APEM MOC/Mobile Integration Guide

Nymi with AspenTech

v1.0

2024-11-19

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 Connected Worker Platform with AspenTech APEM MOC/Mobile Integration Guide This document provides detailed guidance on the deployment and operation of the Nymi-AspenTech integration, to ensure secure, efficient, and compliant industrial processes.

Audience

This guide provides information to NES and AspenTech Administrators. An NES and AspenTech Administrator is the person in the enterprise that manages the Connected Worker Platform with the AspenTech APEM MOC/Mobiles application 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	November 19, 2024	First release of this document.

Related documentation

- **Nymi Connected Worker Platform—Overview Guide**

  This document provides overview information about the Connected Worker Platform (CWP) solution, such as component overview, deployment options, and supporting documentation information.
- **Nymi Connected Worker Platform—Deployment Guide**

  This document provides the steps that are required to deploy the Connected Worker Platform solution.

  Separate guides are provided for authentication on iOS and Windows device.
- **Nymi Connected Worker Platform—Administration Guide**

This document provides information about how to use the NES Administrator Console to manage the Connected Worker Platform (CWP) system. This document describes how to set up, use and manage the Nymi Band™, and how to use the Nymi Band Application. This document also provides instructions on deploying the Nymi Band Application and Nymi Runtime components.

- **Connected Worker Platform Release Notes**

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

How to get product help

If the Nymi software or hardware does not function as described in this document, you can submit a support ticket to Nymi, or email support@nymi.com

How to provide documentation feedback

Feedback helps Nymi to improve the accuracy, organization, and overall quality of the documentation suite. You can submit feedback by using support@nymi.com

AspenTech-Nymi Solution Overview

The AspenTech-Nymi Solution is a direct integration solution that improves identity verification and access control within the Aspen Production Execution Manager MOC v14.5 and Aspen Production Execution Manager Mobile v14.5 applications.

The AspenTech-Nymi Solution allows the AspenTech applications to natively recognise and interact with the Nymi Connected Worker Platform solution and the Nymi Band, to enable real-time, continuous authentication without the need for traditional methods like passwords or key cards. This direct integration ensures that security is maintained without compromising the user experience, while also supporting full compliance with industry regulations.

Users access the AspenTech-Nymi integrated application through their user terminal. After the user authenticates to their Nymi Band, the AspenTech system continuously verifies their identity, and validates their presence across the AspenTech environment, to ensure safe interaction with critical systems.

Deployment Overview

The AspenTech-Nymi Solution requires you to:

- Deploy the Nymi solution with at least one instance of the Nymi Agent in a centralized location.
- Enable the Nymi Agent to use Nymi WebAPI for websocket (ws) or secure websocket (wss) communications.
- Configure the user terminals to use the centralized Nymi Agent.

The following figure provides a high level overview of the components in the Nymi-AspenTech solution.

Components in the AspenTech-Nymi Solution

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

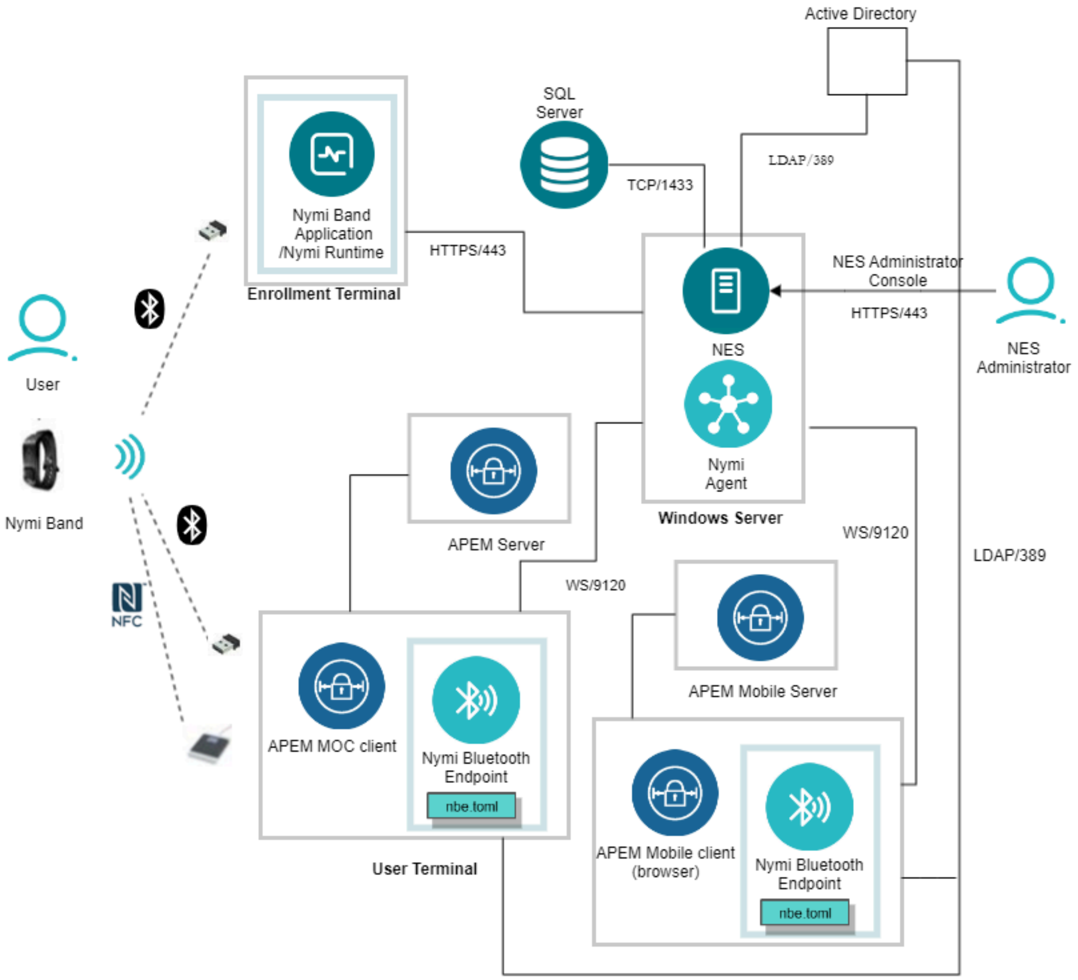


Figure 1: AspenTech-Nymi Solution components and connection ports in a Centralized Nymi Agent Configuration

The AspenTech-Nymi Solution consists of the following components.

