Integration Guide

Nymi AUDA+ Partner Software
v4.0
2024-12-02

Contents

Preface

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

Purpose

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

The Nymi Auda+ Partner Software Integration Guides provides information about how to configure the Connected Worker Platform and *Audi*+ components to allow authenticated users to use the Nymi Band to perform authentication operations in PAS-X.

Audience

This guide provides information to CWP and Auda+ Administrators. A CWP and Auda+ Administrator is the person in the enterprise that manages the CWP with Auda+ in their workplace.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	April 8, 2024	First release of this document.
2.0	June 20, 2024	Second release of this document. Updates include changes to certificate requirements and the addition of enabling check user status in NES.
3.0	July 29, 2024	Third release of this document. Updates include the addition of steps that describe how to restart the Nymi AUDA+ Partner Software service.

Version	Date	Revision history
4.0	December 4, 2024	Fourth release of this document. Update include revisions to the directory location of the Nymi AUDA+ Partner Software installation and the addition of pre-requisite requirements for the SQL user account.

Related documentation

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

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

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

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

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

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

How to get product help

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

How to provide documentation feedback

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

Nymi AUDA+ Partner Software Deployment Overview

The Nymi Auda+ Partner connector software extends the use of the Nymi Band to provide end-user authentication and e-signatures with Koerber PAS-X versions that support the AUDA + interface for third party authentication systems. All PAS-X versions, including 3.2.7 and later, support the AUDA+ interface for third party authentication systems.

The Nymi AUDA+ Partner Software 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 solution with Nymi AUDA+ Partner Software.

Components in a Centralized Nymi Agent Configuration

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

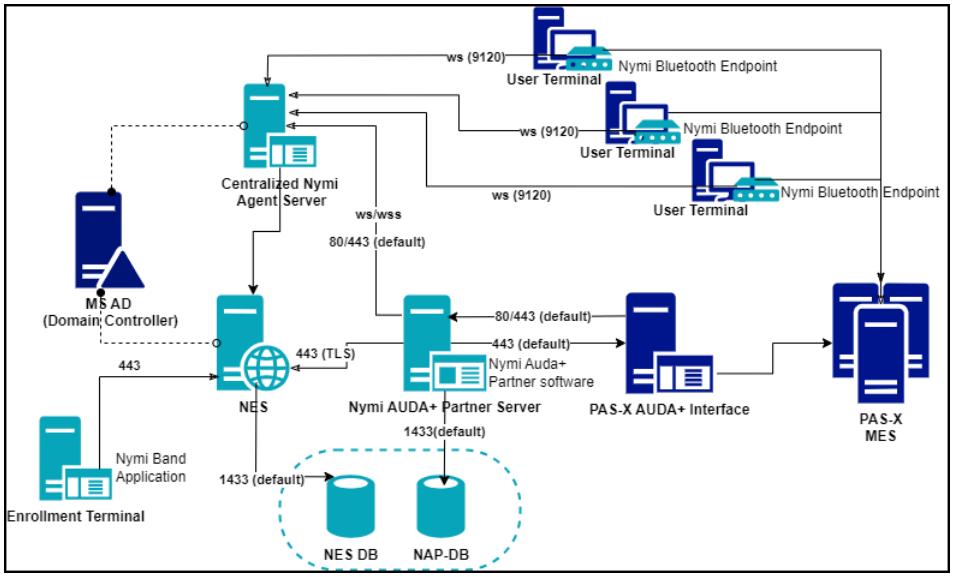

Figure 1: Connected Worker Platform with Nymi AUDA+ Partner Software components and connection ports in a Centralized Nymi Agent Configuration

The Connected Worker Platform with Nymi AUDA+ Partner Software consists of the following components.

Table 2: Connected Worker Platform with Nymi AUDA+ Partner Software Components

Component	Description
Enrollment Terminal	Windows 10 endpoint that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal that you use to enroll a new user and link them to their Nymi Band. The Nymi Band Application requires the Nymi Runtime application, which the Nymi Band Application automatically installs. The Nymi Band Application communicates with the Nymi Band through the Nymi-supplied Bluetooth adapter, which you plug into a USB port on the enrollment terminal.
Nymi Band	A wearable device that 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.

Component	Description
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.
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 Daemon (NBEd) on individual workstations to provide local BLE communication with Nymi Bands through the Nymi-provided BLE Adapter, which you plug into a USB port on the user terminal.
nbe.toml	Configuration file that you create on each user terminal when the solution uses a centralized Nymi Agent. This file defines the hostname on which you installed the Nymi Agent and the connection port on which to communicate with the Nymi Agent.
nbe.toml	Use nbe.toml file to declare the "endpoint_id", which identifies the endpoint uniquiely in both the PAS-X and Nymi systems. The AUDA+ interface requires receive changes on this endpoint with regards to user's authentication state.
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.
Nymi AUDA+ Partner Software	Nymi-provided software that you install in central location on a single machine or in a cluster of two or more machines (in active-passive mode) that is accessible to all user terminals, the centralized Nymi Agent, and the PAS-X AUDA+ server. Provides an interface between the Nymi components and the PAS-X AUDA+ server to support authentication tasks with a Nymi Band tap.
PAS-X AUDA+ Interface	A web application that provides AUDA+ administrators with an interface to manage the PAS-X AUDA+ server configuration.
PAS-X MES	Manufacturing Execution System(MES) that user access to complete authentication tasks. Users can complete tasks such as e-signatures with a Nymi Band tap on an NFC reader or the Nymi-supplied Bluetooth Adapter.

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 the following tasks:

- Log in to the Rockwell FactoryTalk PharmaSuite MES.
- Perform e-signatures within the following Modules:
  - Production Execution Client
  - Production Responses Client
  - Data Manager
  - Production Management Client
  - Recipe & Workflow Designer
  - Production Execution Viewer.

Preparing for an Nymi AUDA+ Partner Software Deployment

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

You can install the Nymi AUDA+ Partner Software on Microsoft Server 2016, 2019, or 2022

The Nymi AUDA+ Partner Software supports the following application versions:

- Koerber PAS-X version 3.2.7 and later
- Connected Worker Platform 1.9.0
- Connected Worker Platform 1.16.0 (pending until testing of the subscribe_identity functionality completes)

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 and Nymi AUDA+ Partner Software server in Active/Passive mode.

TCP Port Requirements

The following table summarizes the TCP port requirements for the Nymi AUDA+ Partner Software deployment.

Table 3: Connection Port Requirements

Purpose	Protocol	Connecting From	Connection To	Port
SQL Access	MS SQL Proprietary	NES	SQL Server	1433/TCP
Manage Nymi AUDA+ Partner configurations	HTTP/HTTPS	PAS-X AUDA+ Interface	Auda+ Partner server	• 80 (For HTTP) • 443 (for HTTPS)

Purpose	Protocol	Connecting From	Connection To	Port
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).

Nymi AUDA+ Partner Software Certificate Requirements

If you use configure the Nymi WebAPI to use secure web sockets, the Nymi AUDA+ Partner Software also requires TLS certificates in PKCS#12 format for secure web socket communications.

If you install the centralized Nymi Agent and the Nymi AUDA+ Partner Software on the same machine as Nymi Enterprise Server(NES), you can use the same TLS certificate fore each component.

If the components reside on different servers, you can use the same TLS certificate for NES, the Nymi AUDA+ Partner Software and the centralized Nymi Agent when the SubjectAlternativeNames includes the FQDN of each component. Ensure that you copy the required TLS certificate files tot the Nymi AUDA+ Partner Software server.

Note: Nymi AUDA+ Partner Software only supports TLS 1.2

The *Nymi Connected Worker Platform—Deployment Guide* provides detailed information about TLS certificate requirements.

