Installation and Configuration Guide

Nymi Connected Worker Platform with POMSnet

v1.0

2022-06-30

Contents

Preface

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

Purpose

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

The Nymi Connected Worker Platform with POMSnet 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.

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 Nymi Enterprise Server (NES). This installation uses the `Nymi Token Service` to install certificates that enable communication between components. This document also provides information about deploying the Connected Worker Platform in a Citrix or RDP environment.
- **Nymi Connected Worker Platform Administration Guide**

  This document provides information about how to use the `NES Administrator Console` to manage the `Connected Worker Platform` (CWP) system. This document describes how to

set up, use and manage the Nymi Band™, and how to use the `Nymi Band Application`. This document also provides instructions on deploying the Nymi Band Application and Nymi Runtime components.

- **Connected Worker Platform with Evidian Installation and Configuration Guide**

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

  This document provides overview information about how to troubleshoot issues that you might experience when using the Nymi solution with Evidian.
- **Nymi SDK for C Developer's Guide**

  This document provides information about how to develop Nymi-enabled Applications by using the `Nymi API(NAPI)`.
- **Nymi SDK for WebSocket Developer's Guide**

  This document provides Nymi developers with an alternative way to utilize the functionality of the `Nymi SDK`, over a WebSocket connection managed by a web-based or other applications.
- **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`.
- **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 and the TCP ports that are used between the components for communication.