Table 2: AspenTech-Nymi Solution Components

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.
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.
User Terminal	Windows 10 or Windows 11 endpoint on which you install Nymi components that allow users to perform authentication tasks with the Nymi Band. Users can perform Nymi Band taps to complete authentication tasks with a supported NFC reader or the Nymi-supplied Bluetooth Adapter. On a thick client user terminal, you install the APEM client software to communicate with the APEM server. On a thin client user terminal, you use a web browser to access the APEM Mobile server.
Nymi Bluetooth Endpoint	Nymi Runtime component that you install on each user terminal. Provides an interface between the Bluetooth Adapter (BLE) and the Nymi Agent. You deploy Nymi Bluetooth Endpoint 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	Use *nbe.toml* file to declare the hostname of the centralized Nymi Agent and optionally, an "endpoint_id", which identifies uniquely identifies the user terminal in both the Aspen Tech and Nymi systems.

Component	Description
Centralized Nymi Agent	Nymi Runtime component that you install in a central location on a single machine or a cluster of two or more machines that is accessible to all user terminals, for example on the server with the NES application. 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. 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.
APEM Server / APEM Mobile Server	Server that: • Receives authentication requests from the Nymi Band through the Nymi Agent. • Processes the requests and uses the Aspen Tech system to verify the identity of the user. • Returns a response based on the authentication status of the user.

Deployment of the Nymi WebAPI

You can deploy the Nymi WebAPI in a centralized or decentralized Nymi Agent configuration.

In a decentralized Nymi Agent configuration, you deploy Nymi Agent and Nymi Bluetooth Endpoint components on each workstation to access a locally installed Nymi-enabled Application(NEA).

In a centralized Nymi Agent configuration, for example, when you use the Nymi Band with Citrix and RDP published applications or desktops, you install:

- Nymi Agent component on a server that multiple workstations can access, such as the Nymi Enterprise Server(NES) server.
- Nymi Bluetooth Endpoint component on each workstation.

Note: For more information about how to deploy a centralized Nymi Agent see the *Nymi Connected Worker Platform—Deployment Guide*.

The Nymi Bluetooth Endpoint and NEA must know the identity of the workstation to which the application wants to connect. By default, this identity is the IP address of the workstation. When you deploy Nymi Agent locally on the client workstation, both components use the loopback address, so they will connect automatically. When you deploy a centralized Nymi Agent, the Nymi Agent subscribes the Bluetooth Endpoint, the Nymi DLL, and WebSocket connections to the Nymi WebAPI by using the source IP of the connection. Therefore, if the Bluetooth Endpoint and application that is using the Nymi WebAPI are on the same host the application will work on connection.

For deployments in an RDP/Citrix environment or when the MES application (NEA) resides on a different host (such as a web or application server), the The IP address of the client that runs the NEA is different from the IP address of the workstation. Therefore, ensure that the NEA can determine the IP address of the client workstation that runs the Nymi Bluetooth Endpoint. You can determine the IP address by using the source IP address of the client requests.

- In remote desktop sessions, the IP address is usually available through Windows Terminal Services APIs.
- If you are not using RDP or Citrix, the IP address is usually available through vendor-specific environments or APIs.
- For remote applications, such as web-based application, you can determine the IP address by using the source IP address of the client requests.

When the application determines the IP address of the client workstation, the application must use the **subscribe** operation to connect to the correct Nymi Bluetooth Endpoint. Keep in mind that multiple IP addresses on the user workstation or NAT between components can interfere with determining client IP addresses and should be taken into consideration during deployment of an application.

If users might move between two or more client workstationsiOS devices, they must terminate their session before switching to another workstation, or the application must take this into account and start a new **subscribe** operation after reconnection.

Use Cases

A user can use their authenticated Nymi Band to perform Nymi Band taps on a supported NFC reader or the Nymi-supplied Bluetooth adapter to complete the following authentication tasks:

- Sign into AspenTech applications.
- Perform e-signatures.

Preparing for an AspenTech-Nymi Solution Deployment

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

The AspenTech-Nymi Solution supports the following application versions:

- Aspen Production Execution Manager MOC v14.5
- Aspen Production Execution Manager Mobile v14.5 applications
- Connected Worker Platform 1.16.0

The following user terminal versions were tested:

- Windows 11 Enterprise 22000.194
- Windows 10 Enterprise 10.0.18362

You can access the ApsenTech user interface from a Chrome or Microsoft Edge browser.

Network and TCP Port Requirements

Review this section for network and TCP Port requirements for the Nymi solution.

Network Requirements

If you use a load balancer in your environment, ensure that you configure the Nymi Agent server in Active/Passive mode.

TCP Port Requirements

The following table summarizes the TCP port requirements for the AspenTech-Nymi Solution deployment.

Table 3: Connection Port Requirements

Purpose	Protocol	Connecting From	Connection To	Port
SQL Access	MS SQL Proprietary	NES	SQL Server	1433/TCP

Purpose	Protocol	Connecting From	Connection To	Port
Manage Nymi AUDA+ Partner configurations	HTTP/HTTPS	PAS-X AUDA+ Interface	Auda+ Partner server	• 80 (For HTTP) • 443 (for HTTPS)
LDAP Access-Active Directory(AD)	LDAP/LDAPS	NES	AD Server	• 389/TCP (For LDAP configurations) • 636/TCP (For LDAPS configurations)
NES Communications	HTTPS	• All User Terminals (thick). • RDP/Citrix server that run NEAs • Centralized Nymi Agent	NES	443/TCP
Supports Centralized Nymi Agent communications.	Websocket	• All User Terminals (thick and thin) • RDP/Citrix Servers that run NEAs	Centralized Nymi Agent	9120/TCP

Nymi WebAPI Configuration Requirements

Review the following requirements for the Nymi WebAPI and Nymi Agent components:

- Provide access to a distinct port for each component, port numbers are described in this document.
- Configure transport layer security on the server or by offloading.
- Ensure that both components have connectivity to NES.
- Ensure that there is no Network Address Translation (NAT) between the Nymi WebAPI of the Nymi Agent and the user terminals.
- When you use a centralized Nymi Agent on the same server as NES, ensure that each component can co-locate with the NES (ensure that you use distinct TCP ports).