Active Directory Requirements

The Nymi AUDA+ Partner Software provides you with a web-based console to manage the system. Nymi AUDA+ Partner Software relies on NES Administrator Active Directory group membership to define users that have administrator access to the Nymi AUDA+ Partner Software console.

Creating the Nymi AUDA+ Partner Software Database

If you use an SQL server that is not on the same machine as NES, install the SQL Server software if required, and then create the Nymi AUDA+ Partner database.

Before you begin

If your SQL server uses SQL authentication, consider the following information when you create the user account:

- In the password, do not use the following characters ***: - ^ * & " < >***
- In the password, do not include the following character sequence ***/!***

- Ensure the account has create, update, delete, read permissions for the database

About this task

Perform the following steps on a machine that has SSMS installed and has access to the SQL Server.

Procedure

1. Open `SQL Server Management Studio (SSMS)`, and then login to the SQL Server.
2. Right-click the SQL instance, and the select **`Properties`**.
3. In the **`Object Explorer`**, select **`Security`**.
4. Select **`SQL Server and Windows Authentication Mode`**, and then click **`OK`**.
5. In the **`Object Explorer`** right-click ***Databases***, and the select ***New Database***.
6. In the `New Database` window, perform the following actions:
   a) In the **`Name`** field, type ***nymiaudadb***.
   b) Click the elipses (...) beside **`Owner`**, and then in the **`Enter the object names to select`** field, type the name of the service account.
   c) Click **`Check names`**.
   d) In the **`Multiple Objects Found`** field, select the service account name, and then click **`OK`**.
   e) On the `Select Database Owner` window, click **`OK`**.
   f) On the **`New Database`** window, click **`OK`**.

Configuring SQL Database for Remote Access

Enable TCP/IP on the SQL instance to allow access to the database.

About this task

Perform the following actions in the `SQL Server Configuration Manager` application.

Procedure

1. In the left navigation pane, expand `SQL Server Network Configuration`, and then select the appropriate Protocols for the SQL Server option.
2. In the right pane, select TCP/IP, and then right-click and select **`Enabled`**.
3. Double-click **`TCP/IP`**.
4. In the `TCP/IP Properties` window, select the **`IP addresses`** tab.
5. Navigate to the `IPALL` section, and then for the **`TCP port`** value, type ***1433***.
   The following figure provides an example of the port setting.

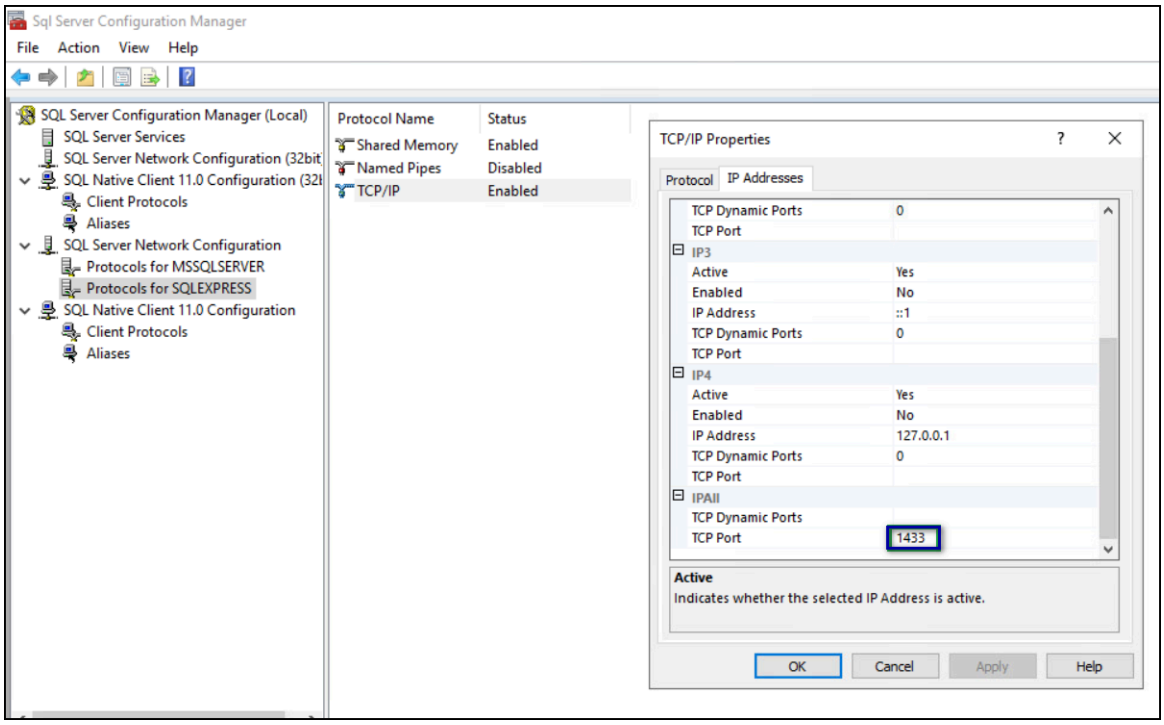

Figure 2: Configuring SQL Port

6. Click **OK**, and then click **Apply**.
7. On the prompt to restart the SQL services, click **OK**.
8. Restart SQL Server services.
9. For SQL Express only, perform the following steps in `SQL Configuration Manager`.
   a) In the left navigation pane, select **`SQL Services`**.
   b) Right-click **`SQL Server Browser`**, and then select **`Properties`**, as shown in the following figure

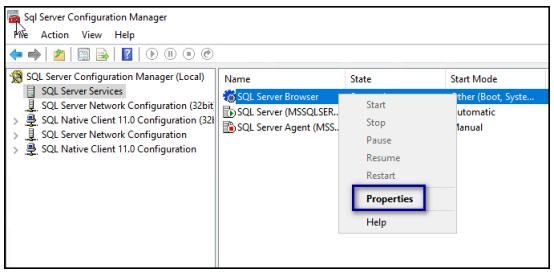

Figure 3: SQL Browser Properties option

   c) On the **`Service`** tab, from the **`Start Mode`** list, select **`Automatic`**, as shown in the following figure.

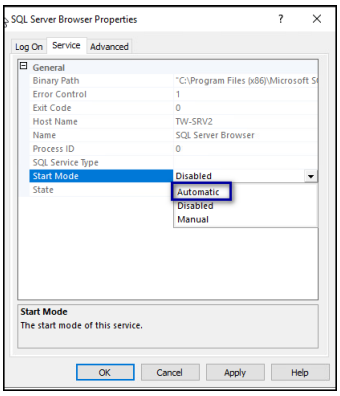

Figure 4: Start Mode

d) Right-click **`SQL Server Browser`** and select **`Start`**.

The SQL Server Browser service state changes to **`Start`**, as shown in the following figure.

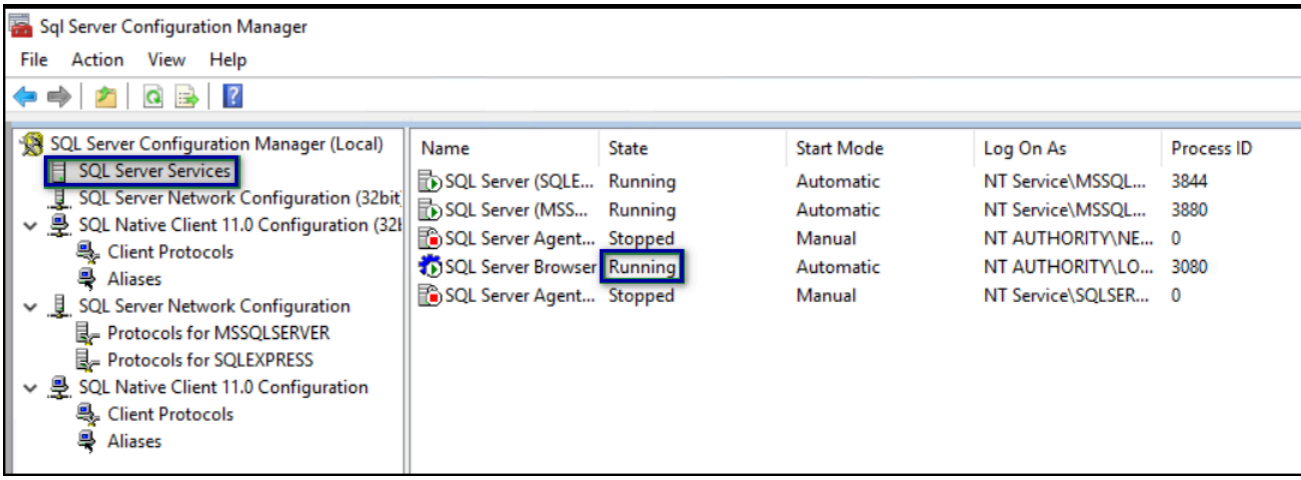

Figure 5: SQL Server Browser service

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.