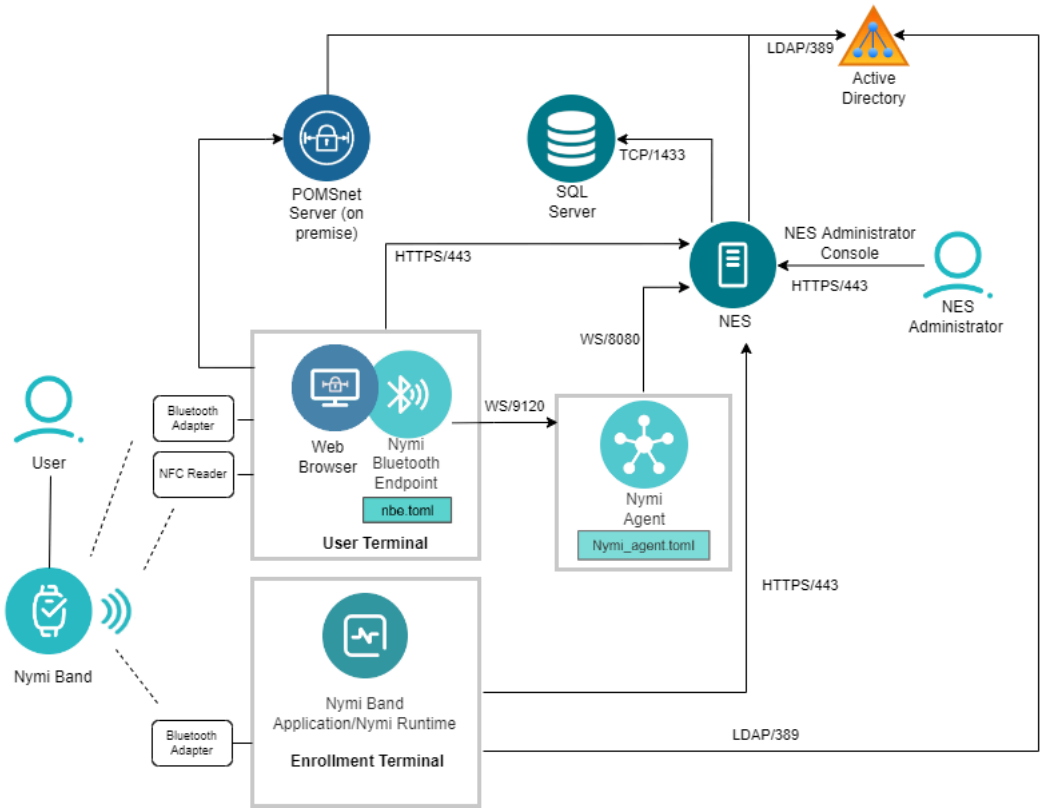


Figure 1: Nymi with POMSnet Overview

Table 2: Components in a Nymi with POMSnet Solution

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

Component	Description
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal and is used 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 machine on which you install Nymi components that allow users to perform authentication tasks with the Nymi Band. 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 is activated by the assigned user's biometrics. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled. See the Nymi Band section in this guide for more information.
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 external directory and database systems, such as 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.
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`. If you do not use a centralized `Nymi Agent`, you must create this file on each user terminal. This file defines the hostname of the NES server and the configuration parameters that support Nymi Band communications between the user terminals and the POMSnet server.

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 9210 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.
Nymi Agent server	Port 8080 to the NES server for web socket communications.
NES server	Port 1443 to the SQL server.

Install and Configure Components

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

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.

Option	Description
	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.

Enrollment Terminal Installation and Configuration

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.

1. Insert the Nymi-supplied Bluetooth adapter into an available USB port.
2. Import the Root CA certificate.
3. Install the Nymi Band Application. The Nymi Band user requires physical access to the network terminal.
4. Set the NES_URL registry key.

Note: The Nymi Band Application includes the `Nymi Runtime` software.

Nymi Band Application Installation

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.

Note: The 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 a customizable Nymi Band Application installation

Perform the following steps to install the Nymi Band Application on a network device.

About this task

Procedure

1. Download the Nymi Band Application package.
2. Double-click to run the Nymi-Band-App-installer-v_*version*.exe installer.

3. Follow the prompts in the Nymi Band Application installation wizard and when prompted, install all the prerequisite packages and BLE device driver from Silicon Labs.
4. 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`*.
5. Close the Nymi Band Application.

Performing a silent Nymi Band Application Installation or Upgrade

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

About this task

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.

Setting the NES URL

After you install the `Nymi Band Application`, ensure that the enrollment process uses the correct NES URL.

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, set 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 it is recommended that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.

7. Click **OK**.

User Terminal Installation and Configuration

Install the Nymi Runtime software on each user terminal. 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.

The Nymi Runtime software contains two installable components, the Nymi Bluetooth Endpoint and Nymi Agent. By default Nymi Runtime installs both components on the user terminal.

in the following configuration scenarios, install the Nymi Bluetooth Endpoint component on each user terminal and the Nymi Agent on a separate server that is accessible to all the user terminals, such as the NES server:

- Users access remote MES applications (on a Citrix or RDP server) from the user terminal.
- MES application relies on web socket communications.
- User terminals reside in a different domain from the NES server.

Local Nymi Agent Installation and Configuration

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

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: Nymi Lock Control and the Nymi Band Application automatically install Nymi Runtime, machines with Nymi Lock Control or Nymi Band Application, it is not necessary for you to install the Nymi Runtime application.

Performing a customizable Nymi Runtime installation or upgrade

Perform the following steps to install or upgrade Nymi Runtime on a network device, on which you want to install a Nymi-enabled application.

About this task

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the `Nymi SDK` distribution package.
3. From the ..*nymi-sdk**windows**setup* folder, run the *Nymi Runtime Installer version.exe* file.
4. On the `Welcome` page, click **`Install`**.
5. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
7. On the `Nymi Runtime Setup` page, click **`Next`**.
8. On the `Service Account` window, click **`Next`**.
9. On the `Ready to install` page, click **`Install`**.
10. Click **`Finish`**.
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`*.

Performing a silent installation or upgrade of Nymi Runtime

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

About this task

Procedure

1. Log in to the network terminal with an account that has administrator privileges.
2. Extract the Nymi API distribution package.
3. Launch the command prompt as administrator.
4. Change to the ..*nymi-sdk**windows**runtime* folder, and then type: *"*Nymi Runtime *Installer version.exe" /exenoui /q*

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

   Note: Ensure that you enclose the command 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.