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.

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.

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.

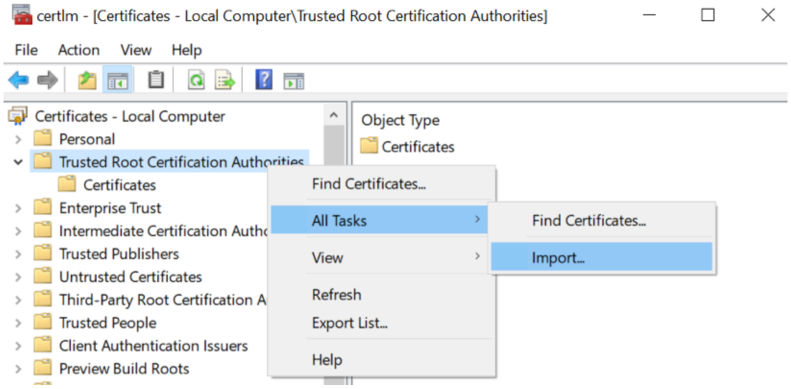
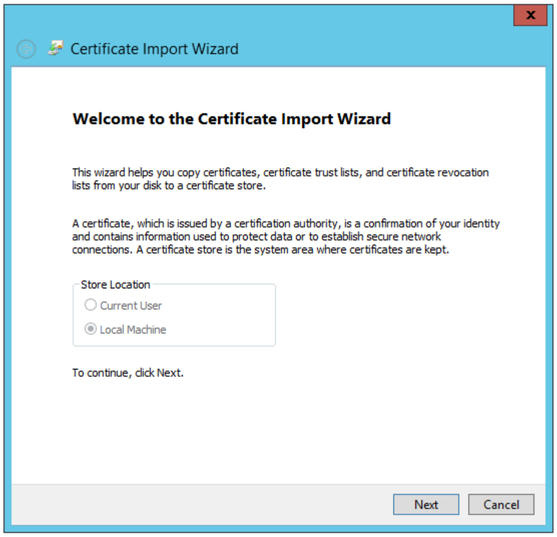

certlm - [Certificates - Local Computer\Trusted Root Certification Authorities]
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root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

Figure 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.



Welcome to the Certificate Import Wizard

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

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

Store Location

○ Current User

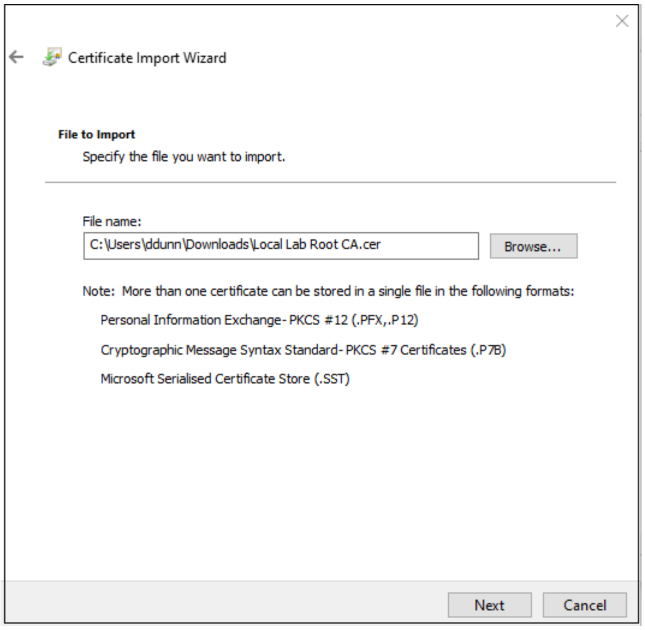
● Local Machine

To continue, click Next.

Figure 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.



File to Import

Specify the file you want to import.

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

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

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

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

Microsoft Serialised Certificate Store (.SST)

Figure 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`**.

Install Nymi Agent on a Centralized Server

You can install the Nymi Agent software with the installation wizard or silently from a command prompt.

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.

