Rockwell PharmaSuite Integration Guide

Nymi Connected Worker Platform
v7.0
2026-02-20

Contents

Preface

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

Purpose

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

The Nymi Connected Worker Platform—Rockwell PharmaSuite Integration Guide provides information about how to configure the Connected Worker Platform and *FactoryTalk®PharmaSuite® MES* components to allow authenticated users to use the Nymi Band to perform authentication operations in the Rockwell FactoryTalk PharmaSuite MES.

Audience

This guide provides information to NES and Rockwell PharmaSuite Administrators. An NES and Rockwell PharmaSuite Administrator is the person in the enterprise that manages the Connected Worker Platform with the Rockwell FactoryTalk PharmaSuite MES in their workplace.

Revision history

The following table outlines the revision history for this document.

Revision history

Version	Date	Revision history
1.0	March 2, 2024	First release of this document.
2.0	May 3, 2024	Second release of this document, updates include: • Addition of the steps to enable the Lock Control option in the active NES policy. • Minor revisions to the *Installing Nymi Bluetooth Endpoint* and *Installing Nymi Runtime* procedures. • Removal of content related to the Windows credential provider.

Version	Date	Revision history
		• Change in recommended location of the *application.log* file.
3.0	May 21, 2024	Third release of this document. Updates include: • Changes to the Overview table. • Movement of the *Install and Configure Nymi Component* after *Install and Configure the Nymi Biometric Authentication Class* • Updates to the *Installing the Nymi Biometric Authentication Class* section to include the requirement to copy the *Negotiate* folder to each user terminal.
4.0	July 16, 2024	Fourth release of this document. Updated to include: • Bluetooth adapter placement recommendations. • Instructions about how to install NegotiateService • Instructions about how to configure Connected Worker Platform Communication Protocol.
5.0	November 28, 2024	Fifth release of this document. Updates include clarifying the content regarding the .NET 4.8 requirement for negotiate.exe in the section *Installing NegotiateService*
6.0	January 15, 2025	Sixth release of this document to correct the Nymi Agent port from 9210 to 9120.
7.0	February 20, 2026	Seventh release of this document to include new content about how to enable the NYMI_PAINT registry key to display a Nymi icon that indicates a user can perform

Version	Date	Revision history
		Nymi Band taps to log on, switch user, and perform e-signatures.

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 with Rockwell PharmaSuite Solution Deployment Overview

The Nymi with Rockwell PharmaSuite Solution extends the use of the Nymi Band with the Rockwell FactoryTalk PharmaSuite MES. The Nymi Band helps automate access to Rockwell FactoryTalk PharmaSuite MES and provides the ability for a user to easily apply their digital signature to process sign-offs.

The deployment of the solution requires the following high level steps:

- An administrator deploys a JAR package on the Rockwell PharmaSuite server.
- Client machines automatically receive the JAR upon runtime download.

Note: The inclusion of the JAR file does not impact the use of the Rockwell FactoryTalk PharmaSuite MES on client machines that do not use the Nymi Band.

Components in a Centralized Nymi Agent Configuration

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

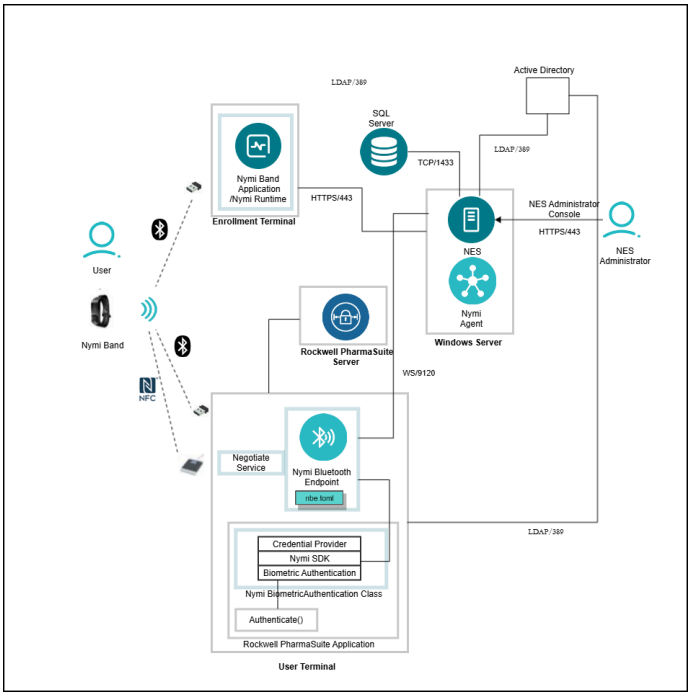

Figure 1: Connected Worker Platform with Rockwell FactoryTalk PharmaSuite MES components and connection ports in a Centralized Nymi Agent Configuration

The Connected Worker Platform with Rockwell Pharmasuite Solution consists of the following components.

Table 1: Connected Worker Platform Components

Component	Description
Enrollment Terminal	Windows 10 or Windows 11 endpoint that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the Nymi Band Application Terminal, which 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 is associated with the biometrics of a single user. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled. **Note:** Nymi Connect for Android supports the BLE component of the Nymi Band only.

Component	Description
NES	Windows-based management server and collection of services that administrators access through a web-based application. NES coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates.
NES Administrator Console	A web 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 a Nymi Band tap on the NFC reader or Bluetooth Adapter.
Nymi Bluetooth Endpoint	A component of the Nymi Runtime that you install on each user terminal. A component of the Nymi Runtime that provides an interface between the Bluetooth Adapter (BLE) and the Nymi Agent. You deploy Nymi Bluetooth Endpoint Daemon (NBEd) on individual workstations to provide Bluetooth communication with Nymi Bands. Nymi Bluetooth Endpoint communicates with the Nymi Bands through the Nymi-provided BLE Adapter, which you plug into a USB port on the user terminal.
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.
Centralized Nymi Agent	Nymi Runtime component that you install on a server that is accessible to all user terminals, for example the NES server. A component of the Nymi Runtime that provides BLE management, manages operations and message routing. Facilitates communication between a Nymi-Enabled Application(NEA) and the Nymi Band, and maintains knowledge of the Nymi Band presence and authenticated states.
Nymi BiometricAuthentication Class (Credential Provider Java Application)	Nymi-provided module that enables the use of the Nymi Band to perform authentication tasks in the Rockwell FactoryTalk PharmaSuite MES. Contains the Credential Provider, Nymi SDK, Jar files, and Biometric Authentication class.