Configuring Check User Status

Perform the following steps to configure NES to provide the status of a user in active directory to a NEA.

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. In the **`Active Directory`** section, select the **`Check User Status`** option.
   The following options appear to customize the active directory user check.

Option	Description
Cache User Status	• Allows NES to cache the status of a user for the time defined in the **`Cache Expiry`** option. • Default: enabled • When this option is enabled, NES contacts AD on the first user status request and stores the results in cache. When an NEA request the status again, NES retrieves the status from cache. • When this option is disabled, NES does not cache the status of users and requires NES to check the status of users every time NES receives a request from the NEA. When you clear this option, the **`Cache Expiry`** option disappears.

Option	Description
Cache Expiry	• Defines the length of time that the status of the user remains valid in cache. • Default: 15 mins • When NES receives a status request from an NEA, and the length of time that the user status has been stored in cache exceeds the cache expiry value, NES contacts AD for the user status and stores the results in cache again.

Set Up 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.

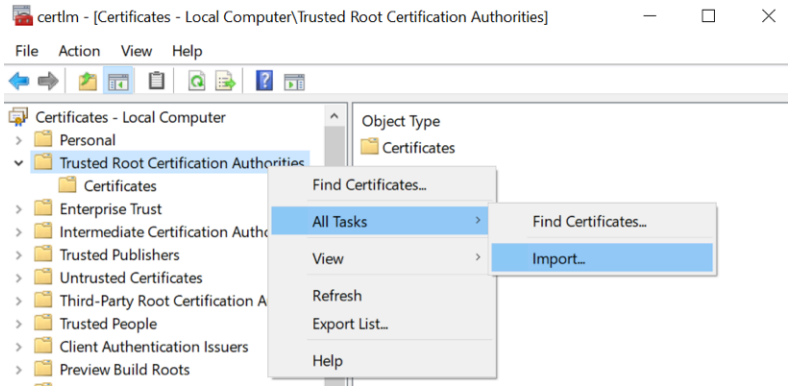

Figure 6: certlm application on Windows 10

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

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

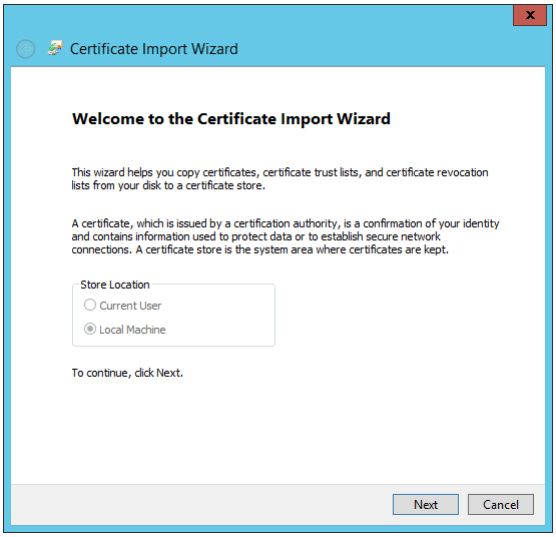

Figure 7: Welcome to the Certificate Import Wizard screen

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

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

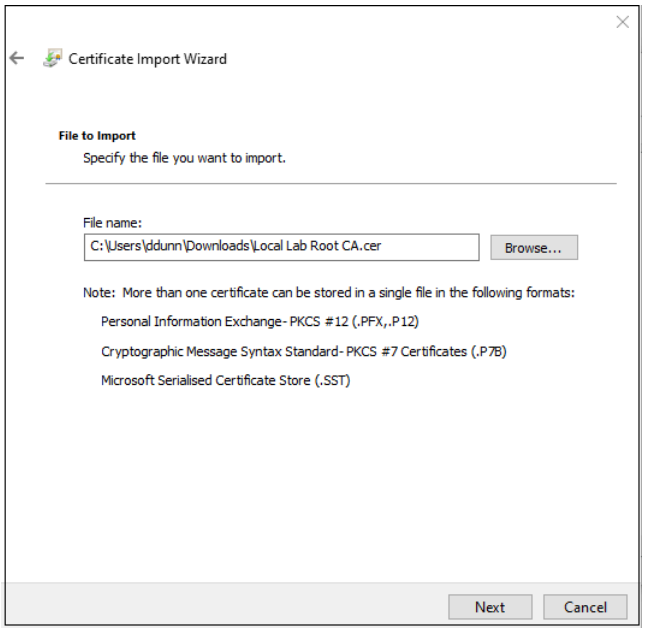

Figure 8: File to Import screen

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.