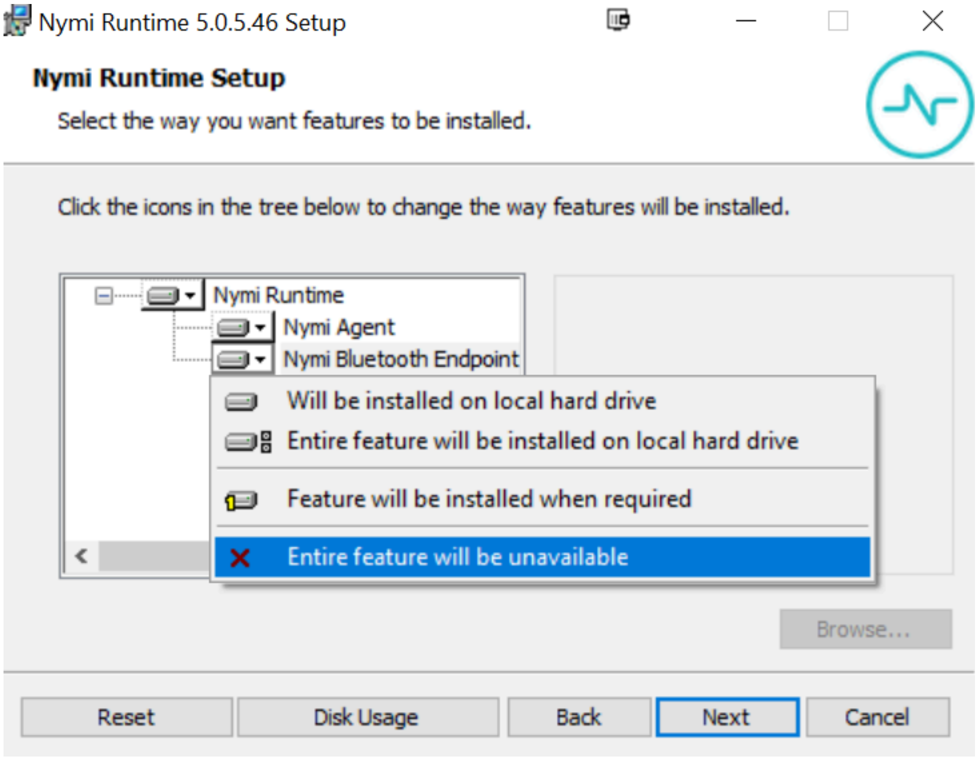
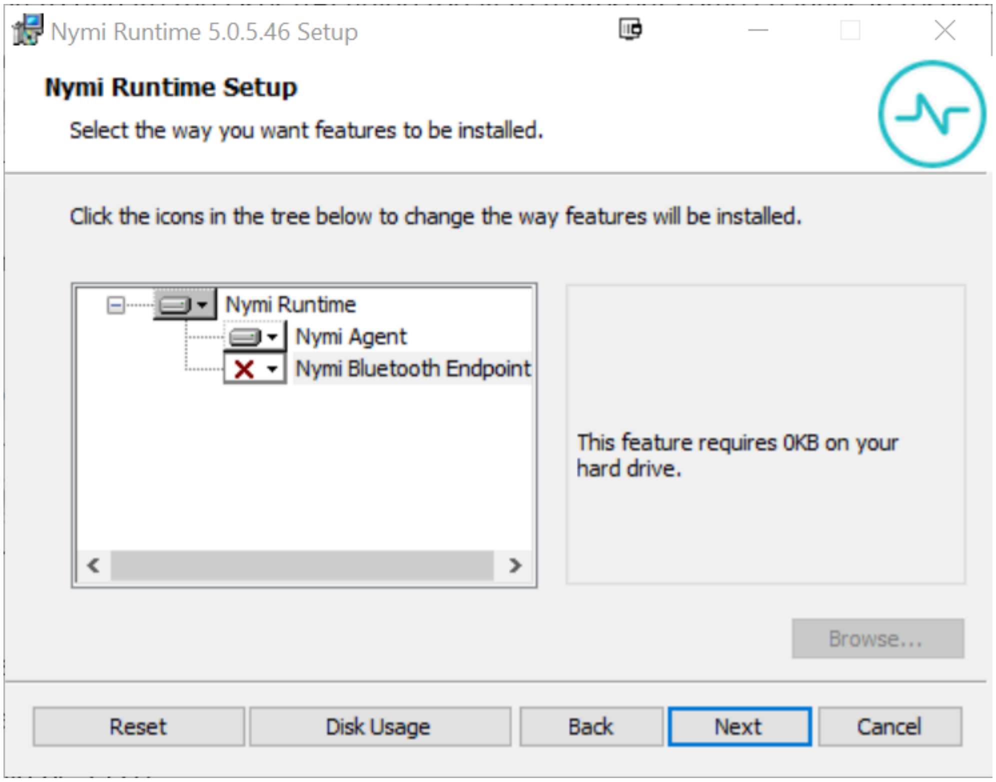

Nymi Runtime 5.0.5.46 Setup
Nymi Runtime Setup
Select the way you want features to be installed.
Click the icons in the tree below to change the way features will be installed.
Nymi Runtime
Nymi Agent
Nymi Bluetooth Endpoint
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Feature will be installed when required
Entire feature will be unavailable
Browse...
Reset
Disk Usage
Back
Next
Cancel

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`**.



Nymi Runtime 5.0.5.46 Setup

Nymi Runtime Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- Nymi Runtime
  - Nymi Agent
  - ☒ Nymi Bluetooth Endpoint

This feature requires 0KB on your hard drive.

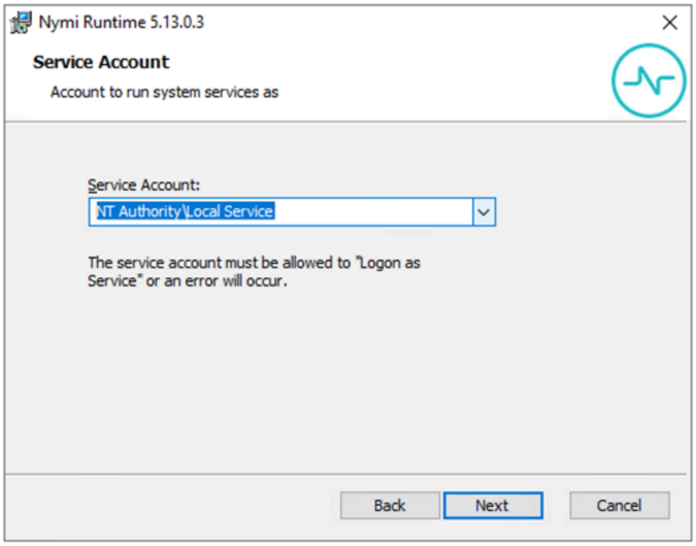
Figure 6: Nymi Bluetooth Endpoint feature is not available

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.



Nymi Runtime 5.13.0.3

Service Account

Account to run system services as

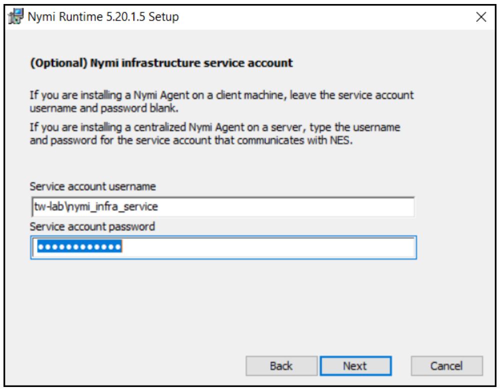
Service Account: NT Authority\Local Service

The service account must be allowed to "Logon as Service" or an error will occur.

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

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



Nymi Runtime 5.20.1.5 Setup

(Optional) Nymi infrastructure service account

If you are installing a Nymi Agent on a client machine, leave the service account username and password blank.

If you are installing a centralized Nymi Agent on a server, type the username and password for the service account that communicates with NES.

