POMSnet Installation and Configuration Guide

Nymi Connected Worker Platform
v3.0
2025-01-15

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.

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: • New *Use Cases* section • Clarifications to the *Nymi Runtime Installation and Configuration* section.
3.0	January 15, 2024	Third release of this document to correct the Nymi Agent port from 9210 to 9120.

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 with Evidian Installation and Configuration Guide**

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

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

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

  This document provides information about how to troubleshoot issues and the error messages that you might experience with the NES Administrator Console, the Nymi Enterprise Server deployment, the Nymi Band, and the Nymi Band Application.
- **Nymi Connected Worker Platform with Evidian Troubleshooting Guide**

  This document provides overview information about how to troubleshoot issues that you might experience when using the Nymi solution with Evidian.
- **Nymi Connected Worker Platform—FIDO2 Deployment Guide**

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

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

- **Nymi Band Regulatory Guide**

  This guide provides regulatory information for the Generation 3 (GEN3) Nymi Band.
- **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 Connected Worker Platform with POMSnet Solution

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.

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

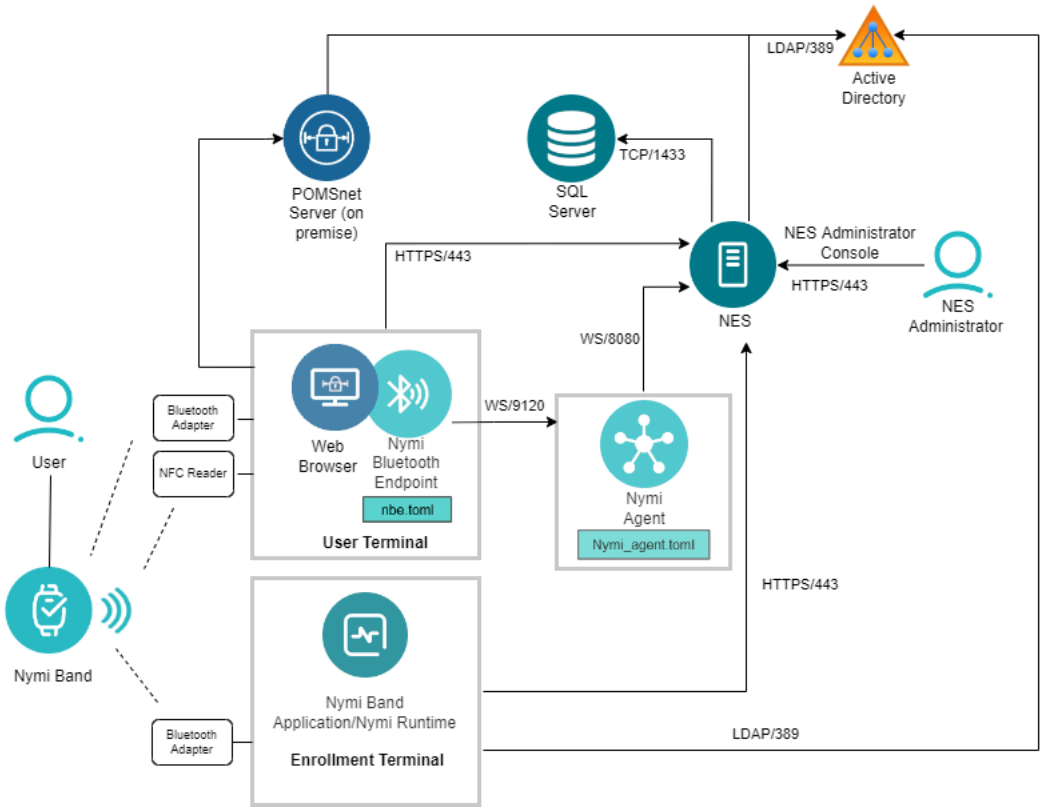

Figure 1: Nymi with POMSnet Overview

Table 2: Components in a Nymi with POMSnet Solution

Component	Description
Enrollment Terminal	Windows 10 endpoint that users access to enroll their Nymi Band.