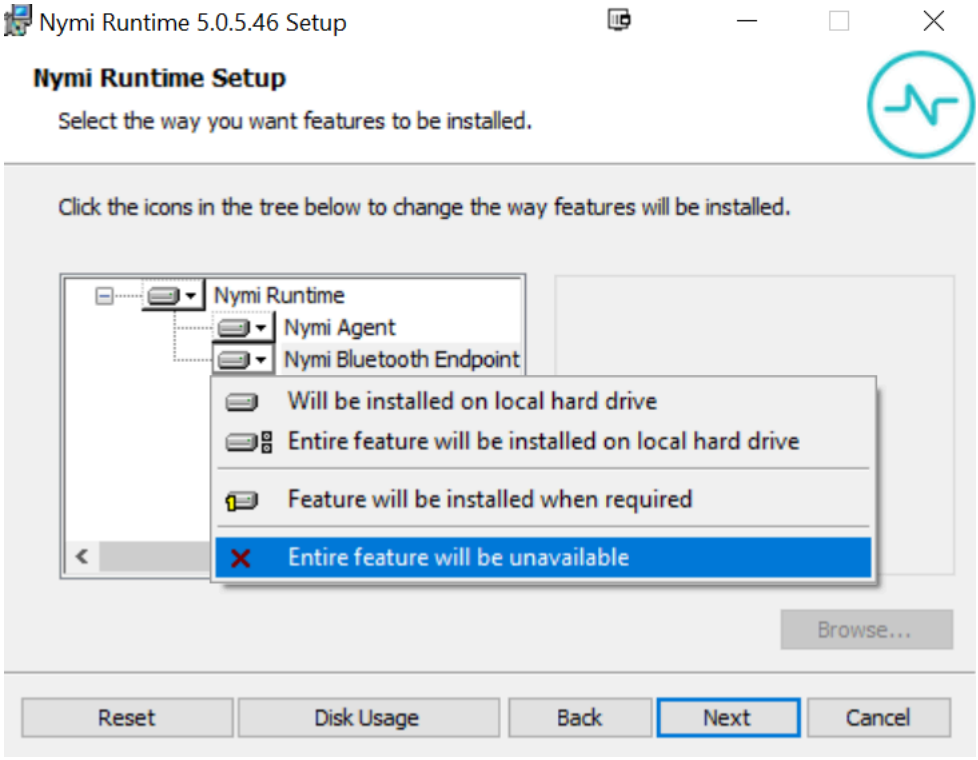

Figure 9: Nymi Bluetooth Endpoint feature will be unavailable

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

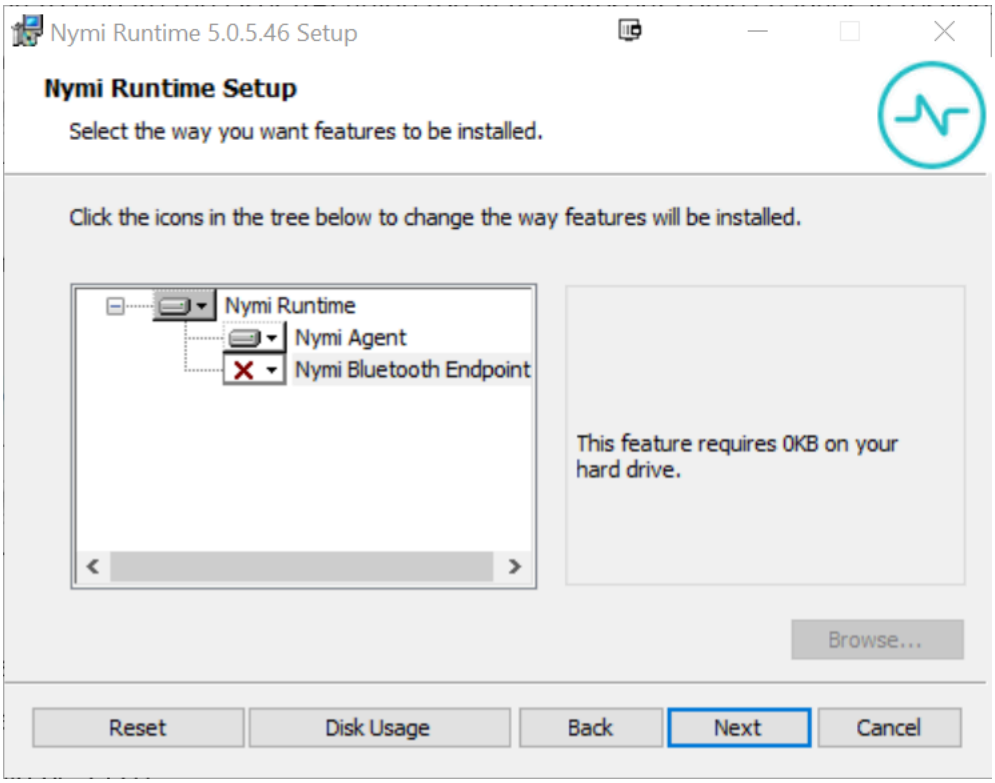

Figure 10: Nymi Bluetooth Endpoint feature is not available

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

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

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

    The following figure shows the `Service Account` window.

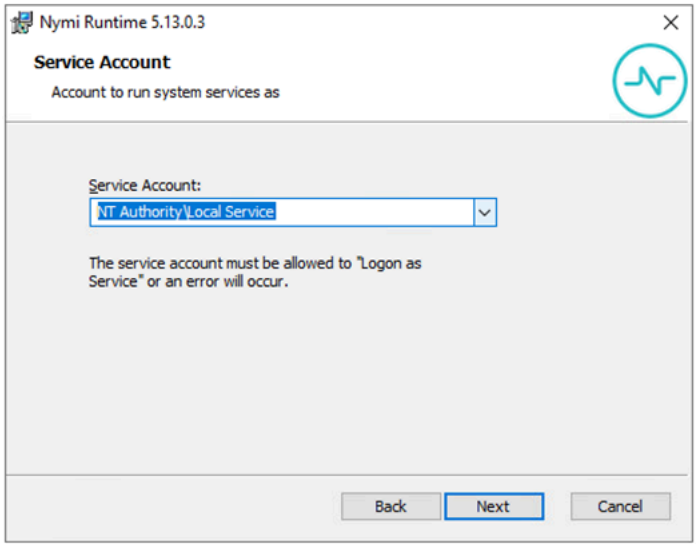

Figure 11: Nymi Runtime Service Account window

11. On the `(Optional) Nymi Infrastructure Service Account` window, specify the username and password of the Nymi Infrastructure Service Account. When you specify the username, include the domain name, for example *tw-lab\nymi_infra_service_acct*. Refer to *Appendix—Record the CWP Variables* for the service account name.

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

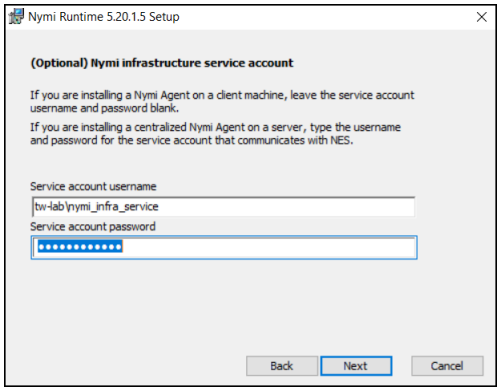

Figure 12: Nymi Infrastructure Service Account window

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`**.

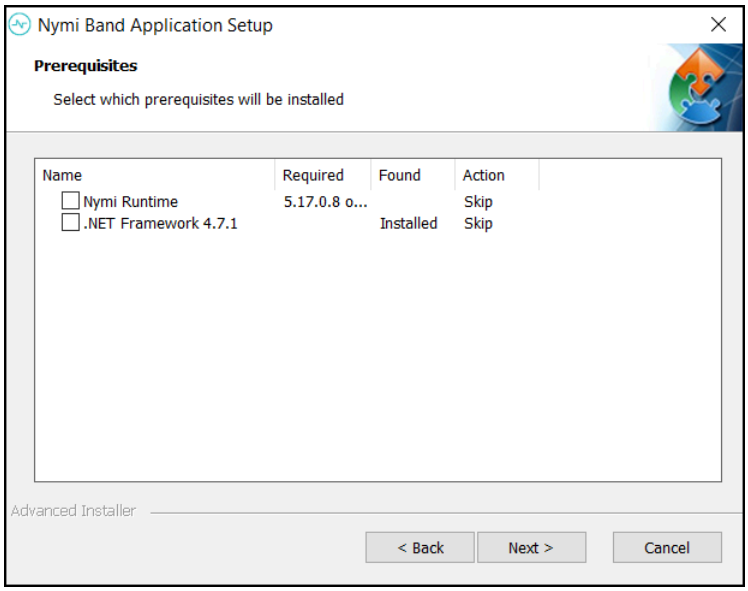

Figure 13: No Nymi Runtime Installation

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.

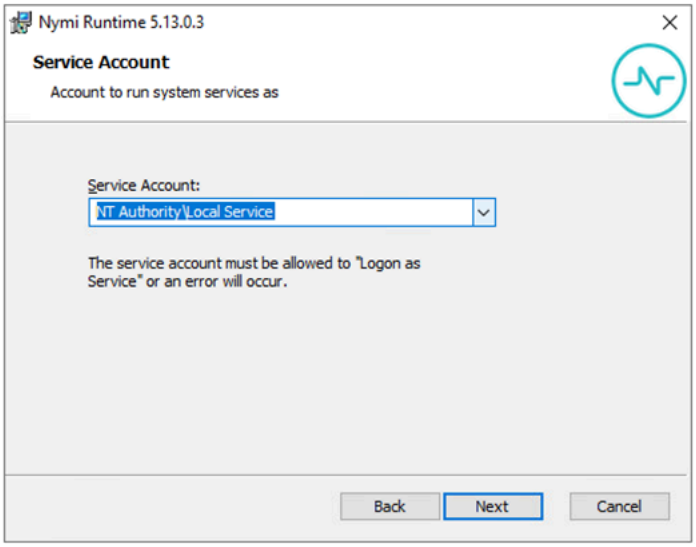

Figure 14: Nymi Runtime Service Account window

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.