Component	Description
Credential Provider	Nymi BiometricAuthentication Class component. An instance created by the Biometric Authentication class that performs the following actions when a user performs a Nymi Band tap: • Connects to Nymi Enterprise Server(NES) to retrieve a token by using the NegotiateLoginWithToken API. • Calls the init() method to initialize NES so that further communication can happen to fetch user name and password when band is tapped. • Returns the credentials to the readyToAuthenticate() method in the Biometric Authentication class.
Nymi SDK	Nymi BiometricAuthentication Class component. Includes the Nymi API (nymi_api.dll) that supports the integration of Rockwell FactoryTalk PharmaSuite MES with the Nymi.
Biometric Authentication	Nymi BiometricAuthentication Class component. Class that contains the the readyToAuthenticate() method, which the Rockwell FactoryTalk PharmaSuite MES calls to perform authentication. Biometric authentication creates the Credential Provider instance and runs a listener, which waits for the user to perform a Nymi Band tap. When user taps their Nymi Band, the Credential Provider returns the username and password, and Biometric Authentication calls the authenticate() method with the username and password.
authenticate()	Rockwell FactoryTalk PharmaSuite MES component.
SQL Server	Database server that contains tables that store information about the NES configuration and the Nymi Bands. Database server that contains tables that store information about the NES configuration and the Nymi Bands. The same SQL server can contain tables that store Evidian audit logs, which include information about when a user completes and authentication event in the Evidian SSO window by tapping their Nymi Band. For Proof of Concept (POC) and pre-production environments, you can use the Nymi-provided SQL Server Express software. For production environments Nymi recommends that you use SQL server. The same server or another server contains the eInfortree database.

Firewall Port Requirements

The following tables summarizes the TCP port requirements for the Nymi with Rockwell PharmaSuite Solution.

Table 2: Firewall Port Requirements

Component	Port Requirements
Enrollment Terminal	Port 389 to the Active Directory server for LDAP communication. Port 636 to the Active Directory server for LDAPS communication. Port 9120 to the centralized Nymi Agent.
User Terminal	Port 443 to the NES server for HTTPS communication. Port 9120 to the centralized Nymi Agent.
NES server	Port 1443 to the SQL server. Port 389 to the Active Directory server for LDAP communication. Port 636 to the Active Directory server for LDAPS communication.

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 with Rockwell PharmaSuite 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 Nymi with Rockwell PharmaSuite Solution deployment.

You can deploy Nymi with Rockwell PharmaSuite Solution in the following CWP environments:

- CWP 1.9.x
- CWP 1.16.x or later

The Nymi with Rockwell PharmaSuite Solution supports the following application versions:

- Rockwell FactoryTalk PharmaSuite MES 10.2
- Rockwell FactoryTalk PharmaSuite MES 11.2

Configure and Deploy the JAR Package

The Nymi with Rockwell PharmaSuite Solution relies on the configuration of a JAR file to allow users to complete authentication tasks such as login and e-signatures with a Nymi Band tap.

The JAR file differs depending on the Rockwell FactoryTalk PharmaSuite MES version:

- Rockwell FactoryTalk PharmaSuite MES 10.2 —*client.jar* file.
- Rockwell FactoryTalk PharmaSuite MES 11.2—*BiometricAuthentication.jar* file.

Perform the following steps to add the JAR file to your existing Rockwell FactoryTalk PharmaSuite MES and configure the module for your environment.

(Nymi-Lead) Configuring the JAR File

Contact your Nymi Solution Consultant to obtain the Nymi BiometricAuthentication Classor Client.jar package.

Before you begin

Your Nymi Solution Consultant configures the package based on information that you provide at the time you request the software. The Nymi Solution Consultant updates configuration files, and then provides the Rockwell Project Delivery Team with the package.

The package differs depending on the Rockwell PharmaSuite version.

About this task

The Nymi Solution Consultant performs the following actions.

Procedure

1. Use an JAR file compatible compression/decompression application, such as 7zip to open the Nymi-provided JAR file (*Client.jar* or *BiometricAuthentication.jar* file.
2. Edit the *config.properties* file in the compressed file, and change the values for the following parameters, as required:

Option	Description
NES_URL	Specifies the URL to the Nymi Enterprise Server(NES) server in the format https://*nes_server_fqdn/instanace_name*. For example: ***NES_URL=https://nes.nymi.com/nes***

Option	Description
Agent_URL	• For centralized Nymi Agent deployments only, uncomment the parameter and specify the hostname that is defined for the Nymi Agent server. For example, ***Agent_URL=ws://agent.nymi.com:9120/socket/websocket*** • For local Nymi Agent deployments only, comment the *Agent_URL* parameter.
Pharmasuite_app.version	• For Rockwell PharmaSuite version 11, specify 11. • For Rockwell PharmaSuite version 10, specify 10.

3. Optionally, to change the location of the application log file, perform the following actions:
   a) Edit the *log4j2.properties* file in the compressed file.
   b) Change the path that appears for the *property.filename* parameter to *${sys:user.home}/.Nymi/Integration/application.log*.
   c) Save the *log4j2.properties* file in the compressed file.

Deploying the JAR Package

The Rockwell Project Delivery Team deploys the Nymi-provided JAR package in your environment.

Provide the Rockwell Project Delivery Team with the JAR package provided to you by Nymi.

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 the Required NES Policies Options

To allow the integration to store encrypted passwords, enable the Nymi Lock Control option in the active NES policy.

About this task

Before users enroll their Nymi Bands, perform the following tasks from a Web Browser to enable the Nymi Lock Control.

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 **`Lock Control`** section, select the **`Enable Nymi Lock Control`** option.
   The following figure provides an example of the Lock Control policy settings.

