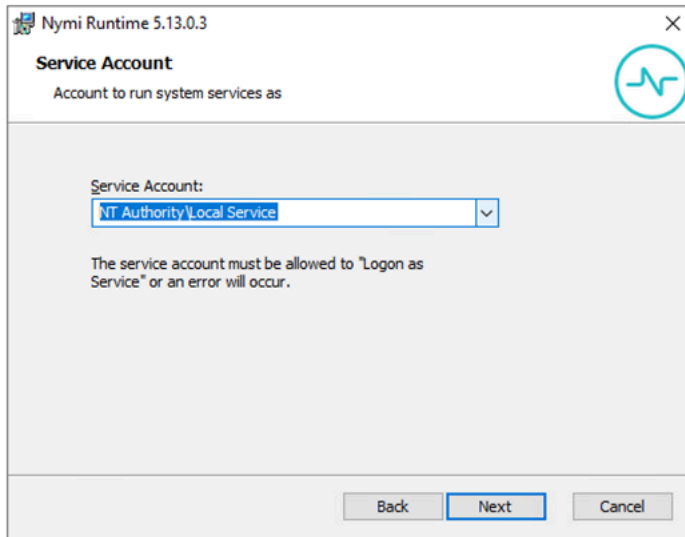
10. On the **Service Account** window, perform one of the following actions to choose the account that starts the service:

- 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 13: 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.

## 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

- Make a copy of the *C:\Nymi\Bluetooth\_Endpoint\nbe.toml* file (On HP Thin Pro, */usr/bin/nbe.toml*).
- Edit the *nbe.toml* file with a text editor in administrator mode.
- 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.

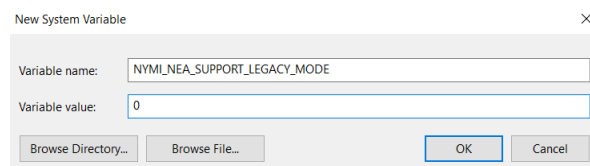
### About this task

**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 then 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 14: New System Variable window**

- c) Click **OK**.

## Set Up User Terminals

On each user terminal that a user uses to access POMSnet and complete authentications tasks with a Nymi Band tap, install and configure the Nymi Bluetooth Endpoint component of the Nymi Runtime software.

### 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.

### Installing Nymi Bluetooth Endpoint

Install the Nymi Bluetooth Endpoint, which is included in the Nymi Runtime installation package, on each user terminal in the environment.