Component	Description
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. 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.
Nymi Band	A wearable device that the assigned user with their biometrics. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled.
NES	A management server and collection of services that provides the NES Administrator Console and 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 Agent	Provides BLE management, manages operations and message routing. Facilitates communication between NEAs and the Nymi Band, and maintains knowledge of the Nymi Band presence and authenticated states. The Nymi Agent is a component of the Nymi Runtime application. You can install Nymi Agent on each workstation or install Nymi Agent in a central location.
Nymi Bluetooth Endpoint	Provides an interface between the Bluetooth Adapter (BLE) and the Nymi Agent. You deploy Nymi Bluetooth Endpoint Daemon (NBEd) on individual workstations to provide local BLE communication with 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.

Component	Description
nymi_agent.toml	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.

Firewall Port Requirements

The following tables summarizes the TCP port requirements for the Nymi with POMSnet 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 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. Port to the POMSnet server. Port 1443 to the SQL server with the eInfotree database.
Nymi Agent server	Port 8080 to the NES server for web socket communications.
NES server	Port 1443 to the SQL server.
SQL Server	Optional. Port 25 to the SMTP server to allow email alerts. Port 389 to the AD server.

Use Cases

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

- Sign into POMSnet.
- Perform e-signatures.

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 and the Nymi-eInfotree Excel Module on the user terminals. *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-sign off, and the password for the user has expired, the e-sign off attempt does not complete.

To support this requirement, configure the NES server to check the status of the user in Active Directory.

When a user uses the 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 NES to provide the status of a user in active directory to a 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	• Allows NES to cache the status of a user for the time defined in the **`Cache Expiry`** option. • Default: enabled • 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. • 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. When you clear this option, the **`Cache Expiry`** option disappears.
Cache Expiry	• Defines the length of time that the status of the user remains valid in cache. • Default: 15 mins • 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.

Set Up the 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 the Nymi Band Application with the Installation Wizard

Perform the following steps to install the Nymi Band Application.

Before you begin

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.

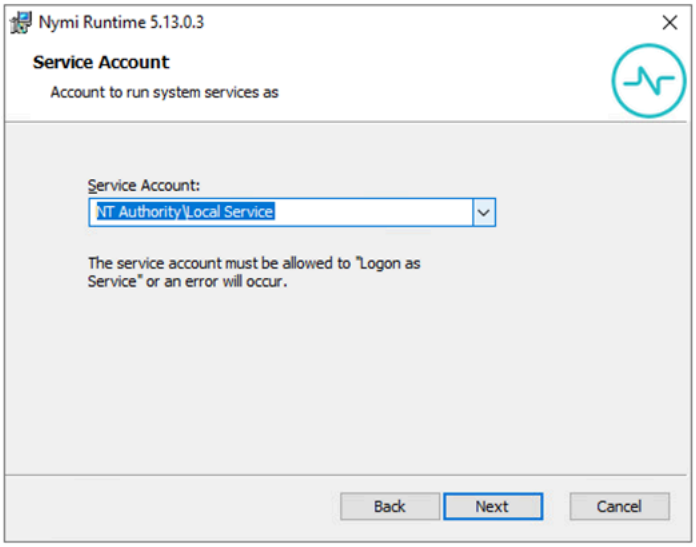

Figure 2: Nymi Runtime Service Account window

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.

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**.

Nymi Runtime Installation and Configuration

The Nymi with POMSnet integration uses the Nymi Runtime application to facilitate communication between NES, the Nymi Band, and POMSnet.

The Nymi Runtime software contains two installable components, the Nymi Bluetooth Endpoint and Nymi Agent.

The Nymi Runtime installation and configuration differs depending on if the environment uses a centralized Nymi Agent or if each user terminal includes a local Nymi Agent.