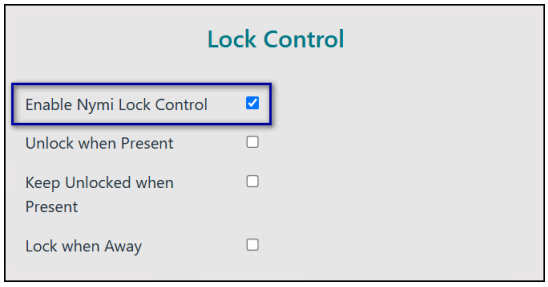

Figure 2: Enable Lock Control

   Note: It is not necessary to select other Lock Control options.
5. Click **`Save`**.

Set Up a Centralized Nymi Agent

When your environment uses iOS devices, applications on RDP/Citrix session hosts, and web-based Nymi-Enabled Application(NEA)s, you must deploy a centralized Nymi Agent on a Windows server in the environment, such as the Nymi Enterprise Server(NES) server.

The Nymi Agent has two server interfaces:

- Standard Nymi Agent interface. By default, standard Nymi Agent interface connect over plain text websocket.
- Nymi WebAPI interface. By default Nymi WebAPI interface is disabled.

Nymi recommends that you configure the Nymi Agent to use secure websocket connections for both standard Nymi Agent interface, and if enabled, the Nymi WebAPI interface. This chapter provides more information.

Importing the Root CA certificate

Perform the following steps only if the Root CA issuing the TLS server certificate is not a Trusted Root CA. For example, when you use a self-signed TLS server certificate.

Before you begin

Install the Root CA on the following machines:

- All user terminals, including user terminals that run Nymi-Enabled Applications
- Enrollment terminal
- Centralized Nymi Agent

About this task

While logged into the user terminal as a local administrator, use the `certlm` application to import the root CA certificate into the Trusted Root Certification Authorities store.

Procedure

1. In the `certlm` window, right-click **`Trusted Root Certification Authorities`**, and then select **`All Tasks > Import`**.
2. On the `Welcome to the Certificate Import Wizard` screen, click **`Next`**.
3. On the `File to Import` screen, click **`Browse`**, navigate to the folder that contains the certificate file, select the file, and then click **`Open`**.
4. On the `File to Import` screen, click **`Next`**.
5. 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`**.
6. On the `Completing the Certificate Import Wizard` screen, click **`Finish`**.

Installing/Updating Centralized Nymi Agent

Install or update the Nymi Agent application, which is included in the Nymi Runtime installation package, on a server in the environment.

About this task

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

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the *..\nymi-sdk\windows\setup* folder, right-click the *Nymi Runtime Installer version.exe* file, and select **`Run as administrator`**.
4. On the `Welcome` page, click **`Install`**.
5. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
7. On the `Nymi Runtime Setup` page, expand **`Nymi Runtime`**.
8. Select **`Nymi Bluetooth Endpoint`**, and then select **`Entire feature will be unavailable`**.
   The following figure provides an example of the `Nymi Runtime Setup` window with option to make **`Nymi Bluetooth Endpoint`** unavailable.

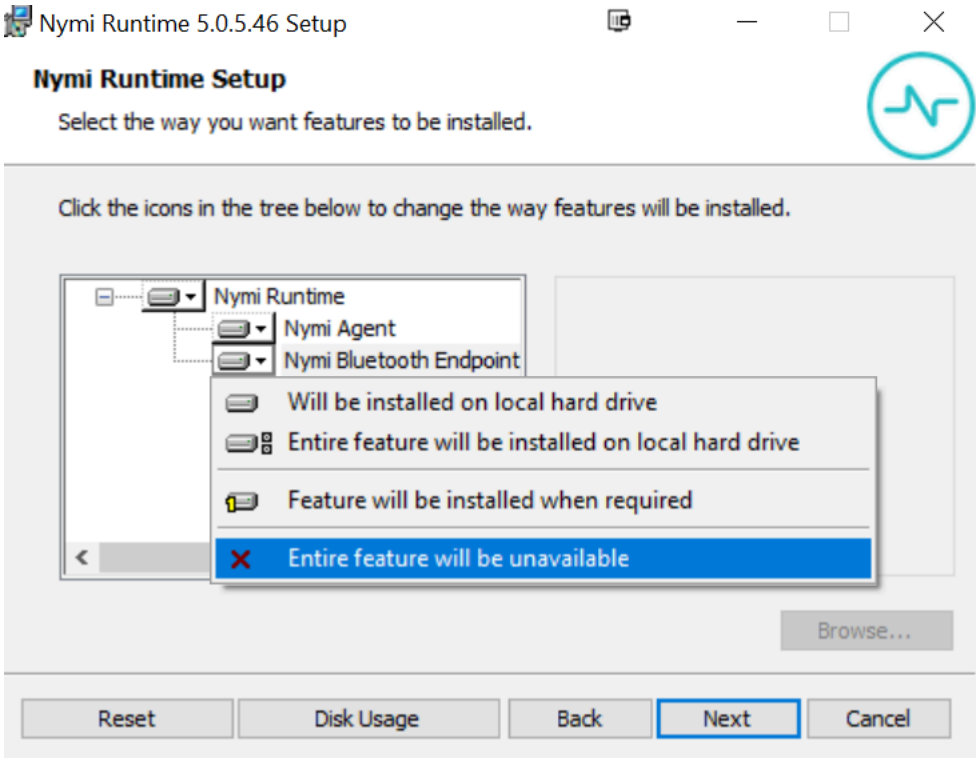

Figure 3: Nymi Bluetooth Endpoint feature will be unavailable

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

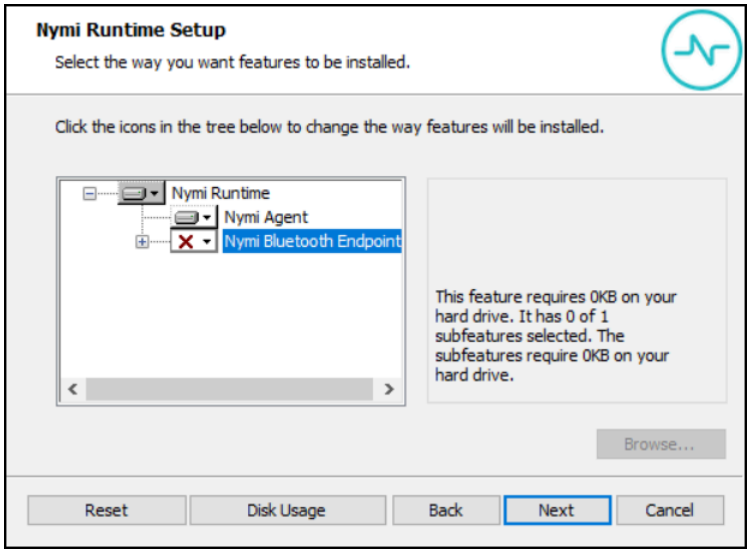

Figure 4: Nymi Bluetooth Endpoint feature is not available

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

    - Accept the default service account NTAuthority\LocalService, click **`Next`**.