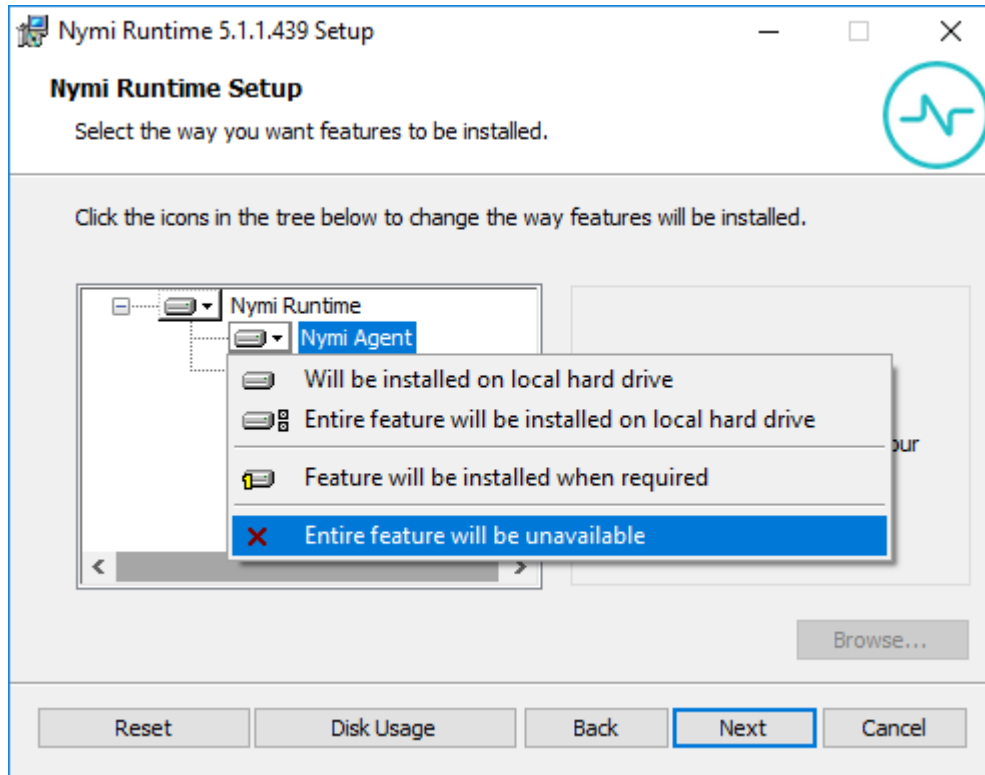
#### About this task

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

#### Procedure

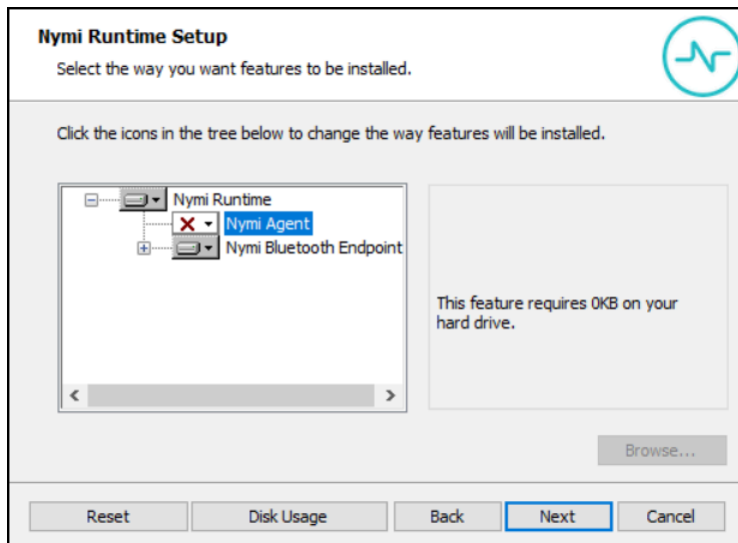
1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the `..\nymi-sdk\windows\setup` folder, right-click the *Nymi Runtime Installer version.exe* file, and select **Run as administrator**.
4. On the **Welcome** page, click **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 15: 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 16: 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**.
11. 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.
12. On the `Ready to install` page, click **Install**.
13. Click **Finish**.
14. On the `Installation Completed Successfully` page, click **Close**.
15. Open the `Windows Services` application and confirm that the `Nymi Bluetooth Endpoint` service appears and the status is `Running`.

## Updating 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:\Wymi\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 replace the default IP address (127.0.0.1) with the FQDN of the machine that is running the remote Nymi Agent.

For example:

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

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

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

## Configuring the Nymi Enterprise Server URL

Perform the following steps to ensure that the negotiate API connects 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**.
4. Right-click **NES**, and then select **New > String value**.
5. In the **value** field, type **URL**.
6. 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.

7. Click **OK**.

## 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

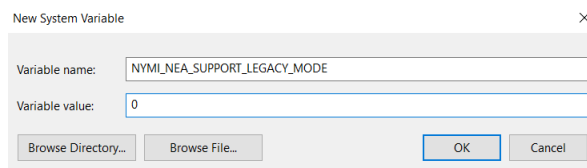
Perform the following steps on all user terminals (for Evidian environments on Wearable user terminals only) where users access Nymi-enabled Applications(NEAs) to disable the legacy protocol. The enrollment terminal only requires the environment variable if users access NEAs on the enrollment terminal.

**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 then 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 17: New System Variable window**







- c) Click **OK**.

# Configuring POMSnet

Perform the following steps to enable the use the Nymi Band with POMSnet.