Local Nymi Agent Configuration

In this configuration you install both components of the Nymi Runtime locally on each user terminal.

Use this configuration when:

- Users access POMSnet from a web browser on their user terminal.
- User terminals reside on the same domain as the NES server.

Centralized Nymi Agent Configuration

In this configuration, you install a centralized Nymi Agent on a separate server, and then install the Nymi Bluetooth Endpoint component on each user terminal.

Use this configuration when:

- Users access the MES applications from a web browser within a remote session host, such as Citrix or RDP server.
- MES application relies on WebAPI websocket communications. The Nymi SDK Developer Guide—Webapi(Windows) provides more information about Nymi WebAPI.
- User terminals reside in a different domain from the NES server.

Local Nymi Agent Installation and Configuration

You can install Nymi Agent and the Nymi Bluetooth Endpoint components of the Nymi Runtime on the user terminals that are a member of the same domain as the NES server.

(Windows) Install Nymi Runtime

Nymi Runtime facilitates communication between NES and the Nymi Bands.

Install the Nymi Runtime on each user terminal on which you will also install a Nymi-enabled Application. You can perform a customizable installation or a silent installation.

Note: The Bluetooth (BLE) driver is installed with the installation of Nymi Runtime. The BLE driver may also be installed separately by going to the Nymi SDK package and installing the *BleDriver .msi* file.

Performing Nymi Runtime Installation or Update with the Installation Wizard

Perform the following steps to install or update Nymi Runtime on the user terminals.

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Create a backup copy of the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file.
3. Extract the Nymi SDK distribution package.
4. From the *..\nymi-sdk\windows\setup* folder, right-click the *Nymi Runtime Installer version.exe* file, and select **`Run as administrator`**.
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` page, 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`**.
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 `Installation Completed Successfully` page, click **`Close`**.
12. In the `Windows Services` applet, confirm that you can see the *Nymi Agent* and *Nymi Bluetooth Endpoint* services, and that the status of each service is *`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 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*.
protocol = "ws"	[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 = "9120"	[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.

Parameter and Sample Value	Section Name	Description
cacertfile = "/path/to/cacertfile.pem"	[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"
certfile = "path/certfile.pem"	[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"

Parameter and Sample Value	Section Name	Description
keyfile = "path/keyfile.pem"	[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.
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"*

Parameter and Sample Value	Section Name	Description
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.
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.

Parameter and Sample Value	Section Name	Description
port = 4443 or *port = 8080*	[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: • For the *ws* protocol, uncomment *port = 8080*. • For the *wss* protocol, uncomment *port = 4443*.
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"

Parameter and Sample Value	Section Name	Description
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 a Centralized Nymi Agent

When your environment uses iOS devices, thin clients, and web-based Nymi-enabled Applications, you must deploy a centralized Nymi Agent on a Windows server in the environment, for example, the NES server.

The Nymi Agent has two server interfaces, the standard Nymi Agent interface and the Nymi WebAPI interface. By default, standard Nymi Agent interface connect over plain text websocket and the 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.

Performing a Nymi Agent Installation or Update By Using the Installation Wizard

Install 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 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.