   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

The silent installation process creates an installation log file in the *%temp%* directory named Nymi Runtime_*version_time*.*log*

Configuring the Nymi Agent toml File

Configuration settings for the `Nymi WebAPI` are contained in a toml file. If the `Nymi WebAPI` is not configured (the toml file does not exist), the `Nymi Agent` runs with the `Nymi WebAPI` disabled by default.

A sample configuration file named *nymi_agent_default.toml* file is included in the `Nymi SDK` package and is installed by default in the *C:\Nymi\NymiAgent* directory. In order to enable the WebSocket simply make a copy of the file and name it *nymi_agent.toml*.

When you edit the *nymi_agent.toml* to configure `Nymi Agent` with `WebAPI`, ensure that:

- Each interface uses a distinct TCP port (do not use 9120/tcp)
- Machine has connectivity to NES
- Network Address Translation (NAT) does not exist between the `Nymi Agent` machine and the user terminals.
- `Nymi Agent` can co-locate with the NES (ensure that you use distinct TCP ports)

General Application Settings

These settings are application-wide and enable you to define the logging level.

- error: log only errors
- warn: log both errors and warnings
- info: log errors, warnings, and activity
- debug: log everything including debugging information

The following is the default setting: *log_level = "warn"*

Enterprise Server Settings

The *NES* section defines settings that affect the embedded Nymi-enabled Application (NEA), which is the basis `Nymi WebAPI`.

Table 4: Enterprise Service

Description	Setting
Sets the NEA name for the embedded NEA `WebAPI` server application.	*`nea_name = "NymiAgent"`*
The host URL for the NES server. Include only the protocol and hostname portion of the URI. For example, replace `https://server.name.local` with your nes_url.	*`nes_url = "https://server.name.local.com"`* For example, https://myserver.name.local.com

Description	Setting
'The directory service name for NES. For example if your NES URL is https://server.name.local.com/NES, the directory name is NES.	`directory_service_id = "NES"`
The TLS client root CA certificate bundle to use when communicating with NES. If it is not specified a built-in bundle containing well known root CAs is used. Specify the path to a CA certificate or bundle to customize the trusted CA bundle using the PEM format.	Certificate bundle in PEM format for the signing CA certificate chains for the TLS certificates that are used by NES and `WebAPI`.
cacertfile = "cacertfile.pem"	

Note: An NEA expects a Nymi Bluetooth Endpoint with an endpoint name that is the based on the network interface address used to communicate with the agent. If the NEA and `Nymi Bluetooth Endpoint` connect to the `Nymi Agent` on different network interfaces, the Nymi-enabled Application will not see the endpoint and will report it as missing with a status code of 5100. Nymi recommends that additional interfaces be disabled or to set a static well-known endpoint ID in the *nbe.toml* of the endpoint terminal and supply the endpoint ID to the Nymi-enabled Application to manually subscribe after connecting to the Nymi Agent.

on the network interface address that is used to communicate with the `Nymi Agent`. If the NEA and `Nymi Bluetooth Endpoint` connect to the `Nymi Agent` on different network interfaces, the Nymi-enabled Application does not find the endpoint and reports that the endpoint is missing (status code 5100).

For local environments where the `Nymi Bluetooth Endpoint` and the NEA runs on the same computer, and the computer has more than one interface that can contact the `Nymi Agent`, use the computer as the topic name for the `Nymi Bluetooth Endpoint` and the NEA to communicate.

For Citrix/RDP scenarios, use the client computer name as the topic name to support communications between the `Nymi Bluetooth Endpoint` that runs on the client computer and the NEA that runs on the Citrix/RDP host. Ensure that the NEA subscribes to the topic by using the client name of the session.

WebAPI Protocol Settings

The following table provides settings used to set the WebAPI application.