## Procedure

1. Log into POMSnet as an administrator.
  2. Navigate to **Main menu > System Administration > Configuration Manager**
  3. Search for the parameter *biometric*.
  4. Set the parameter **BiometricAuthenticationEnabled** to *True*, and then save the change.
  5. For the parameter *BiometricAuthenticationHost*, perform one of the following actions:
    - When you install the Nymi Agent on each user terminal, leave the parameter set to the default value *localhost*.
    - When you use a centralized Nymi Agent, set the parameter to the URL of the Nymi Agent, and then save the change.
  6. For a centralized Nymi Agent, set the **BiometricAuthenticationPort** parameter to the correct connection port. The default connection port for the Nymi Agent is 9120.
- The following image provides an example of the Configuration Manager window.

Parameters					
Drag a column header and drop it here to group by that column					
Action	Parameter Name	Default Value	Value	Parameter Description	
	BiometricAuthenticationAuthURL		https://<FQDN>/NES	Optional authentication URL to pass to the biometric authentication service. If not specified, required URL will need to be configured directly in the biometric authentication service. If specified, the value must be the fully qualified URL including protocol, host and URL path such as https://servername.companyname.com/nas	
	BiometricAuthenticationDebug	false	false	Enables logging of debug messages to the javascript console.	
	BiometricAuthenticationEnabled	false	true	Whether biometric authentication is enabled.	
	BiometricAuthenticationHost	localhost	<FQDN>	Hostname of local biometric authentication service.	
	BiometricAuthenticationPort	8000		TCP port on which local biometric authentication service is listening.	
	BiometricAuthenticationProtocol		ws	Protocol to use for communication with the biometric authentication service. Only supported values are ws and wss (for web sockets, and secure web sockets, respectively).	

**Figure 18: POMSnet Configuration Manager window**

7. Log out of the POMSnet application.

# Using the Nymi Band with POMSnet

You can tap the Nymi Band on a connected NFC Reader (NFC Tap) or the Nymi-supplied Bluetooth adapter (BLE Tap) to sign into POMSnet and to perform e-signatures. NFC Taps do not require you to plug in a Bluetooth adapter.

## POMSnet Login

Perform the following steps on a user terminal with access to POMSnet.

1. Connect to the POMSnet Aquila login page.

The POMSnet server connects to the Nymi Agent and displays a message indicating that there is a connection to the authentication service, as shown in the following figure.



**Figure 19: POMSnet Aquila web page**

2. Tap an authenticated Nymi Band against the NFC reader or Bluetooth Adapter.

The user log in completes and the POMSnet application appears.

## E-signatures

Perform an operation in POMSnet that requires an e-signature.

1. Perform operations in POMSnet that require an e-signature. When the pop-up window prompts for a username and password, perform a Nymi Band tap.
2. Perform second e-signature with a Nymi Band tap as required.

The following figure provides an example of an e-signature window.

Electronic Signature initiated at 11/20/2024 03:10:28

i

Reason:  
Edit equipment

Comment:  

Comment

Entering your user ID and password constitutes an electronic signature

Connected to authentication service. Tap device on NFC reader.

First User:

Manual Entry

OK

Cancel

Second User: \*

Second User

Password: \*

Password

**Figure 20: POMSnet e-signature window**

Copyright ©2025 Nymi Connected Worker Platform POMSnet Installation and Configuration Guide v4.0 37