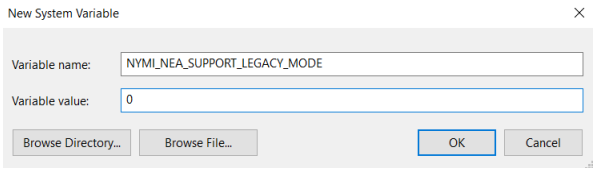

Figure 15: New System Variable window

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.

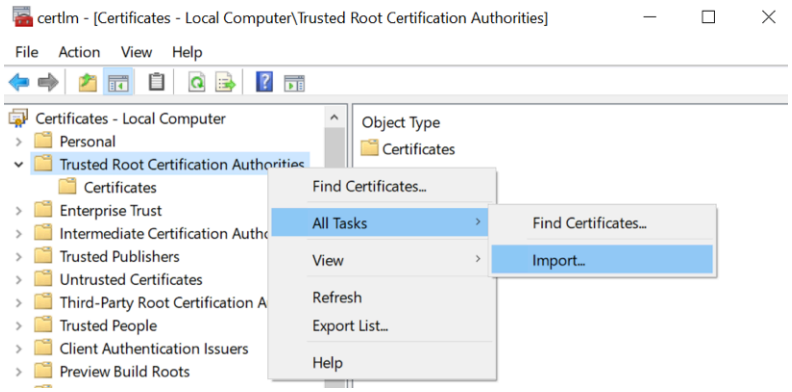

Figure 16: certlm application on Windows 10

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

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

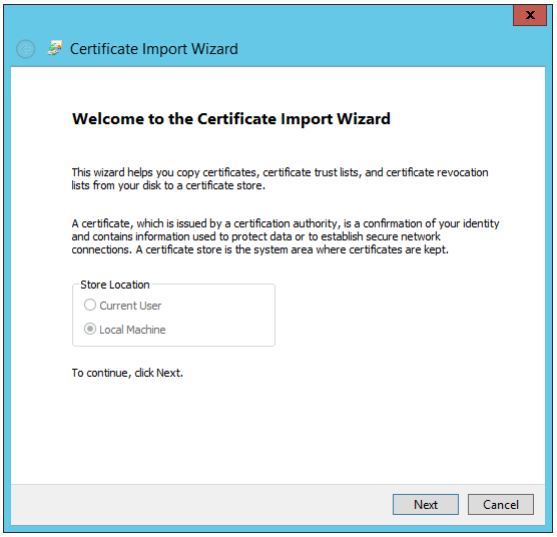

Figure 17: Welcome to the Certificate Import Wizard screen

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

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

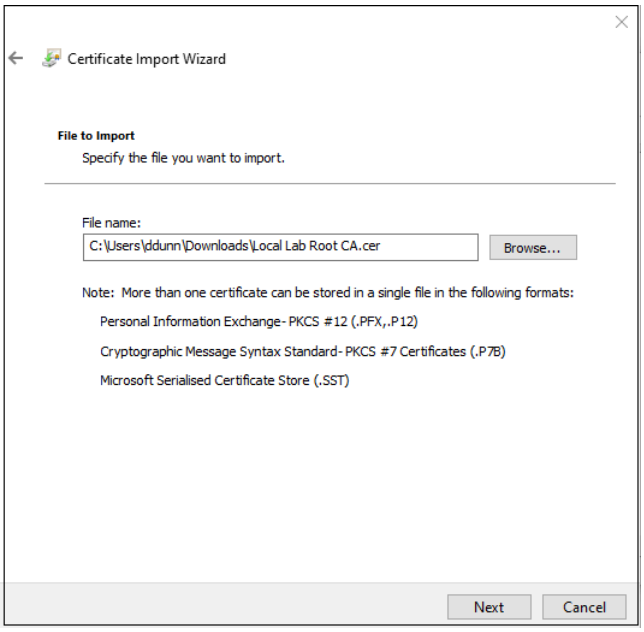

Figure 18: File to Import screen

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`**.