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

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

The following figure shows the Service Account window.

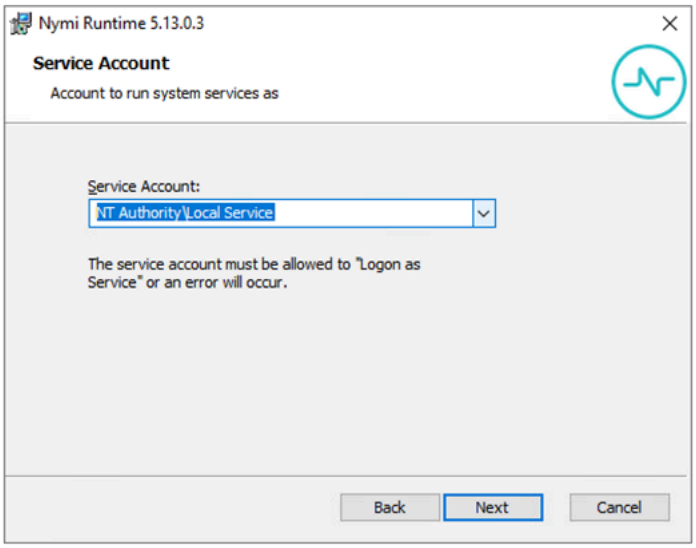

Figure 5: Nymi Runtime Service Account window

11. On the (Optional) Nymi Infrastructure Service Account window, specify the username and password of the Nymi Infrastructure Service Account. When you specify the username, include the domain name, for example *tw-lab\nymi_infra_service_acct*.

The following figure shows the Nymi Infrastructure Service Account window.

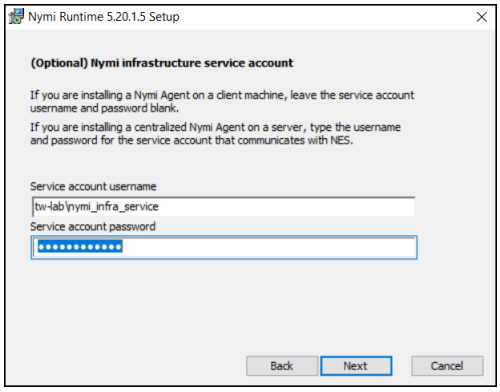

Figure 6: Nymi Infrastructure Service Account window

The installer creates the following files in the *C:\Nymi\NymiAgent\certs* folder:

- credentials-contains the encrypted credentials for the Nymi Infrastructure Service Account
- Private key, which is used to encrypt the credentials.
- Public key, which is used to encrypt the credentials.

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

Set Up Enrollment Terminal

There are two methods that you can use to configure the computer that users use to perform Nymi Band enrollments.

Decentralized Enrollment Terminal	You install the Nymi Band Application on one or more thick client user terminals. This method: • Organizations control when and where a user can perform an enrollment. • Supports a supervised enrollment process.
Centralized Enrollment Terminal	You install the Nymi Band Application on a Citrix session host and users can access the Nymi Band Application from the Citrix Storefront. This method: • Allows users to perform enrollments from any thin client. • Supports an unsupervised enrollment process.

Nymi recommends that you deploy a decentralized enrollment terminal.

Set Up a Decentralized Enrollment Terminal

Before a user can enroll and authenticate the Nymi Band, the NES Administrator must perform the following actions on at least one machine in the environment (the enrollment terminal). You cannot use a thin client as an enrollment terminal.

- Insert the Nymi-supplied Bluetooth adapter into an available USB port.
- Install the Nymi Band Application. The Nymi Band user requires physical access to the enrollment terminal.
- Set the NES_URL registry key.

Install the Nymi Band Application

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

You can perform a customizable installation or a silent installation.

Installing/Updating the Nymi Band Application

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Before you begin

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

Procedure

1. Download the Nymi Band Application package.
2. Double-click the *Nymi-Band-App-installer-v_`version`.exe* file.
3. On the `User Account Control` window, click **`Yes`**.
4. On the `Prerequisites` window, click **`Next`**.
5. On the `Welcome` page, click **`Install`**.
6. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
7. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
8. On the `Nymi Runtime Setup` window, click **`Next`**.
9. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
   - Accept the default service account 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.

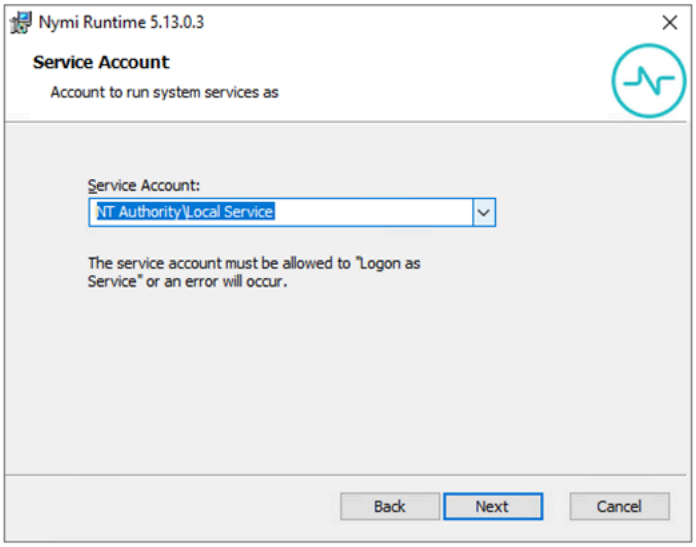

Figure 7: Nymi Runtime Service Account window

10. On the `(Optional) Nymi Infrastructure Service Account`, click **`Next`**.

Only deployments that use web-based Nymi-enabled Applications(NEAs) with a centralized Nymi Agent require you to configure the Nymi Infrastructure Service Account.