Table 5: WebAPI Protocol Settings

Description	Example
Specify the protocol supported by the `Nymi WebAPI` server. Use the default protocol *ws* to support a plain WebSocket using `ws://...` URL scheme. Use `wss` to support a secure WebSocket using TLS and the `wss://...` URL scheme. Set the protocol to *wss* in production environments.	*protocol = "wss"*

Description	Example
The server port to listen for `Nymi WebAPI` client WebSocket connections on. The default depends on the `protocol` settings. For the *ws* protocol the default port is 8080. For the *wss* protocol the default port is 4443. You can set an alternate port using this setting.	*port = 4443 port = 8080*
Certificate bundle in PEM format for the signing CA certificate chains for the TLS certificates that are used by NES and `WebAPI`.	`cacertfile = "/path/to/certfile.pem"`
The path to the server certificate in PEM format.	*certfile = "/path/to/certfile.pem"*
The path to the server certificate private key in PEM format.	*keyfile = "/path/to/keyfile.pem"*

Note: The `Nymi Agent` must be able to receive incoming WebSocket connections on TCP port 9120 (used for communication with `Nymi Bluetooth Endpoint`) and on the TCP port configured for `Nymi WebAPI` connections (default 8080 when using the ws protocol, and default 4443 when using the wss protocol). Ensure that these ports are open bi-directionally in the firewall on the machine that runs the `Nymi Agent`.

Centralized Nymi Agent Installation and Configuration

Install the `Nymi Agent` component on a server that all user terminals can access, for example, the NES server.

Installing the Nymi Agent

Install the `Nymi Agent` application, which is included in the `Nymi Runtime` installation package, on a machine in the environment.

About this task

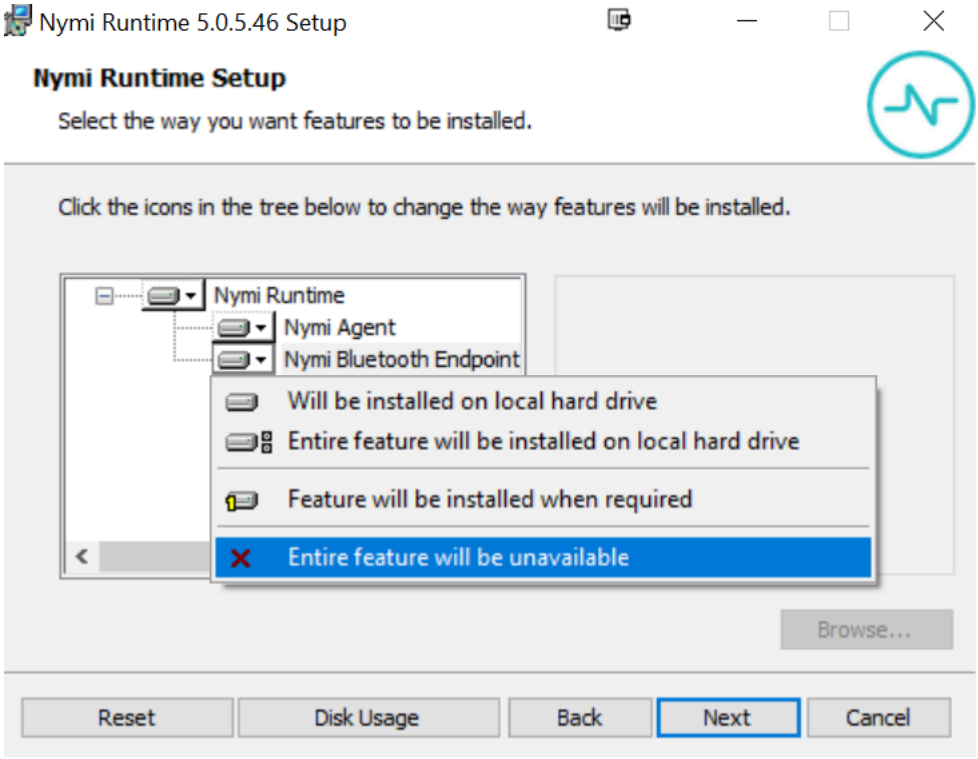
When you install the `Nymi Runtime` software, you can choose to install the `Nymi Agent` application only.