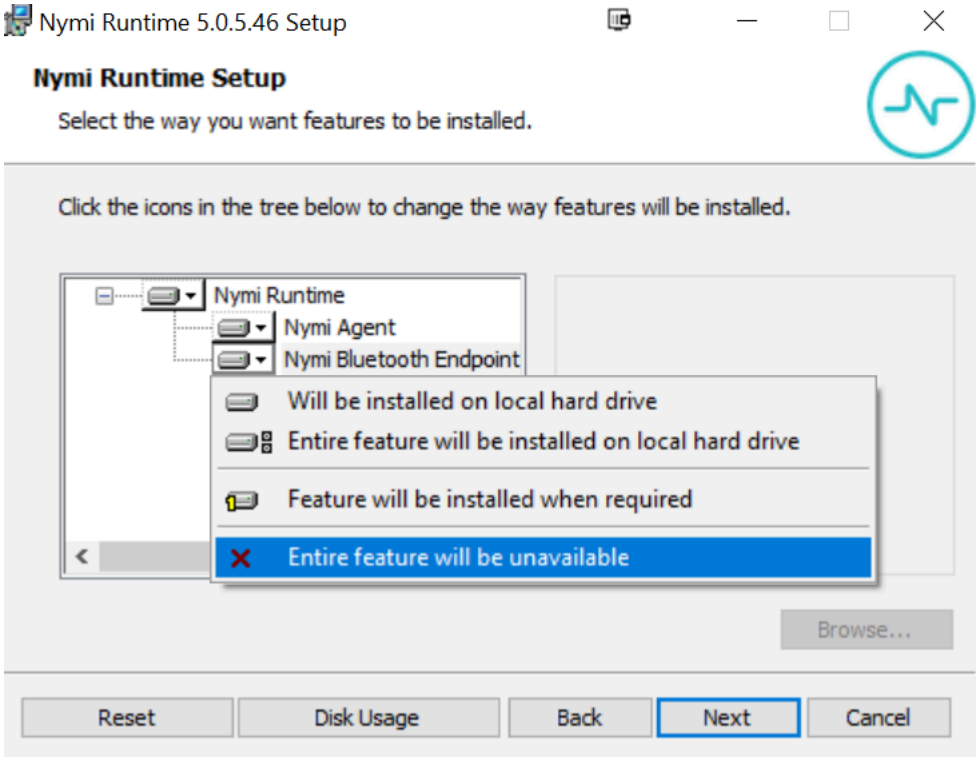

Figure 3: Nymi Bluetooth Endpoint feature will be unavailable

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

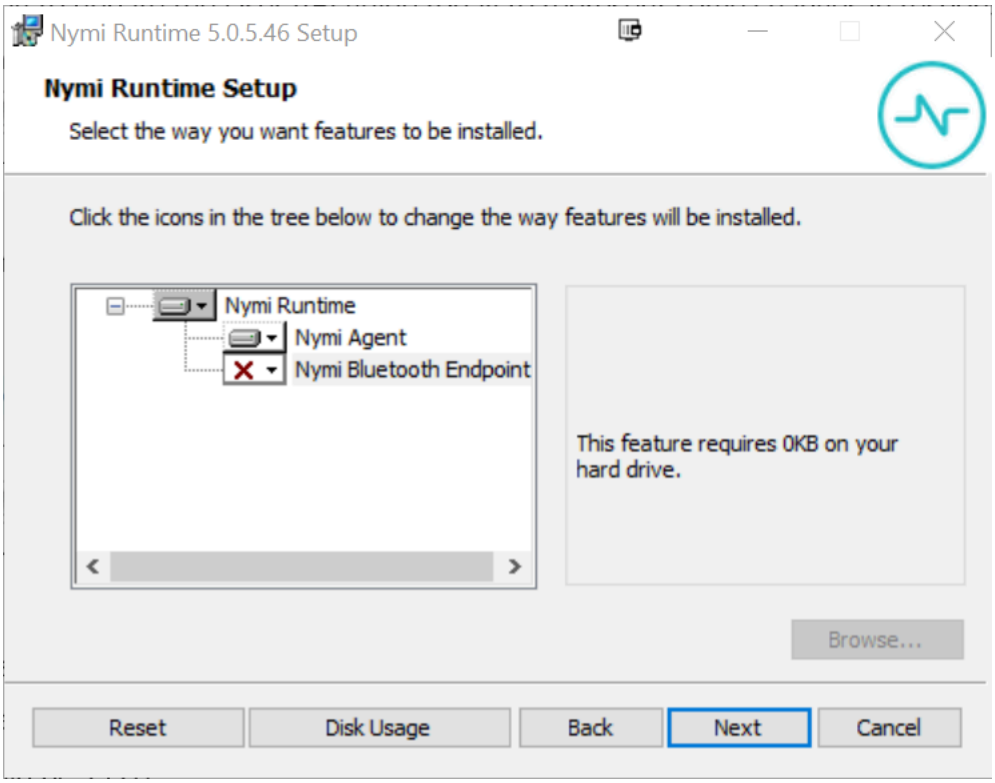

Figure 4: Nymi Bluetooth Endpoint feature is not available

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.