11. On the `Ready to install` page, click **`Install`**.
12. Click **`Finish`**.
13. On the `Installation Completed Successfully` page, click **`Close`**.
14. On the `Welcome to Nymi Band Application Setup Wizard` window, click **`Next`**.
15. On the `Select Installation Folder` window, click **`Next`** to accept the default installation location.
16. In the `Ready to Install` window, click **`Install`**.
17. On the `Completing the Nymi Band Application Setup Wizard` window, click **`Finish`**.

What to do next

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

Installing the Nymi Band Application Silently

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

Before you begin

Before you install the Nymi Band Application, install the Nymi Runtime

Procedure

1. Save the Nymi Band Application package, provided to you by your Nymi Solution Consultant.
2. Launch the command prompt as administrator.
3. From the folder that contains the Nymi Band Application, type *Nymi-Band-App-installer-v_`version`.exe /exenoui /q*

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

   The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, the Nymi Band Application and Nymi Runtime applications appear in the `Program and Features` applet.

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

Configuring the Nymi Enterprise Server URL

After you install the Nymi Band Application, perform the following steps to ensure that the enrollment process connect to the correct Nymi Enterprise Server(NES).

Procedure

1. Run *regedit.exe*

2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software > Nymi`**.
4. Right-click **`Nymi`**, and then select **`New > Key`**. Name the key **`NES`**.
5. Right-click **`NES`**, and then select **`New > String value`**.
6. In the **`Value`** field, type ***`URL`***.
7. 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.
8. Click **`OK`**.

Set Up Centralized Enrollment

In this configuration, you perform the following steps:

- Install the Nymi Band Application on the Citrix/RDP server, without installing Nymi Runtime.
- Configure the Nymi Band Application to use the centralized Nymi Agent.
- Install the Nymi Bluetooth Endpoint on the thin client that users will use to access the Nymi Band Application.
- Configure the Nymi Bluetooth Endpoint on the thin client enrollment terminal to use the centralized Nymi Agent.

Installing the Nymi Band Application on RDP/Citrix Session Host

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Procedure

1. Download the Nymi Band Application package.
2. Double-click the *Nymi-Band-App-installer-v_`version`.exe* file.
3. On the `User Account Control` window, click **`Yes`**.
4. On the `Welcome to Prerequisites` window, click **`Next`**.
5. On the `Prerequisites` window, clear the option to install Nymi Runtime, as shown in the following figure, and then click **`Next`**.

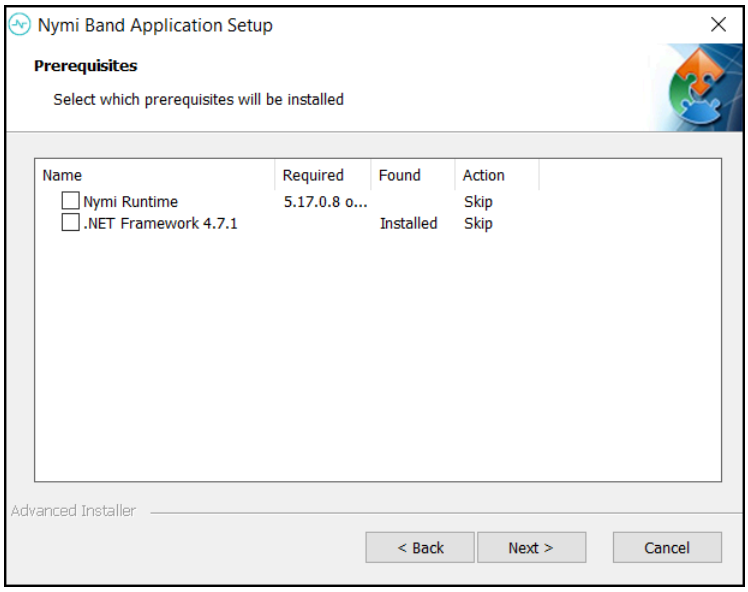

Figure 8: No Nymi Runtime Installation

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`**.
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**.
4. Right-click **Nymi**, and then select **New > Key**. Name the key **NES**.
5. Right-click **NES**, and then select **New > String value**.
6. In the **Value** field, type ***URL***.
7. 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.
8. Click **OK**.

Install and Configure the Nymi Bluetooth Endpoint

Install the Nymi Bluetooth Endpoint on the thin client that users will access to connect to the Citrix/RDP centralized enrollment terminal. You can install the Nymi Bluetooth Endpoint silently or with the installation wizard.

After you install the Nymi Bluetooth Endpoint, you must update the *nbe.toml* file.

Installing the Nymi Bluetooth Endpoint

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

About this task

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

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. 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`**.