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, run the *Nymi Runtime Installer version.exe* file.
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 2: 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`**.

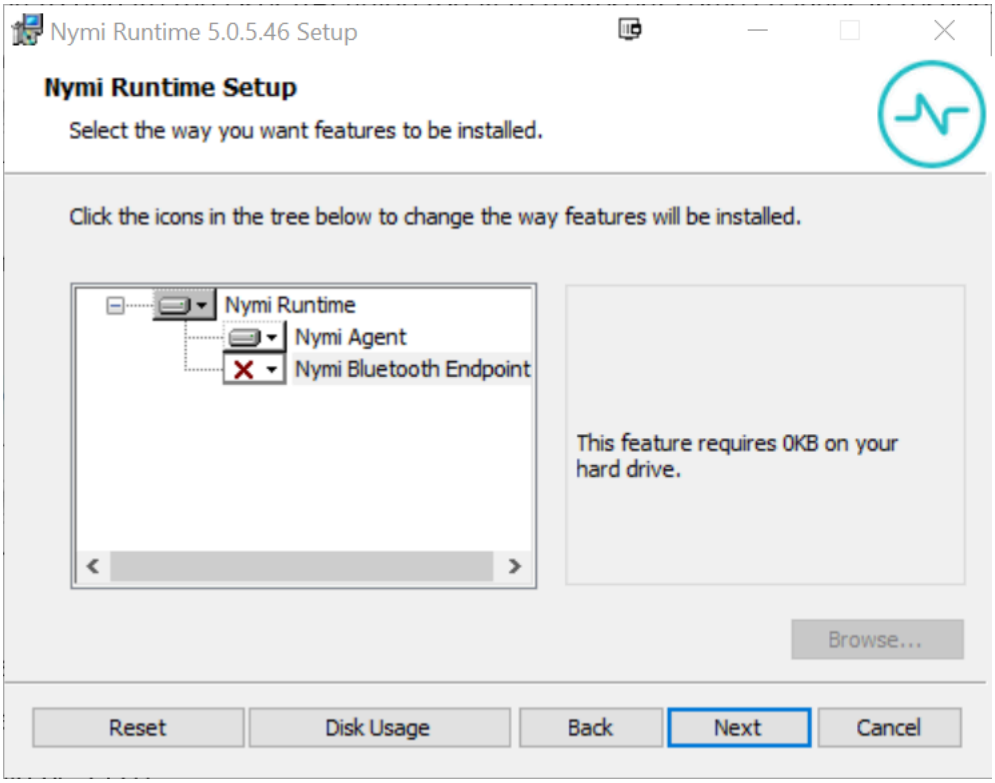


Figure 3: Nymi Bluetooth Endpoint feature is not available

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

Results

Note: Take the following TCP port requirements into consideration:

- Nymi Agent receives incoming WebSocket connections on TCP port 9120, which is used for communication with Nymi Bluetooth Endpoint.
- Nymi WebAPI receives incoming WebSocket connections on the TCP port configured for Nymi WebAPI connections (default 8080 when using the ws protocol, and default 4443 when using the wss protocol).

Ensure that firewalls allow incoming communication on these ports on the server that runs the Nymi Agent.