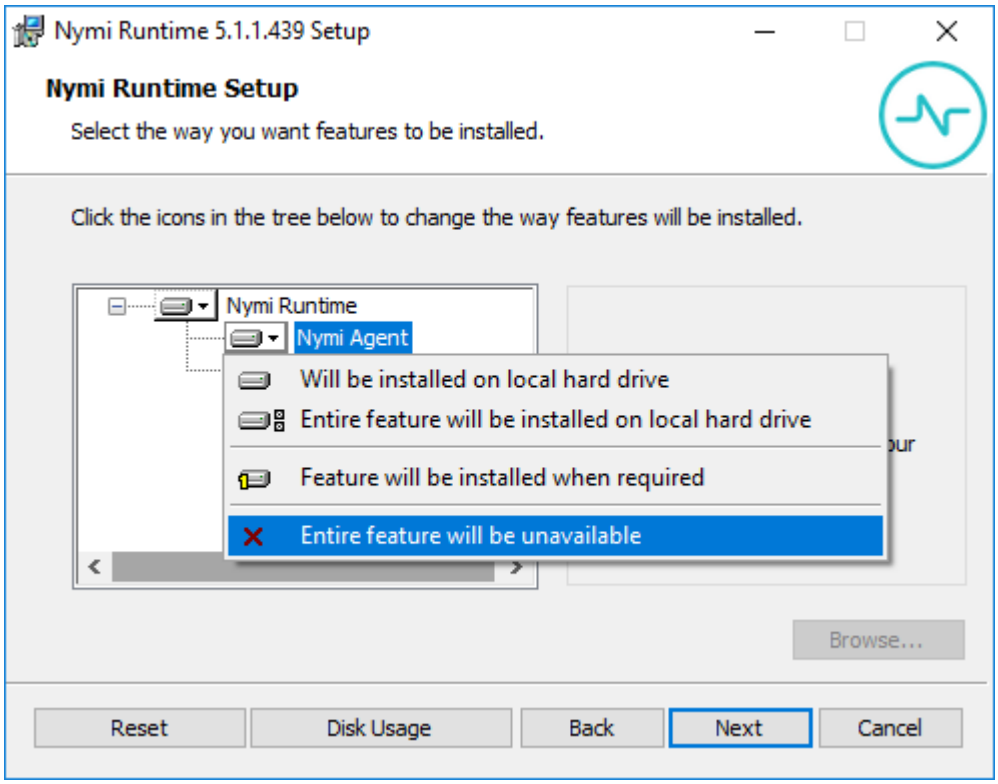

Figure 19: Nymi Agent feature will be unavailable

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

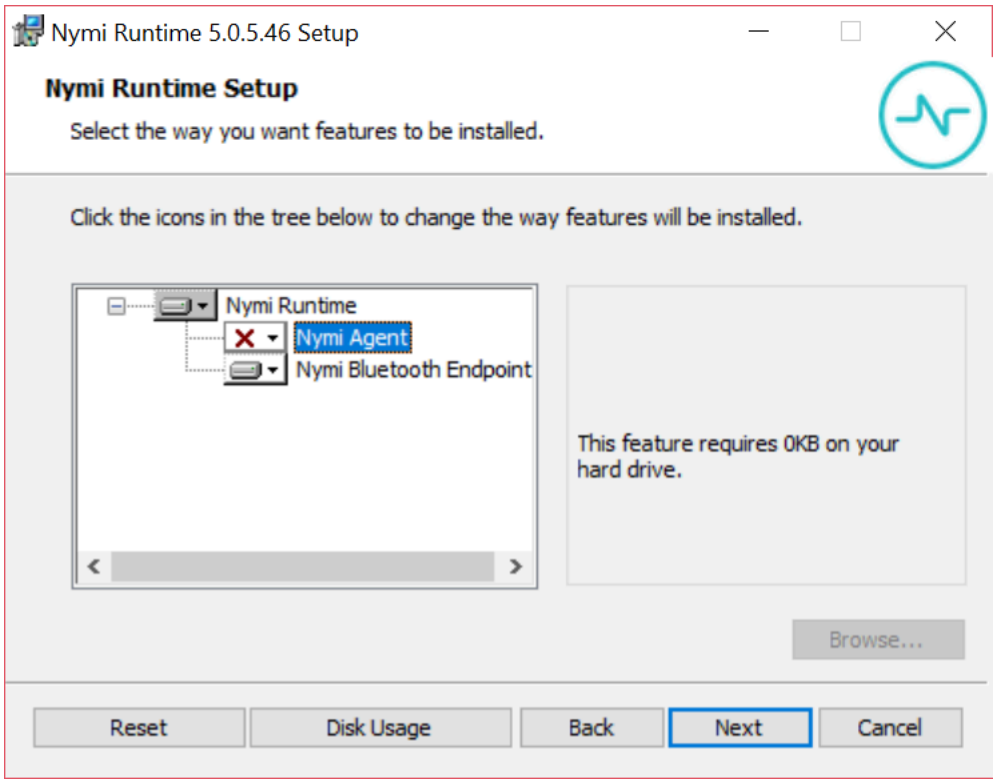

Figure 20: Nymi Agent feature is not available

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.

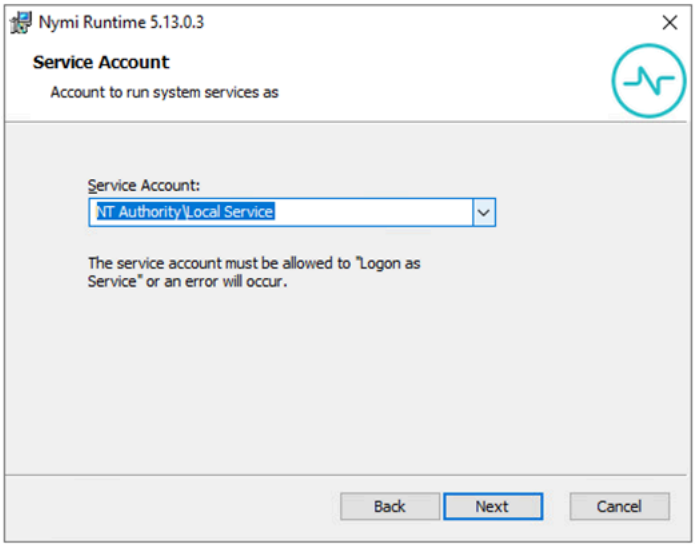

Figure 21: Nymi Runtime Service Account window

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.

(Windows and HP Thin Pro) 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.

   On Windows:

   a. Press the Windows key on the keyboard, or click the start button on the toolbar. Enter "Services" in the search bar. The Services application window appears.
   b. Search for **`Nymi Bluetooth Endpoint`** in the Services application.
   c. Right-click **`Nymi Bluetooth Endpoint`** and restart it.

   On HP Thin Pro:

   a. Stop the Nymi Bluetooth Endpoint service by typing ***killall -9 nbed***.
   b. Start the Nymi Bluetooth Endpoint by typing ***/usr/bin/nbedstart***.
6. On HP Thin Pro only, revert the file system to read-only access.
   a) Open **`X Terminal`**.

b) Type:

```
fslock
```

c) Close the terminal.

7. On HP Thin Pro only, Revert to **User** mode from the system menu, or log in using the credentials of a person in the user domain group.

What to do next

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

Configuring the Connected Worker Platform Communication Protocol

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

About this task

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

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

Procedure

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

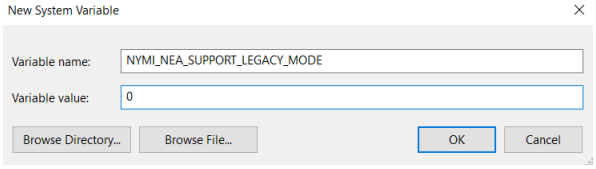

Figure 22: New System Variable window

   c) Click **OK**.

Install and Configure the Nymi AUDA+ Partner Software

Perform the following steps to install the Nymi AUDA+ Partner Software on a server, for example the Nymi Enterprise Server(NES), and configure the software for your environment.

Contact your Nymi Solution Consultant to obtain the Nymi AUDA+ Partner Software.

Importing and Root and Intermediate Certificates

Import the root and intermediate certificates into the Java Development Kit runtime trusted certificate store. To connect with NES, Centralized Nymi Agent, and PAS-X AUDA+ Interface, the Nymi AUDA+ Partner Software requires the root and intermediate certificates.

About this task

Perform the following steps for each root CA and intermediate certificate.

Procedure

1. Extract the Nymi AUDA+ Partner Software package to the *C:\Nymi*.

   Note: The installation process creates files in the *C:\Nymi* folder.
2. From a command prompt, navigate to the *..\jdk\bin* subdirectory of the extracted package.
3. Type ***keytool -import -file `ca_cert_file` -alias `Certificate-ALIAS` -keystore C:\Nymi\nymiaudapartner-`version`\jdk\lib\security\cacerts***

   where:

   - `ca_cert_file` is the name and path of the root or intermediate CA certificate file.
   - `ca_cert_alias` is the alias name of the root or intermediate CA certificate file.
   - `version` is the version name of the package

   For example: ***keytool -import -file C:\Nymi\NymiCerts\NymiCA.cer -alias NymiCA -keystore C:\Nymi\nymiaudapartner-1.0.0-dev.13+master\jdk\lib\security\cacerts***
4. On the **`Enter keystore password`** prompt, type ***changeit***, and then press **`Enter`**.
   The keytool starts the certificate import process and reports the status in the Command Line window.
5. On the **`Trust this certificate`** prompt, type ***Yes***.

Configuring the Nymi AUDA+ Partner Software

Use the Nymi-supplied configuration tool to configure the Nymi AUDA+ Partner Software

About this task

Perform the following steps from a command prompt on the server that will manage the Nymi AUDA+ Partner Software.

Procedure

1. From the command prompt window, navigate to the root of the folder that contains the extracted Nymi AUDA+ Partner Software package.
2. Type *configure.bat*, and then press **Enter**.
3. On the **Enter the NES URL** prompt, type the URL for NES in the following format:
   https://nes_server/NES_service_name/

   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.

   For example ***https://tw-srv1.tw-lab.local/nes***
4. On the **Enter the path to the TLS 'keystore'** prompt, type the absolute path to the TLS keystore file.
   For example: ***C://NymiCerts//TLS.pfx***
5. On the **Enter the port Nymi AUDA+ Partner will listen on** prompt, example port number:

   - 80 — Default port for HTTP
   - 443 — Default port for HTTPS
6. On the **Enter the database host name** prompt, type the FQDN of the MS SQL server.
7. On the **Enter the database port number** prompt, type the port number to connect to the SQL Server. The default port number is 1433.
8. On the **Enter the database instance name** prompt, type the instance name for the Nymi AUDA+ partner database. For example, ***nymiaudadb***.

9. On the **`Enter the database username`** prompt, type the username of an account that has write access to the SQL database.
10. On the **`Enter the database password`** prompt, type the password the user account.
11. On the **`Enable Nymi AUDA+ Partner for identity subscription 'subscribe_identity'`** prompt, type ***y*** when you use Connected Worker Platform 1.15 and later.