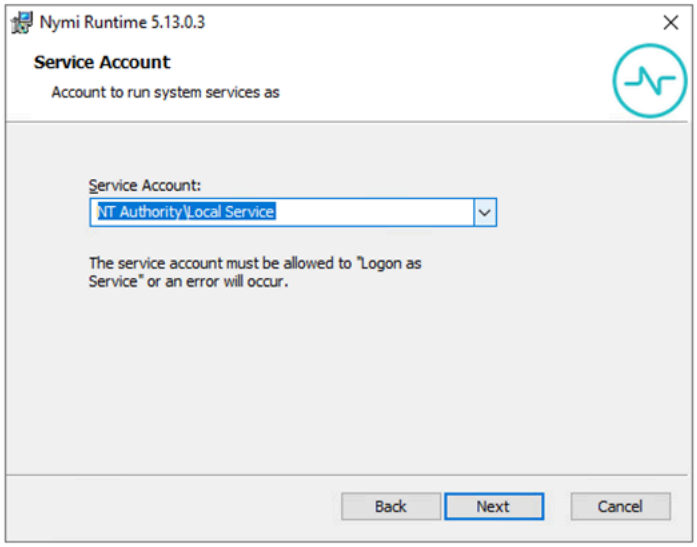

Figure 5: Nymi Runtime Service Account window

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*. Refer to *Appendix—Record the CWP Variables* for the service account name.

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

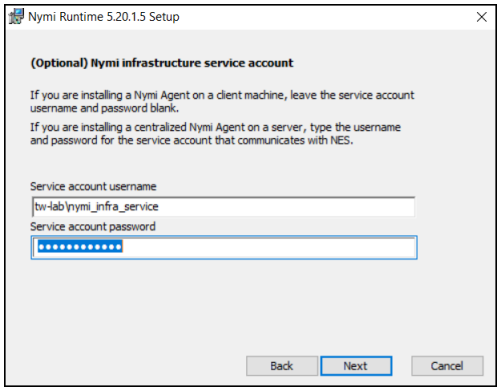

Figure 6: Nymi Infrastructure Service Account window

    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
    - Public key

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

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. Create a backup copy of the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file.
3. Extract the Nymi SDK distribution package.
4. From the *..\nymi-sdk\windows\setup* folder, right-click the *Nymi Runtime Installer version.exe* file, and select **`Run as administrator`**.
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, expand **`Nymi Runtime`**.
9. Select **`Nymi Agent`**, and then select **`Entire feature will be unavailable`**, as shown in the following figure, and then click **`Next`**.