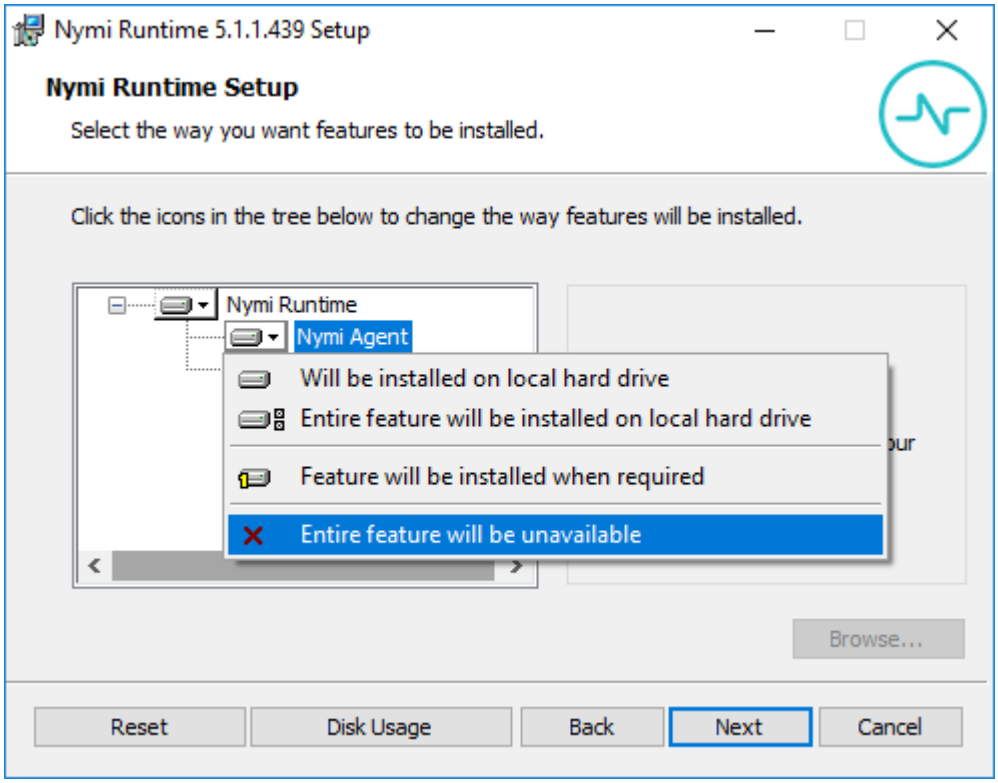
Installing Nymi Bluetooth Endpoint

About this task

Install the `Nymi Bluetooth Endpoint`, which is included in the `Nymi Runtime` installation package, on each user terminal in the environment. 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, run the *Nymi Runtime Installer version.exe* file.
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.