    Note: If you enable identity subscription, disable legacy protocol on each user terminal. The section *Configuring the Connected Worker Platform Communication Protocol* in the *Nymi Connected Worker Platform—Deployment Guide* provides more information.
12. On the **`Enter the FQDN for the Nymi Agent`** prompt, type the FQDN of the centralized Nymi Agent server.
13. On the Enter the port number on which the Nymi Agent listens for web socket API connections, refer to *C:\Nymi\NymiAgent\nymi_agent.toml* file for the Centralized Nymi Agent to find out the port number configured for the websocket API:
14. On the **`Is Nymi Agent listening on TLS for WS API connections`** prompt, type one of the following values:
    - Y—If you configured Nymi WebAPI with secure websocket(wss).
    - N—If you configured Nymi WebAPI with websocket(ws).
15. On the **`Enter the URL for the PAS-X AUDA+ URL`** prompt, type the URL to PAS-X AUDA+ in the following format:

    http://*auda_server*:*port*/auda/*version#* where:
    - *auda_server* is the hostname of the PAS-X AUDA+ server.
    - *port* is the port on which to connect to the PAS-X AUDA+ server.
    - *version#* is the version number.

    For example, http://auda.tw-lab.local:9040/auda/V1
16. On the **`Enter the interval in milliseconds for the Nymi Auda Partner to send heartbeat requests`** prompt, type the interval in seconds that the Nymi AUDA+ Partner Software sends an HTTP heartbeat request to the PAS-X AUDA+ URL. Nymi recommends that you set the value to ***50000***.
17. On the **`Press any key to continue`** prompt, press any key.
    The configuration tool installs the software and create the following directories and files at the root of the extracted folder:
    - *conf* folder that contains the configuration file.

      Note: The configuration file contains the values that you provided at each prompt. The database password appears in an encrypted format.
    - *certs* folder that the certificate files.
    - *logs* folder that contains the log file.
18. Close the `Command Prompt` window.

Running the Nymi AUDA+ Partner Software

You can run the Nymi AUDA+ Partner Software as a Windows service or a standalone application. Nymi recommends that you install run the Nymi AUDA+ Partner Software as a Windows service.

Running Nymi AUDA+ Partner Software as a Windows Service

Perform the following steps to configure Nymi AUDA+ Partner Software as a Windows service.

About this task

Procedure

1. Update the PATH variable on the server to include the *C:\Nymi\NymiAudaPartner\jdk\bin* directory.
2. Set the `JAVA_HOME` variable to *C:\Nymi\NymiAudaPartner\jdk\bin*.

   The Nymi AUDA+ Partner Software requires Java Development Toolkit (JDK) and includes the software in the installation package. If your environment already includes JDK 8.0 or later, you can point `JAVA_HOME` to that installed JDK instance location.
3. From a command prompt, navigate to *C:\Nymi\NymiAudaPartner* folder.
4. Type ***NymiAudaPartner.exe install***. On the `User Account Control` dialog, click **Yes**. The executable installs Nymi AUDA+ Partner Software as a Windows service.
5. Type ***NymiAudaPartner.exe start***. On the `User Account Control` dialog, click **Yes**. The Nymi AUDA+ Partner Software service starts.

Running Nymi AUDA+ Partner Software as a Standalone Application

To the run the Nymi AUDA+ Partner Software as a standalone application, navigate to the Nymi AUDA+ Partner Software folder and in the *bin* folder, run *start.bat*

When Nymi AUDA+ Partner Software starts, the application creates and writes messages in the *C:\Nymi\NymiAudaPartner\logs\NymiAudaPartner.log* file.

Note: The maximum file size for the *NymiAudaPartner.log* is 10MB. When the log file reaches the maximum file size, the Nymi AUDA+ Partner Software renames the log file and creates a new *NymiAudaPartner.log* file.

Configuring the Nymi AUDA+ Partner Software Dashboard

Connect to the Nymi AUDA+ Partner Console and update the configuration to enable a connection to the PAS-X AUDA+ server.

About this task

Procedure

1. From a web browser, connect to the Nymi AUDA+ Partner Console URL.

   The URL format is as follows: ***https://`servername`:`port`/nymiaudapartner***

   where:

   - *`servername`* is the FQDN of the Nymi AUDA+ Partner Software server.
   - *`port`* is one of the following port numbers:
     - 80 — For HTTP
     - 443 — For HTTPS
2. In the **`Username`** and **`Password`** fields, type the username and password of a NES administrator.
3. Click **`Sign in`**
4. From the menu, click **`Configuration`**.
5. On the `Configuration` window, click the **`Edit`** button beside the configuration.
6. In the **`Instance ID`** field, type the instance ID of the Nymi AUDA+ Partner.
7. In the **`Username`** and **`Password`** fields, type the username and password to communicate with PAS-X AUDA+ using (HTTP) basic authentication.

   Note: When communicating with PAS-X AUDA+ using basic authentication (via HTTP), the account name must be the same with the AUDA+ administrators.
8. Click **`Update configuration`**.

Manage the Nymi AUDA+ Partner Software Environment

Review this section for information about how to manage the deployment environment.

Log Files

The *C:\Nymi\NymiAudaPartner* directory contains the log files for the Nymi AUDA+ Partner Software.

When you start the Nymi AUDA+ Partner Software as an application or service, the process creates a *nymiaudapartner.log* file that contains status information and error messages that can assist you in troubleshooting issues. The maximum file size for the log is 10 MBs.

Restarting the Nymi AUDA+ Partner Software Service

If you stop the Nymi AUDA+ Partner Software service, perform the following steps.

Before you begin

Before you perform the following steps, ensure that you shutdown all instances in a Nymi AUDA+ Partner Software cluster.

About this task

This procedure requires access to a SQL client or editor that you can use to run queries on the database, such as SSMS.

Procedure

1. Log in to the Nymi AUDA+ Partner Software server.
2. Use SSMS to connect to the Nymi AUDA+ Partner Software database, with an account that has administrator access to the SQL database.
3. Load and execute the *resetterminal.sql* query file, which you can find in *.. \nymiaudapartner-1.0.0+3.zip\nymiaudapartner-1.0.0+3\dbscripts\mssql* folder of the Nymi AUDA+ Partner Software package.
4. Start the Nymi AUDA+ Partner Software service.

Configure User Terminals

Configuring the user terminals is a two-step process:

- Define an endpoint ID for each user terminal, which the identifies the user terminal and allows the Nymi AUDA+ Partner Software to communicate with the correct user terminal.
- Add a reference to the user terminal in the Nymi AUDA+ Partner Console.

  You can use the Nymi AUDA+ Partner Console to add user terminals one at a time or in bulk.

Defining the User Terminal Endpoint ID

About this task

Perform the following steps on each user terminal.

Procedure

1. Edit the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file.
2. At the end of the file, create a new parameter named `endpoint_id` and set the value to the host name of the user terminal, enclosed in double quotes.

   For example: ***endpoint_id = "LABLC"***.

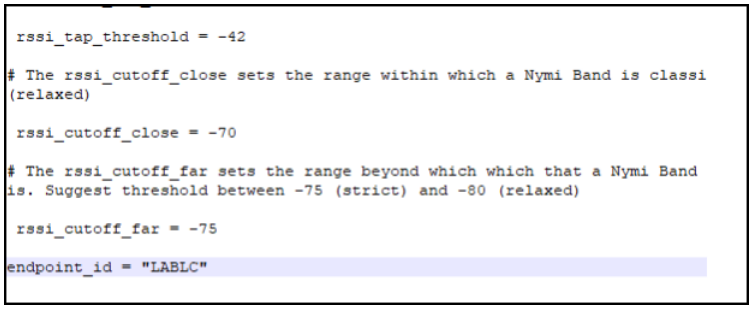

Figure 23: Endpoint_id example

3. Save the file.
4. Restart the Nymi Bluetooth Endpoint service.

Add User Terminals to Nymi AUDA+ Partner Console

The Nymi AUDA+ Partner Software interacts with the Nymi Bluetooth Endpoint service on a user terminal to detect and react to changes in Nymi Band authentication states.