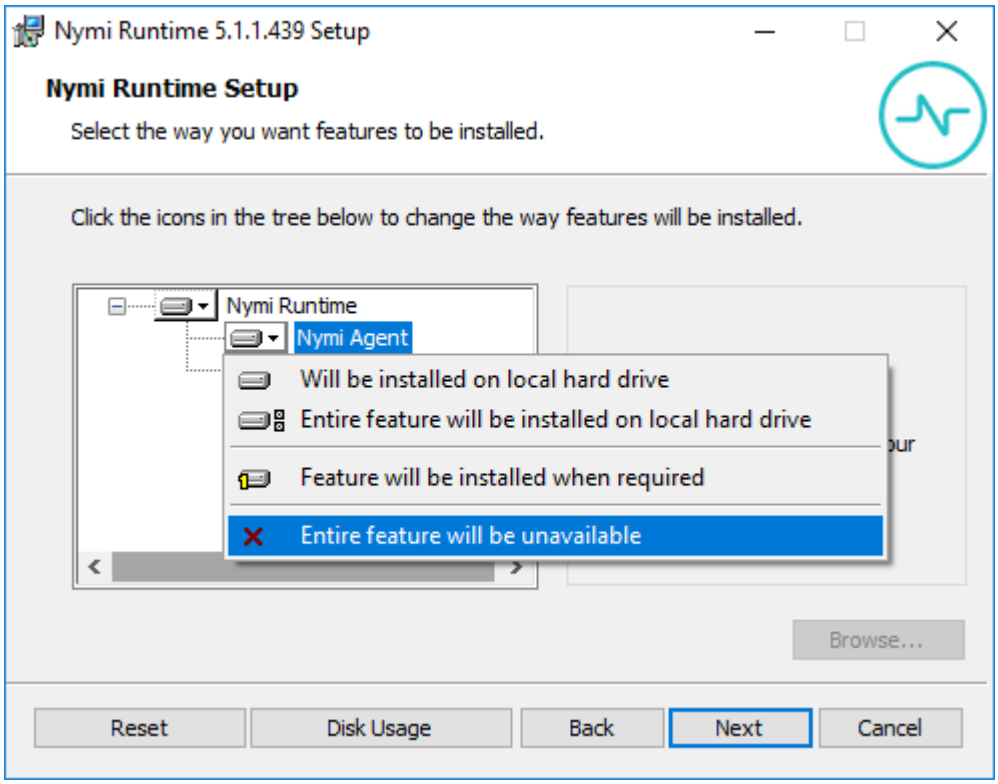

Figure 7: Nymi Agent feature will be unavailable

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

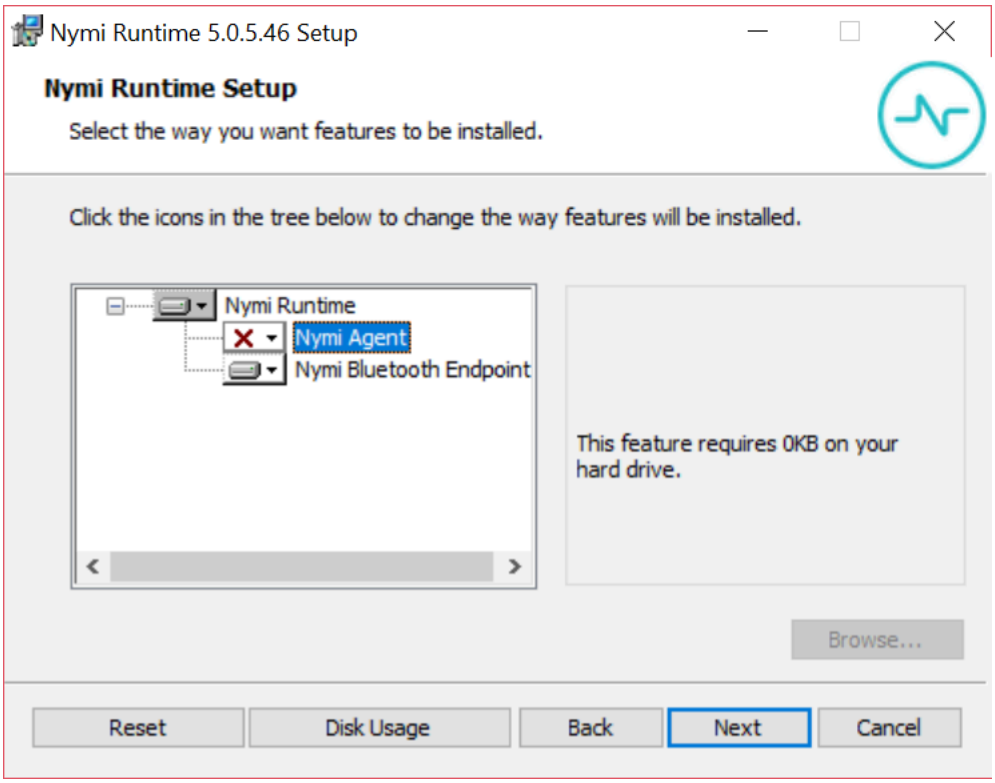

Figure 8: Nymi Agent feature is not available

11. 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`**.
12. 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.
13. On the `Ready to install` page, click **`Install`**.
14. Click **`Finish`**.
15. On the `Installation Completed Successfully` page, click **`Close`**.
16. 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:\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 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 POMSnet

About this task