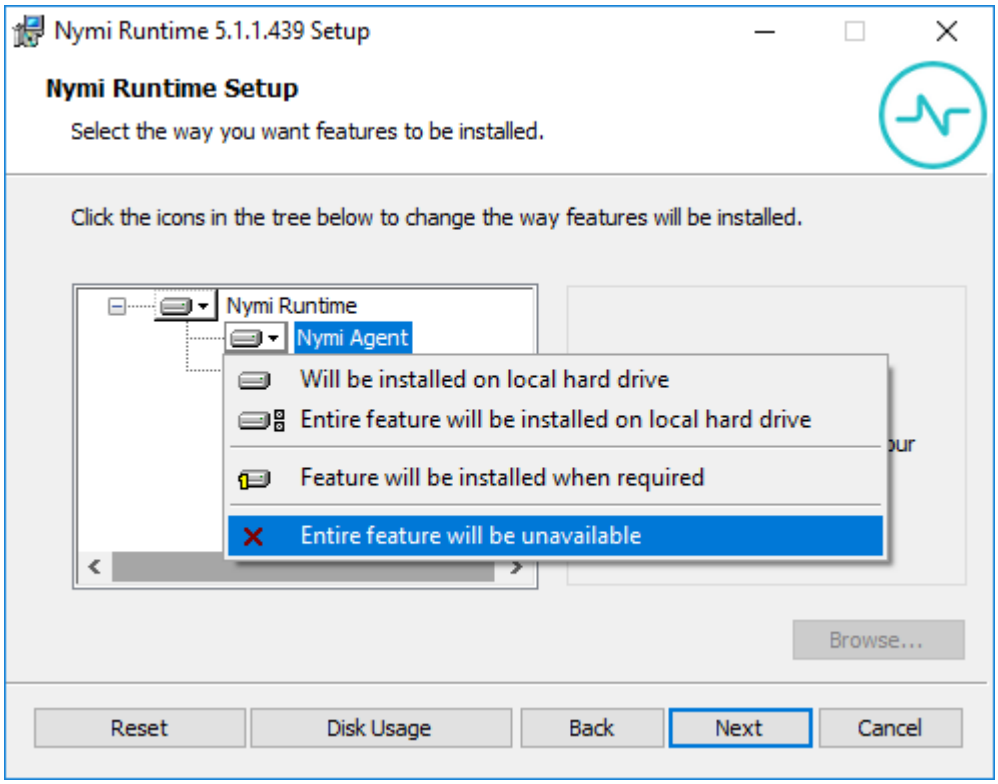

Figure 9: Nymi Agent feature will be unavailable

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

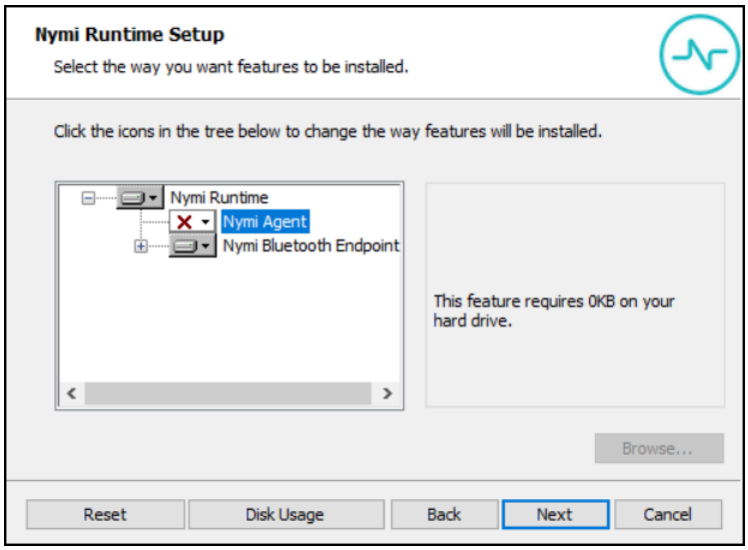

Figure 10: Nymi Agent feature is not available

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.

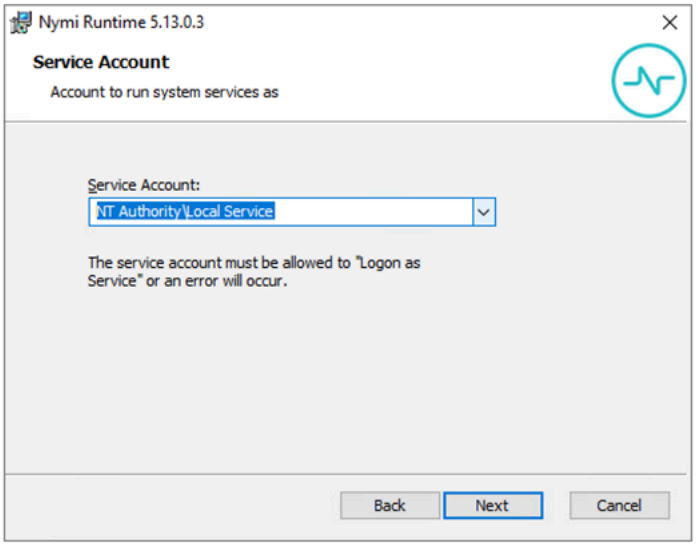

Figure 11: Nymi Runtime Service Account window

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.

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.

Configuring the Communication Protocol

If you use the enrollment terminal to also access applications, 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.

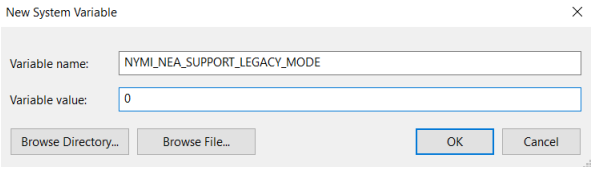

Figure 12: New System Variable window

   c) Click **`OK`**.

Set Up User Terminals

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

Bluetooth Adapter

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

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

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

Note: The presence of liquids between the Nymi Band and Bluetooth adapter negatively affects the Bluetooth signal quality. This includes beverages and the human body. If Bluetooth (BLE) taps behave unexpectedly, consider another placement for the Bluetooth adapter, or edit the Nymi Bluetooth Endpoint configuration file to adjust the signal strength thresholds to perform a BLE tap.

Installing Nymi Bluetooth Endpoint

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

About this task

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

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. 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`**.