For example, when a user authenticates to their Nymi Band, the user can perform Nymi Band taps on an NFC reader or the Bluetooth adapter to complete authentication tasks in the PAS-X MES. When the user de-authenticates their Nymi Band, they cannot complete authentication tasks with a Nymi Band tap in the PAS-X MES.

You can add users terminals one at a time or in bulk.

Adding Terminals Manually

Refer to this section to add user terminals one at a time.

About this task

Log in to the Nymi AUDA+ Partner Console, and then perform the following steps for each user terminal.

Procedure

1. On the **`Terminals`** tab, enter the host name of the user terminal.

   Note: The host name must match the *endpoint_id* value that you defined in the *nbe.toml* file of the user terminal.

2. Click **`Add Terminal`**, as shown in the following figure.

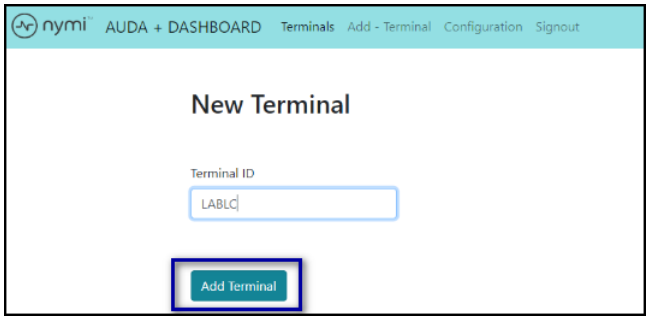

Figure 24: Add Terminal button

The Nymi AUDA+ Partner Console navigates to the `Terminal Status` page. The `Terminal Status` table displays information about the added terminals.

Property Name	Value
Terminal ID	Host name of the user terminal.
Active User	User name of the user who last performed a Nymi Band tap on the user terminal to create electronic signature. If no user has performed a Nymi Band tap on the user terminal, the value is empty.
Status	State of the terminal: • *unmanaged*—Initial status. • *managed*—Indicates that a user has performed a Nymi Band tapped on the user terminal.
Active Band	Nymi Band ID of Nymi Band of the active user.
Manage Terminal	Provides the option to delete a user terminal from the Nymi AUDA+ Partner Console.

The following figure provides an example of the `Terminal Status` window.

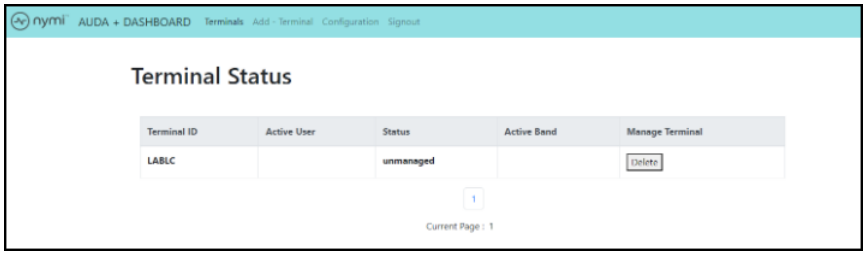

Figure 25: Terminal Status Window after a Successful Import Operation

Adding User Terminal in Bulk

The Nymi AUDA+ Partner Console supports adding terminals in bulk.

Procedure

1. Create a *CSV* file with the following 4 headers in the first row:

   Terminal, User, Status, Authmode

2. Specify the Endpoint ID and an unmanaged status of each user terminal on subsequent rows. It is not necessary to specify values for the user and Authmode.

   For example, to add 3 user terminals named WinTerminal_1, WinTerminal_2, and WinTerminal_3 to the Nymi AUDA+ Partner Console, create a CSV file in the following format:

   ```
   Terminal,User,Status,Authmode
   Winterminal_1,,unmanaged,
   Winterminal_2,,unmanaged,
   Winterminal_3,,unmanaged,
   ```

   Note: Do not include spaces before or after the commas.

3. Log in to the Nymi AUDA+ Partner Console and click **`Terminals`**.
4. Click **`Choose File`**, as shown in the following figure.

   Figure 26: Choose CSV File button

5. On the `Open` window, navigate to the folder that contains the *CSV* file, select the file, and then click **`Import Terminals`**.
   The Nymi AUDA+ Partner Console displays a `Terminal Uploads Status` window, with the results of the import.

Results

The `Terminal Uploads Status` window can display the following results:

- Import succeeded for all user terminals.

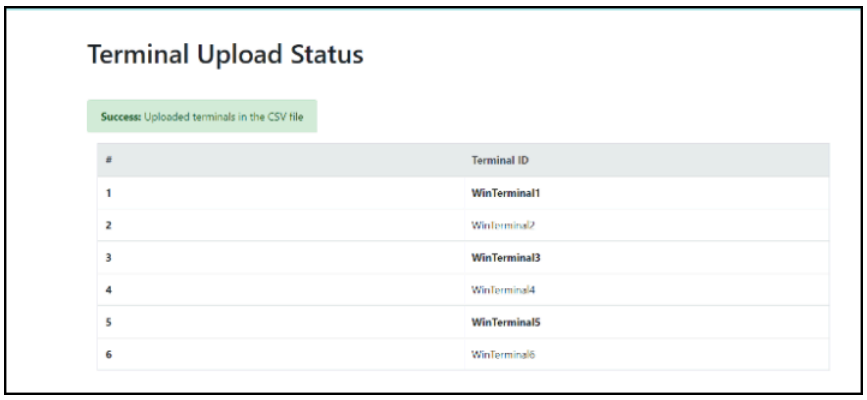

Figure 27: Successful user terminal import

- Import fails for some user terminals because the user terminals already exists in the Nymi AUDA+ Partner Console.

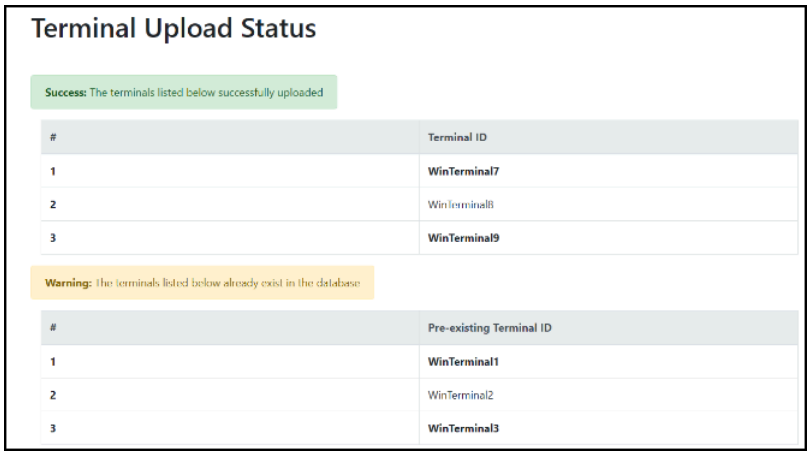

Figure 28: Unsuccessful user terminal import

- Import fails for all user terminals because of *CSV* file format issues.

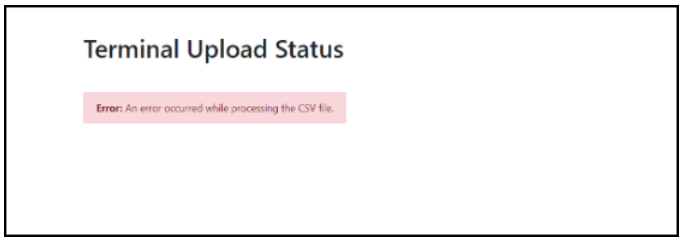

Figure 29: Failed user terminal import

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