Service account username: tw-lab\nymi_infra_service

Service account password: ••••••••••••

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
- Public key

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

Performing a Silent Nymi Agent Installation or Update

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. You can install the Nymi Agent silently by typing one of the following commands:

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

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

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

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

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

   Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.
2. Perform the following steps to ensure that the Nymi Agent uses the Nymi Infrastructure Service Account to communicate with Nymi Enterprise Server(NES).
   a) Create a text file named *creds.txt* that contains two lines:
      - Username of the Nymi Infrastructure Service Account
      - Password of the Nymi Infrastructure Service Account

   b) Open a Command prompt with the **`Run as Administrator`** option.

   c) From the command prompt change to the *C:\Nymi\NymiAgent\Tools* directory, and type the following command:

      cryptoutil.exe encrypt-service-account -i C:\Nymi\NymiAgent\creds.text -o C:\Nymi\NymiAgent\

      The *Cryptoutil* tool 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

   d) Permanently delete the *C:\Nymi\NymiAgent\creds.txt* file.

Configuring the Nymi Agent

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

About this task

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

Procedure

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

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

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

Parameter and Sample Value	Section Name	Description
protocol = "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.
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"

Parameter and Sample Value	Section Name	Description
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"
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.

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

Parameter and Sample Value	Section Name	Description
protocol = *"wss"* or *protocol* = *"ws"*	[webapi]	Required for Nymi WebAPI. Defines the connection protocol. If your deployment does not use Nymi WebAPI, leave both lines commented out. If your deployment uses Nymi WebAPI, uncomment one of the following lines: • *protocol* = *"wss"* To enable secure websocket connections. • *protocol* = *"ws"* To use plain text websocket connections. **Note:** Requires the configuration of the *cacertfile*, *certfile*, and *keyfile* parameters in the [webapi] section.
port = *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*.

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

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

- CA root certificate bundle in PEM format (when you use a Trusted Root CA only)
- Server certificate in PEM format
- Server certificate private key in PEM format

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

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

Set Up the Enrollment Terminal

You can install the Nymi Band Application on a Citrix/RDP server or install the Nymi Band Application on a thick client enrollment terminal.

Centralized Enrollment Terminal

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.

Decentralized Enrollment Terminal

In this configuration you install the Nymi Band Application and the Nymi Runtime software on a thick client enrollment terminal.

Deploy a Centralized Enrollment Terminal

When you deploy a centralized enrollment terminal, you install the Nymi Band Application on the Citrix/RDP server, and then install the Nymi Bluetooth Endpoint on the thin client that users will access to connect to the Citrix host and perform the enrollment.

Install a Centralized Nymi Band Application

You can install the Nymi Band Application on a Citrix RDP server using the installation wizard or silently.

Install the Nymi Band Application Silently

Before you perform a silent installation of the Nymi Band Application you must install the Nymi Runtime software.

Installing Nymi Bluetooth Endpoint Silently

Procedure

Run a Command Prompt as administrator.

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

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

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

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

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

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

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

What to do next

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

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.

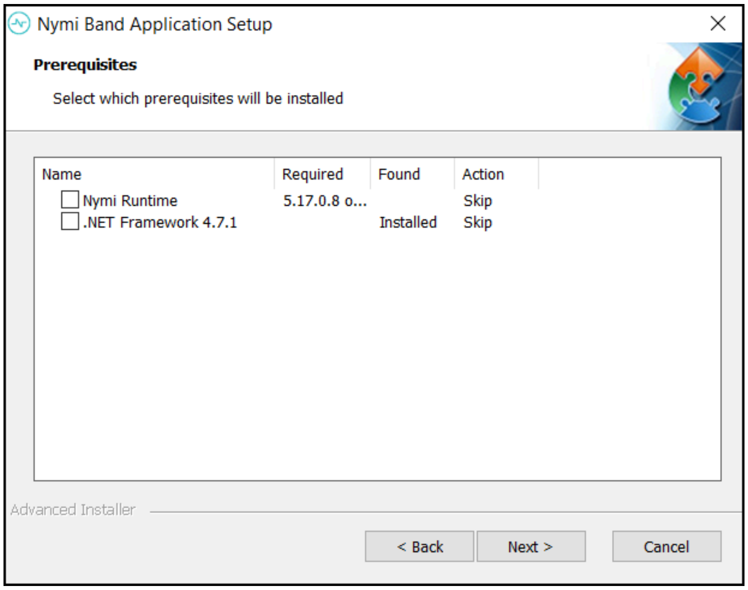
   Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

Installing the Nymi Band Application with the Installation Wizard

Perform the following steps to install the Nymi Band Application.

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`**.



Nymi Band Application Setup

Prerequisites

Select which prerequisites will be installed

Name	Required	Found	Action
☐ Nymi Runtime	5.17.0.8 o...		Skip
☐ .NET Framework 4.7.1		Installed	Skip

Figure 9: 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**.

Editing the Nymi Bluetooth Endpoint Configuration File

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

About this task

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

Procedure

1. Make a copy of the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file (On HP Thin Pro, */usr/bin/nbe.toml*).
2. Edit the *nbe.toml* file with a text editor in administrator mode.
3. Edit the default agent_url parameter and perform the following changes:
    - For WSS:
        - Change the protocol from ws to wss
        - Replace `127.0.0.1` with the FQDN of the centralized Nymi Agent machine.
    - For WS, replace `127.0.0.1` with the IP address of centralized Nymi Agent machine.

    For example, for WSS:

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

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

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

What to do next

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

Deploy a Decentralized Enrollment Terminal

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

Install the Nymi Band Application

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

You can perform a customizable installation or a silent installation.

Install the Nymi Band Application Silently

Before you perform a silent installation of the Nymi Band Application you must install the Nymi Runtime software.

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.

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.

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.

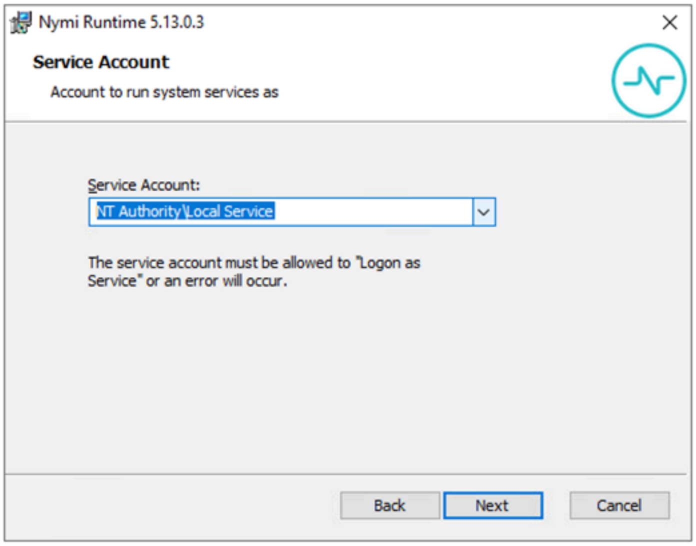
Procedure

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.