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 port. The default port for the Nymi Agent is 9120.
   The following image provides an example of the `Configuration Manager` window.

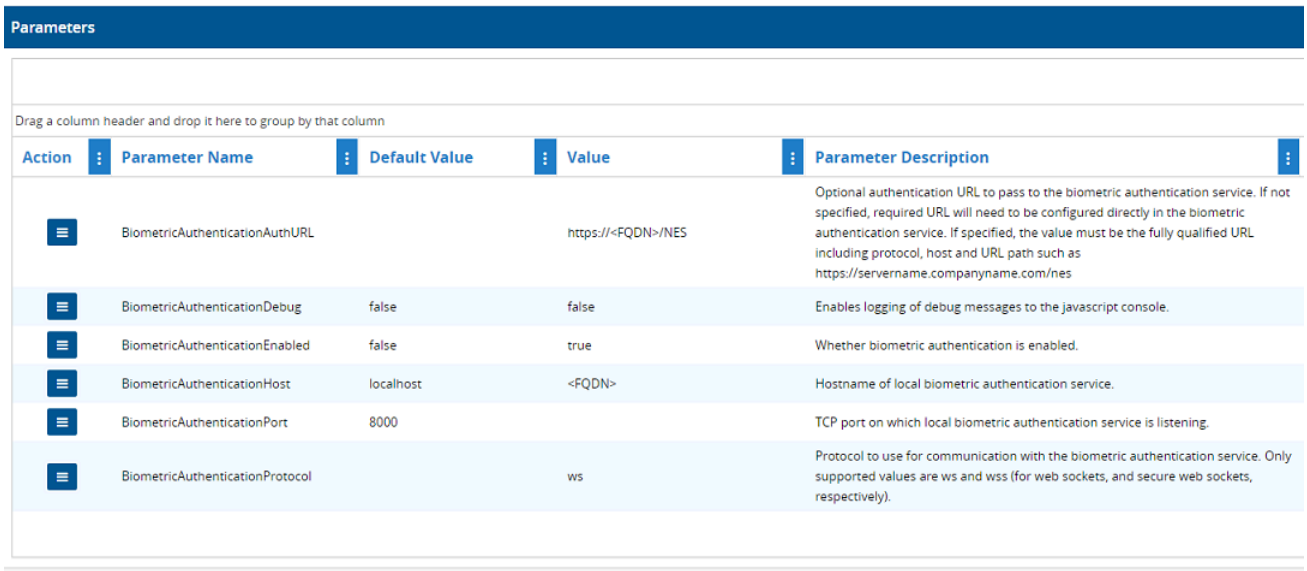

Figure 9: POMSnet Configuration Manager window

7. Log out of the POMSnet application.

Using the Nymi Band with POMSnet

Use the Nymi Band to sign into POMSnet and to perform e-signatures.

About this task

Perform the following steps on a user terminal with a connected NFC Reader and Bluetooth adapter.

Procedure

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 10: POMSnet Aquila web page

2. Tap an authenticated Nymi Band against the NFC reader.
   The user log in completes and the POMSnet application appears.

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