`Figure 4: Nymi Agent feature will be unavailable`

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

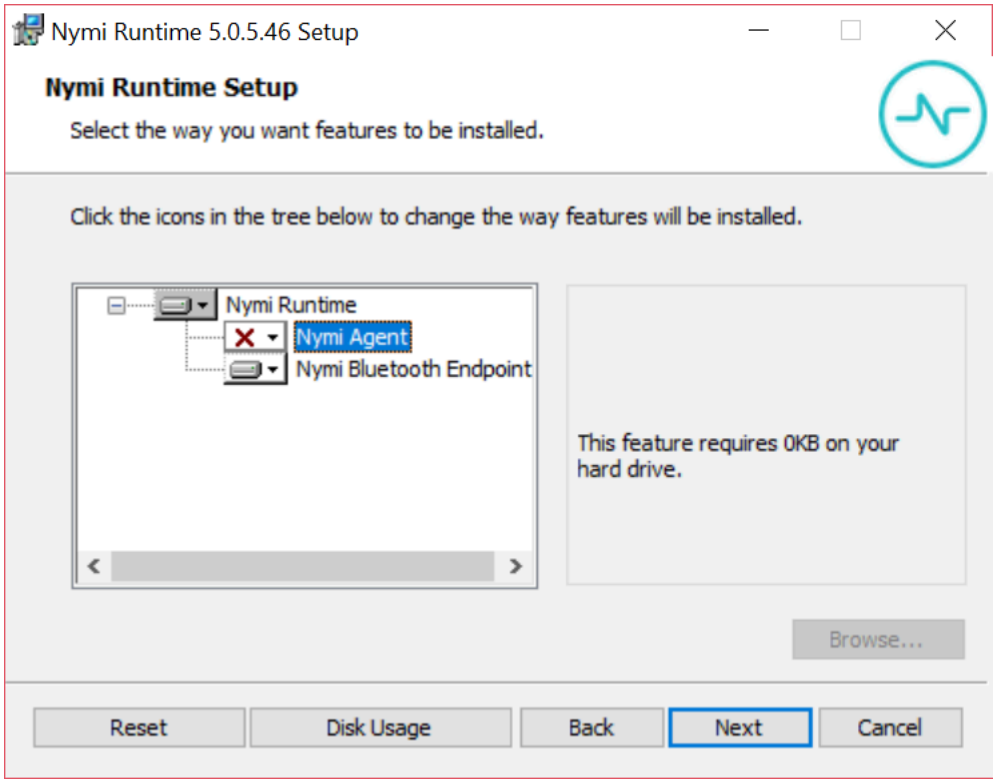


Figure 5: Nymi Agent feature is not available

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

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.default.toml* file (On HP Thin Pro, */usr/bin/nbe.default.toml*), and name the file *nbe.toml*.
2. Edit the *nbe.toml* file with a text editor.
3. Edit the 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.

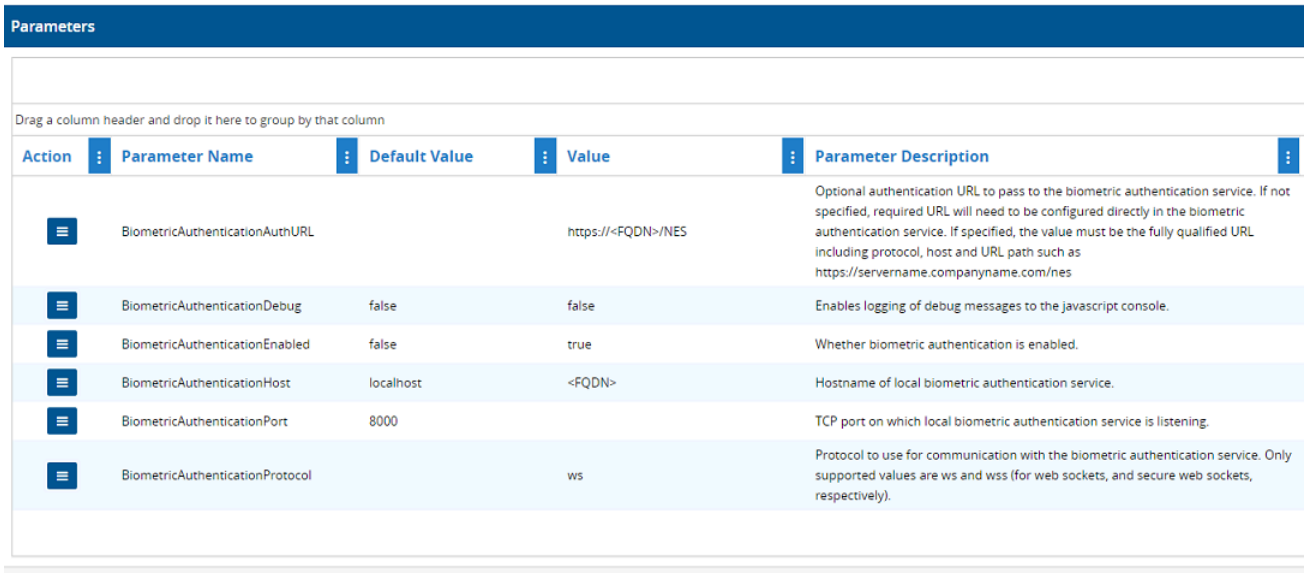
4. Save the *nbe.toml* file.
5. Restart the `Nymi Bluetooth Endpoint` service.

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 6: 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 7: POMSnet Aquila web page`

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

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