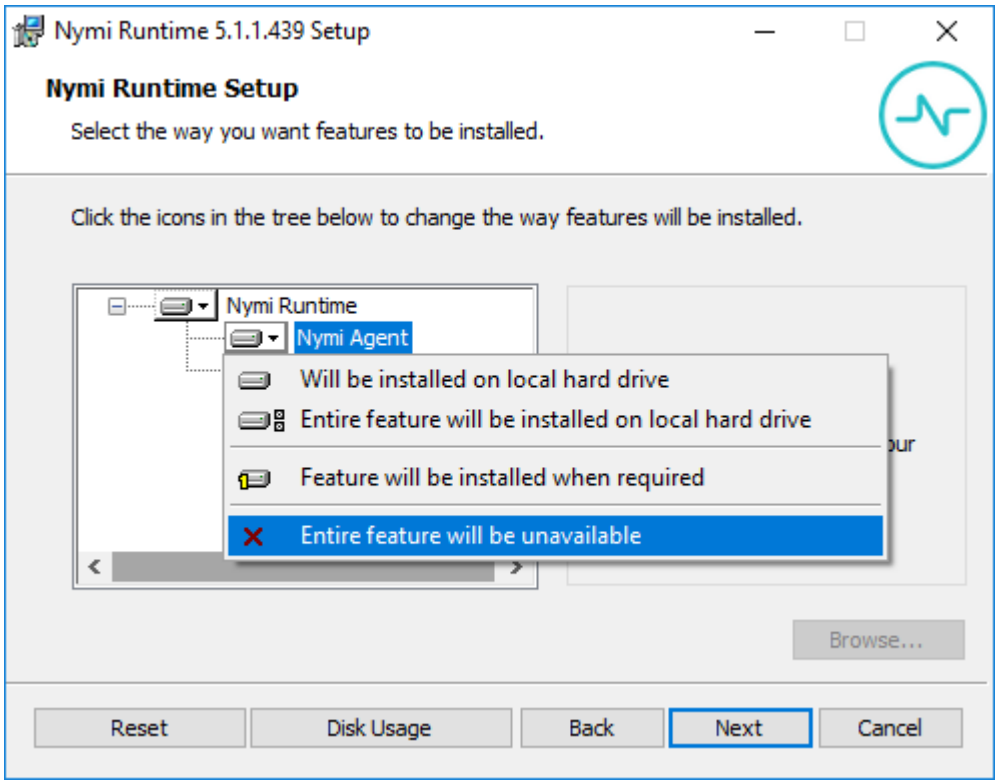

Figure 13: Nymi Agent feature will be unavailable

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

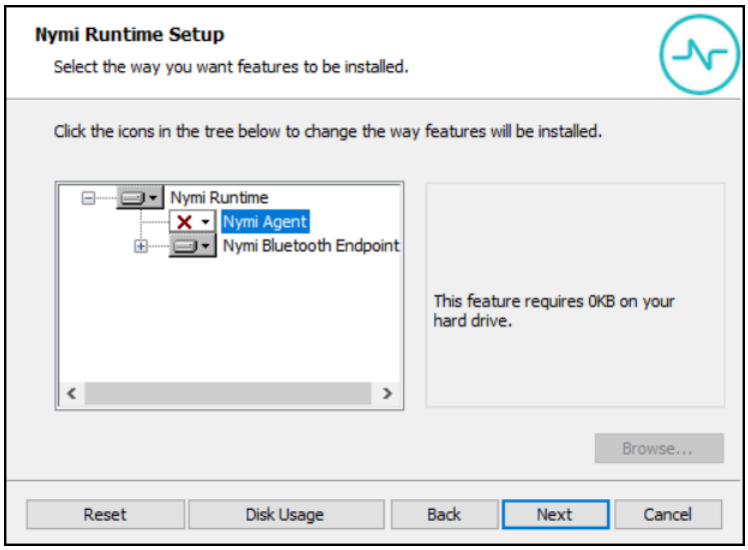

Figure 14: Nymi Agent feature is not available

11. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
    - Accept the default service account NTAuthority\LocalService, click **`Next`**.
    - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.
12. On the `(Optional) Nymi Infrastructure Service Account`, click **`Next`**.

    Only deployments that use web-based Nymi-enabled Applications(NEAs) with a centralized Nymi Agent require you to configure the Nymi Infrastructure Service Account.
13. On the `Ready to install` page, click **`Install`**.
14. Click **`Finish`**.
15. On the `Installation Completed Successfully` page, click **`Close`**.
16. Open the Windows `Services` application and confirm that the Nymi Bluetooth Endpoint service appears and the status is Running.

Updating the Nymi Bluetooth Endpoint Configuration File

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

About this task

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

Procedure

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

3. Edit the default agent_url parameter and replace the default IP address (127.0.0.1) with the FQDN of the machine that is running the remote Nymi Agent.

   For example:

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

   where ***agent.nymi.com*** is the FQDN of the remote Nymi Agent machine.
4. Save the *nbe.toml* file.
5. Restart the Nymi Bluetooth Endpoint service.

Create User Terminal Registry Keys

The Nymi with Rockwell PharmaSuite Solution requires several registry keys on the user terminals to support the use of the Nymi Band to complete authentication tasks.

Configuring the Nymi Enterprise Server URL

Perform the following steps to ensure that the negotiate API connects to the correct Nymi Enterprise Server(NES).

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software`**.
4. Right-click **`NES`**, and then select **`New > String value`**.
5. In the **`Value`** field, type ***URL***.
6. Double-click **`URL`** and in the **`Value Data`** field, type ***https://nes_server/NES_service_name/*** or ***http://`nes_server`/`NES_service_name`*** depending on the NES configuration

   where:

   - ***`nes_server`*** is the FQDN of the NES host. The FQDN consists of the ***hostname.domain_name***. You can also find the FQDN by going to the server on which you deployed NES viewing the properties of the computer. The ***`nes_server`*** is the value that appears in the **`Full computer name`** field.
   - ***`NES_service_name`*** is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
7. Click **`OK`**.

Configuring the NES Authentication Service

Perform the following steps to define the service mapping for the NES Authentication Service.

Before you begin

Determine the NES Authentication Service by logging into the NES Administrator Console, and then clicking **About**.

The following figure provides an example of the NES Authentication Service URL with the service mapping highlighted.