The service account must be allowed to "Logon as Service" or an error will occur.

Figure 10: 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.

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`**.

(Optional) Configuring the Communication Protocol

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

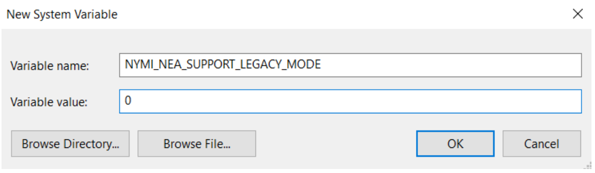
About this task

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

Procedure

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

   The following figure provides an example of the new variable.



New System Variable

Variable name: NYMI_NEA_SUPPORT_LEGACY_MODE

Variable value: 0

Figure 11: New System Variable window

c) Click **OK**.

Set Up User Terminals for Authentication Tasks

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

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

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

  Apple Support provides more information.

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

Bluetooth Adapter Placement

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

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

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

Note: The presence of liquids between the Nymi Band and Bluetooth adapter negatively affects the Bluetooth signal quality. This includes beverages and the human body. If Bluetooth

(BLE) taps behave unexpectedly, consider another placement for the Bluetooth adapter, or edit the Nymi Bluetooth Endpoint configuration file to adjust the signal strength thresholds to perform a BLE tap (see *Edit the nbe.toml File* in the).

Importing the TLS Certificate into Firefox

If you have issued your own TLS root certificate using a private certificate authority (CA), before Firefox can open a WebSocket connection for the NEA, you need to import the TLS certificate.

About this task

See *https://wiki.mozilla.org/CA/AddRootToFirefox* in the Mozilla documentation for more information.

Procedure

1. Open Firefox web browser.
2. In the right pane, navigate to **`Options`**.
3. Select **`Privacy and Security`**.
4. Under **`Certificates`** click **`View Certificates`** and then select **`Authorities`**.
5. Click **`Import`** and select the TLS root certificate from your machine.
6. Click **`OK`**.
7. Run the Nymi WebAPI and open the WebSocket connection by using Firefox.

Importing the Root CA Certificate in Citrix/RDP Environments

Perform the following steps only if the Root CA issuing the NES TLS server certificate is not a Trusted Root CA (for example, if a self-signed TLS server certificate is used for NES). Install the Root CA on each user terminal on which you installed Nymi Bluetooth Endpoint to support the establishment of a connection with the NES host.

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.

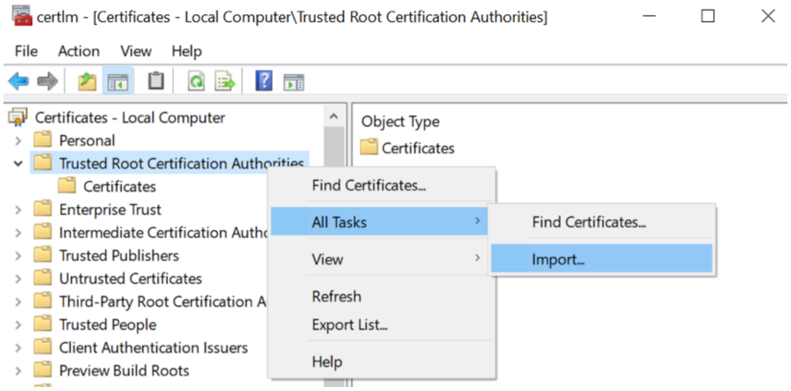
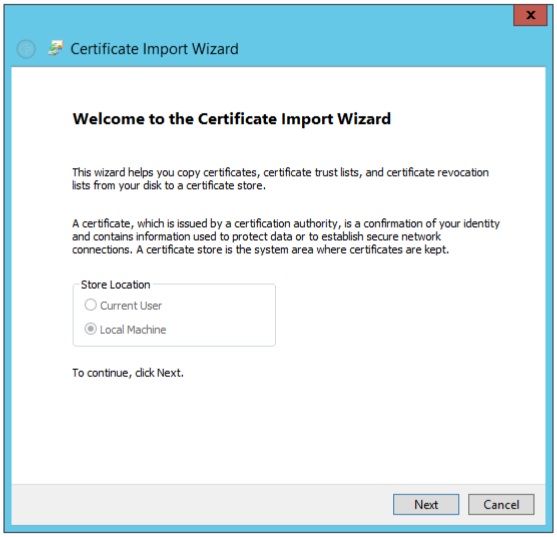

certlm - [Certificates - Local Computer\Trusted Root Certification Authorities]
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root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

Figure 12: certlm application on Windows 10

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

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



Welcome to the Certificate Import Wizard

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

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

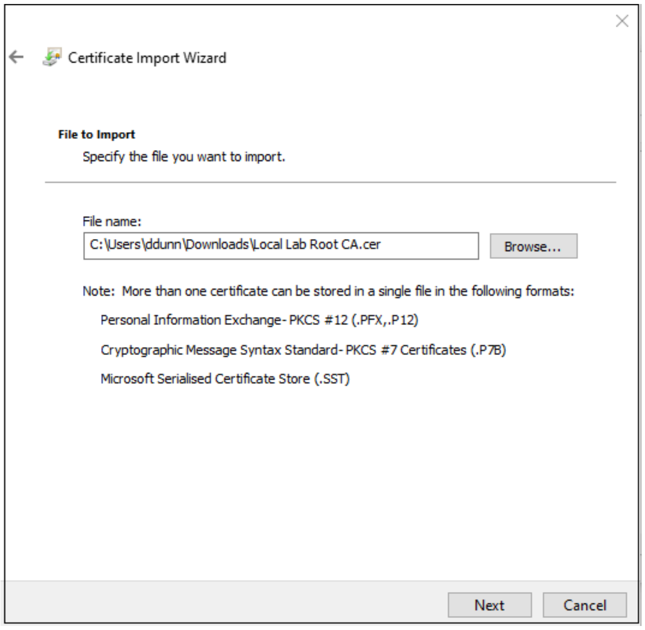
Store Location
○ Current User
● Local Machine

To continue, click Next.