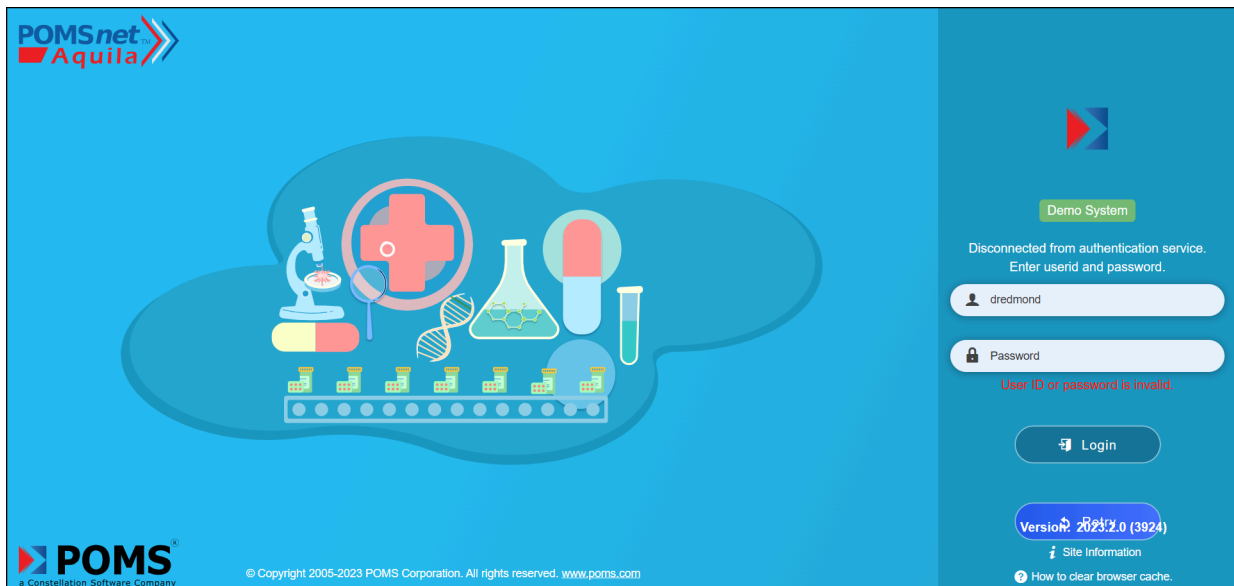
# Troubleshooting POMSnet Issues

Review this section for information that can assist you in troubleshooting issues when using the Nymi with POMSnet solution.

## Disconnected from authentication service

This error message appears when you connect to the POMSnet log in page.

The following image provide an example of the error message.



**Figure 21:**

When you set the POMSnet *BiometricAuthenticationDebug* parameter to **True**, and then start **Developers Tools** in your browser, the following message appears:

```
websocket connection to 'wss://hostname:port/'
Disconnected from authentication service. Enter userid and password.
```

### Cause

By default POMSnet 2022 attempts to establish connection to the Nymi Agent over secure websocket (wss) but the Nymi Agent is configured to use websocket (ws).

### Resolution

Log into the POMSnet interface with the username and password of an administrator. In Configuration Manager, set the **BiometricAuthenticationProtocol** parameter to **WS**.

## Biometric authentication service is not configured to return user status

This error appears on the POMSnet log screen.

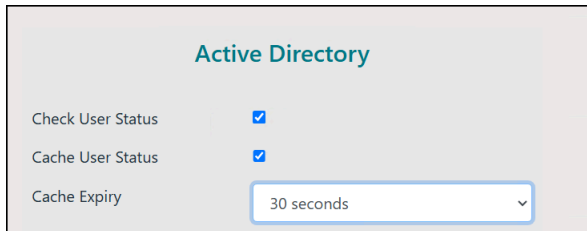
### Cause

POMSnet 2022.1.0 (3157) and later enforces the confirmation of the status of a user account in Active Directory.

### Resolution

1. Log into the NES Administrator Console as a CWP Administrator and edit the active policy.
2. In the **Active Directory** section, select **Check User Status**.
3. In the **Active Directory** section, select **Cache User Status**.
4. From the **Cache Expiry** list, select **30 seconds**.
5. Click **Save**.

The following figure shows the **Active Directory** section.



Active Directory	
Check User Status	<input checked="" type="checkbox"/>
Cache User Status	<input checked="" type="checkbox"/>
Cache Expiry	30 seconds

6. Close the POMSnet browser window and connect to POMSnet again.

Copyright ©2025  
Nymi Inc. All rights reserved.

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

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

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

Published in Canada.  
Nymi Inc.  
Toronto, Ontario  
[www.nymi.com](http://www.nymi.com)