Figure 13: Welcome to the Certificate Import Wizard screen

4. On the `File to Import` screen, click **`Browse`**, navigate to the folder that contains the root certificate file, select the file, and then click **`Open`**.
5. On the `File to Import` screen, click **`Next`**.

   The following figure shows the `File to Import` screen.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

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

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

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

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

Microsoft Serialised Certificate Store (.SST)

Figure 14: File to Import screen

6. On the `Certificate Store` screen, accept the default value **`Place all certificates in the following store`** with the value **`Trusted Root Certification Authorities`**, and then click **`Next`**.
7. On the `Completing the Certificate Import Wizard` screen, click **`Finish`**.

(Windows) Install the Nymi Bluetooth Endpoint

You can install the Nymi Bluetooth Endpoint software with the installation wizard or silently from a command prompt.

Installing the Nymi Bluetooth Endpoint By Using the Installation Wizard

Install the Nymi Bluetooth Endpoint, which is included in the Nymi Runtime installation package, on each Citrix or RDP client in the environment. When you install the Nymi Runtime software, you can choose to install the Nymi Bluetooth Endpoint only.

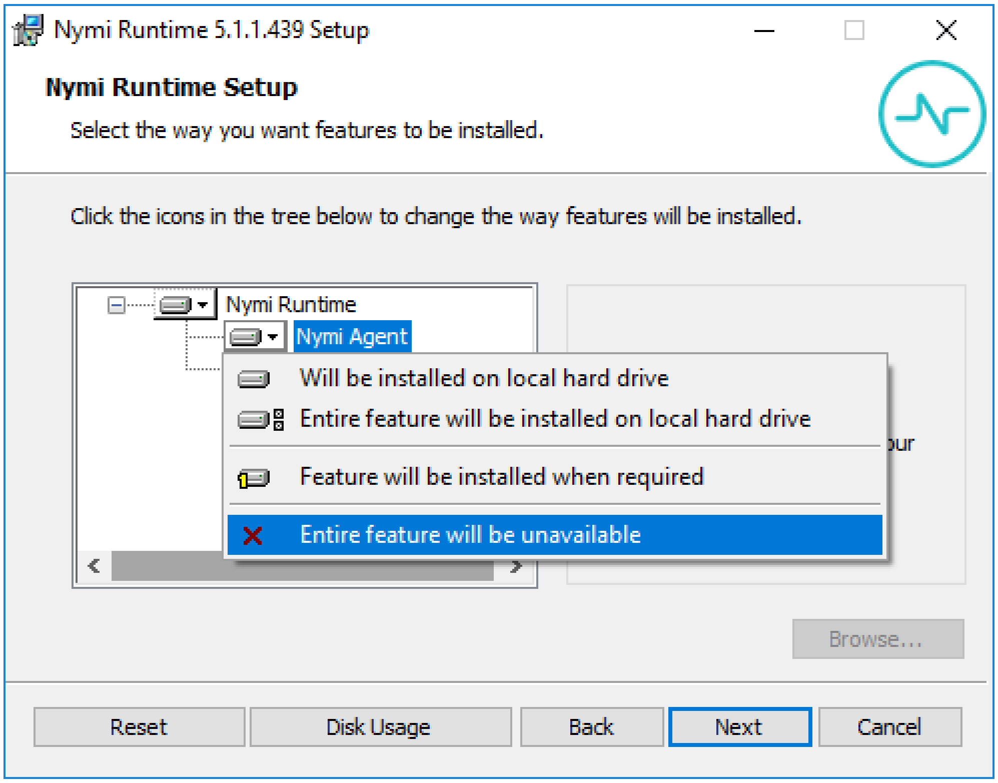
About this task

Perform the following steps to install Nymi Bluetooth Endpoint manually.

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`**.



Nymi Runtime 5.1.1.439 Setup

Nymi Runtime Setup

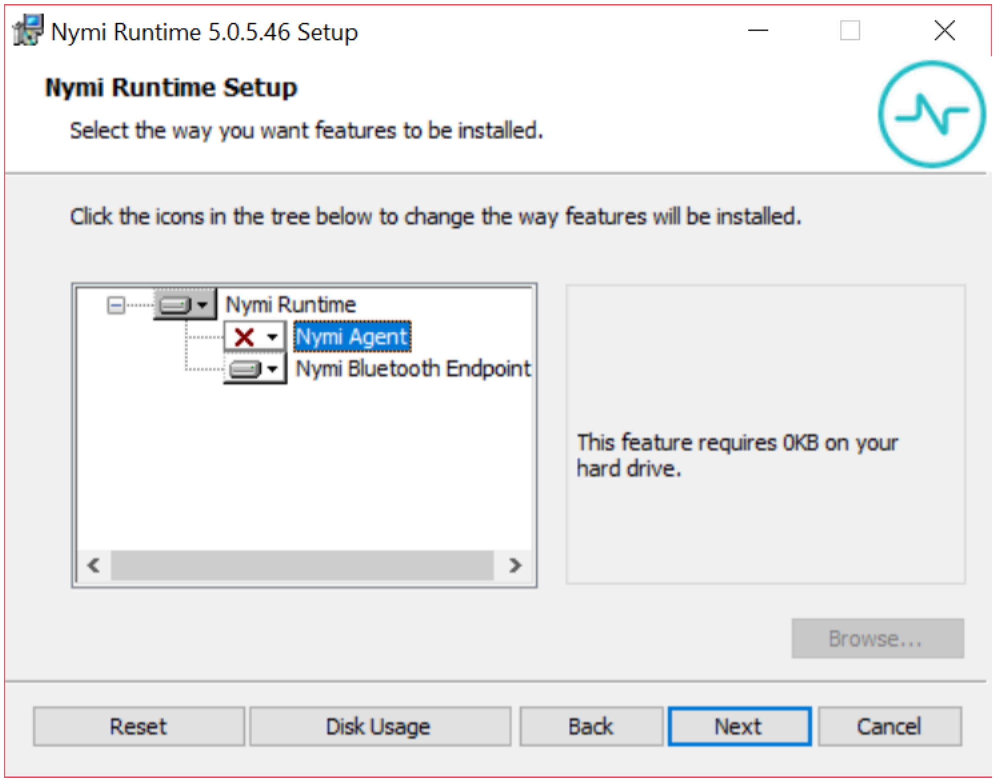
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

Nymi Runtime
Nymi Agent
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Feature will be installed when required
Entire feature will be unavailable
Browse...
Reset
Disk Usage
Back
Next
Cancel

Figure 15: Nymi Agent feature will be unavailable

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



Nymi Runtime 5.0.5.46 Setup

Nymi Runtime Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- Nymi Runtime
  - ☒ Nymi Agent
  - Nymi Bluetooth Endpoint

This feature requires 0KB on your hard drive.

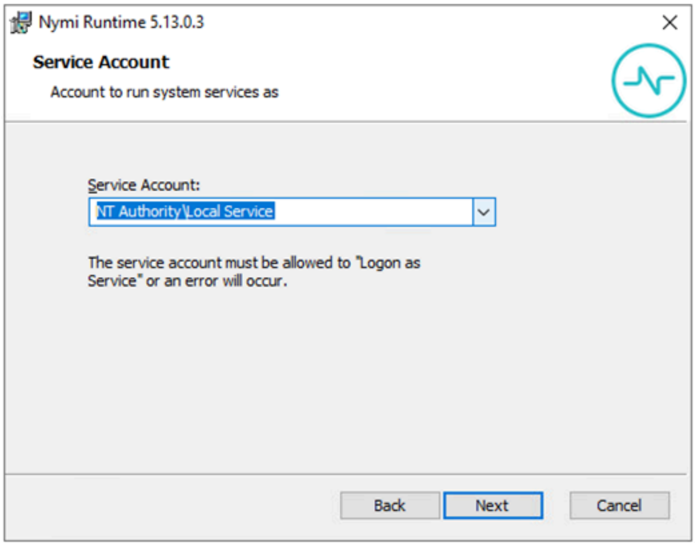
Figure 16: Nymi Agent feature is not available

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`**.

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.



Nymi Runtime 5.13.0.3

Service Account

Account to run system services as

Service Account: NT Authority\Local Service

The service account must be allowed to "Logon as Service" or an error will occur.

Figure 17: Nymi Runtime Service Account window

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

What to do next

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

Installing Nymi Bluetooth Endpoint Silently

Procedure

Run a Command Prompt as administrator.

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

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

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

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

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

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

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

What to do next

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

Editing the Nymi Bluetooth Endpoint Configuration File

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

About this task

Perform the following steps on each user terminal.

Procedure

1. Edit the *nbe.toml* file with a text editor in administrator mode.
2. 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.
3. Optionally, at the end of a file create a new parameter to specify the endpoint ID in the following format:

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

Configuring the Connected Worker Platform Communication Protocol

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

About this task

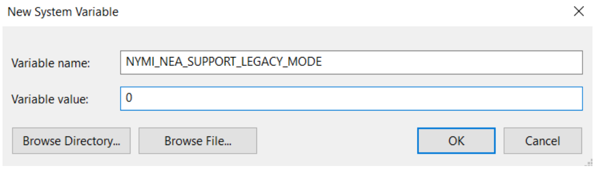
Perform the following steps on all user terminals (for Evidian environments on Wearable user terminals only) where users access Nymi-enabled Applications(NEAs) to disable the legacy protocol. The enrollment terminal only requires the environment variable if users access NEAs on the enrollment terminal.

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

Procedure

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

   The following figure provides an example of the new variable.

   New System Variable

   Variable name: NYMI_NEA_SUPPORT_LEGACY_MODE

   Variable value: 0

   Figure 18: New System Variable window

   c) Click **`OK`**.

Configuring APEM Mobile

Perform the following steps to allow user terminals to use the Nymi Band to complete authentication tasks with APEM Mobile.

Procedure

1. Log into the APEM Mobile console and navigate to the `General Settings` page.
2. Expand **`Nymi Configuration`**
3. **`Nymi Websocket API URL`** field, perform the following steps:
   a) From the list, select the protocol that the user terminals will use to connect to the Nymi Agent server:
      - ws—when you use the websocket protocol
      - wss—when you use the secure websocket protocol

   b) In the **`Please enter IP/Hostname:Port`** field, type the IP address or FDQN of the Nymi Agent and connection port. For example:

      agent.nymi.com:9120
4. Optionally, in the **`Endpoint ID`** field, specify the endpoint ID of the Nymi Bluetooth Endpoint.

Configuring APEM MOC

You can configure APEM MOC to support the Nymi Band by editing a file on the APEM server, which applies to all user terminals, or edit a file on each user terminal, to restrict which user terminals allow a Nymi Band tap.

Procedure

1. To provide Nymi Band support on all user terminals, perform the following steps on the APEM server:
   a) Edit the *C:\Program Files(x86)\AspenTech\AeBRS\cfg_source\path.m2r_cfg* file.

      For x64 MOC, edit the *C:\Program Files\AspenTech\AeBRS\cfg_source\path.m2r_cfg* file.

   b) In the **`NYMI CONFIGS`** section, uncomment the *NYMI_WS_API* parameter and update the value to specify the hostname and port number of your Nymi Agent server.

      For example: ***NYMI_WS_API = ws://agent.nymi.com:9120***

      Note: If you use secure web sockets, change the protocol from *ws* to *wss*.

   c) Save the file.
2. To provide Nymi Enterprise Server support on certain user terminals, perform the following steps on the each applicable user terminal:
   a) Edit the *C:\Program Files\AspenTech\AeBRS\cfg_source\local.m2r_cfg* file.

   b) In the **`NYMI CONFIGS`** section, uncomment the *NYMI_WS_API* parameter and update the value to specify the hostname and port number of your Nymi Agent server.

      For example: ***NYMI_WS_API = ws://agent.nymi.com:9120***

      Note: If you use secure web sockets, change the protocol from *ws* to *wss*.

   c) If required, uncomment the **`NBE_ID`** parameter, and specify the endpoint ID of the user terminal.

   d) Save the file.

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