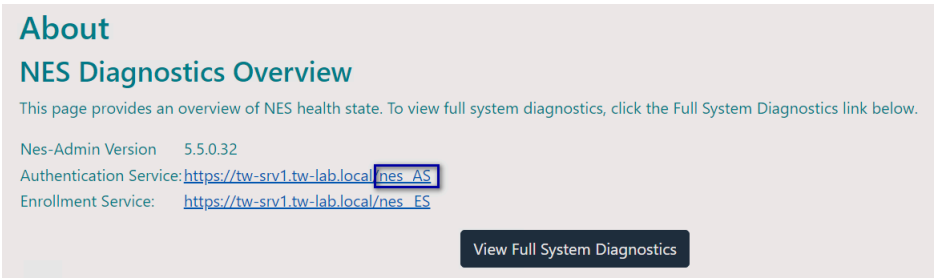

Figure 15: NES Authentication Service

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.
   On Citrix machines, navigate to **HKEY_CURRENT_USER > Software > Nymi**.
4. Right-click **NES**, and then select **New > String value**.
5. In the **Value** field, type ***AuthenticationService***.
6. Double-click ***AuthenticationService*** and in the **Value Data** field, type the service mapping for the NES Authentication Service, for example ***nes_AS***.
7. Click **OK**.

Enabling Nymi Paint

Nymi Paint enables the display of a Nymi icon on the login page and within the e-signature popup, which provides users with a clear visual indicator that Rockwell FactoryTalk PharmaSuite MES initialization completed and they can complete authentication tasks with a Nymi Band tap.

About this task

Perform the following steps on all user terminals.

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software**.
4. Right-click *NES*, and then select **New > String Value**.
5. In the **Name** field, type ***NYMI_PAINT***.

6. Edit **NYMI_PAINT**.
7. In the **Value Data** field, type ***TRUE***.
8. Click **OK**.
9. Close Registry Editor.

Results

On screens that support a Nymi Band tap, a Nymi Band icon appears.

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.

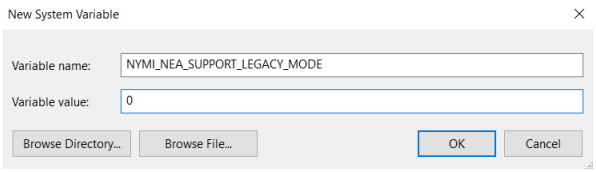

Figure 16: New System Variable window

   c) Click **OK**.

Install Negotiate

The solution relies on the Negotiate service to support Nymi Band taps.

The procedure to install Negotiate differs depending on the CWP version.

(CWP 1.16.0 and later only) Installing NegotiateService

Install the NegotiateService to secure communications between the components in the Nymi with Rockwell PharmaSuite Solution.

Before you begin

The NegotiateService requires .NET 4.8 or later. When .NET 4.8 is installed, the v4.0.30319 folder appears in the *C:\Windows\Microsoft.NET\Framework64* folder. If required, download .NET from Microsoft, and then install the software on each user terminal.

About this task

Perform the following steps on each user terminal.

Procedure

1. Determine the SID for the user terminals in the domain:
   a) Connect to the Active Directory server and run Windows Powershell as an administrator.
   b) Type ***Get-ADGroup -Filter {Name -eq "domain users"} \| Select SID***
      The following figure provides an example of the command and results.

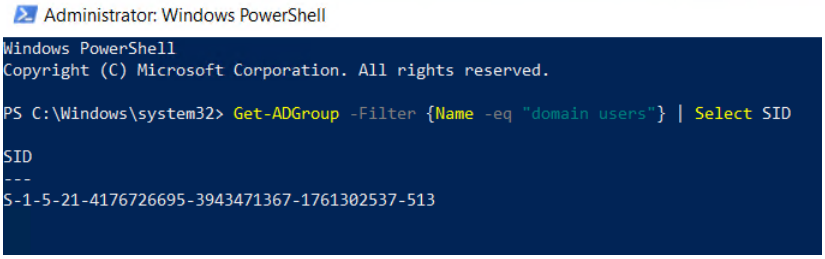

Figure 17: Get-ADGroup Command

   c) Copy the SID that appears in the output.
2. Perform the following steps on each user terminal:
   a) Download and extract the contents of the WindowsNegotiateService package to a folder.
   b) Copy the *NegotiateService* folder from the extracted folder to *C:\Nymi*.
   c) Open a command prompt as an administrator, and then change to *C:\Windows\Microsoft.NET\Framework64\v_`version_number`* directory.
      Where `version_number` is v4.0.30319 or later.
   d) Type ***InstallUtil.exe C:\Nymi\NegotiateService\NegotiateService.exe***
      The following figure provides an example of the command the results.

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319>InstallUtil.exe C:\Nymi\NegotiateService\NegotiateService.exe
Microsoft (R) .NET Framework Installation utility Version 4.8.9037.0
Copyright (C) Microsoft Corporation.  All rights reserved.


Running a transacted installation.

Beginning the Install phase of the installation.
See the contents of the log file for the C:\Nymi\NegotiateService\NegotiateService.exe assembly's progress.
The file is located at C:\Nymi\NegotiateService\NegotiateService.InstallLog.
Installing assembly 'C:\Nymi\NegotiateService\NegotiateService.exe'.
Affected parameters are:
   logtoconsole =
   assemblypath = C:\Nymi\NegotiateService\NegotiateService.exe
   logfile = C:\Nymi\NegotiateService\NegotiateService.InstallLog
Installing service NegotiateService...
Service NegotiateService has been successfully installed.
Creating EventLog source NegotiateService in log Application...

The Install phase completed successfully, and the Commit phase is beginning.
See the contents of the log file for the C:\Nymi\NegotiateService\NegotiateService.exe assembly's progress.
The file is located at C:\Nymi\NegotiateService\NegotiateService.InstallLog.
Committing assembly 'C:\Nymi\NegotiateService\NegotiateService.exe'.
Affected parameters are:
   logtoconsole =
   assemblypath = C:\Nymi\NegotiateService\NegotiateService.exe
   logfile = C:\Nymi\NegotiateService\NegotiateService.InstallLog

The Commit phase completed successfully.

The transacted install has completed.
```

Figure 18: InstallUtil Command

e) Type the following command:

sc sdset NegotiateService "D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;RPWPCR;;;DU)(A;;RPWPCR;;;SID)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Where *SID* is the SID that you copied from the **Get-ADGroup** output.

The following figure provides an example of the command the results.

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319>sc sdset NegotiateService "D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOC
OCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;RPWPCR;;;DU)(A;;RPWPCR;;;S-1-5-21-4176726695-3943471367-1761302537-513)S:(AU;FA;CCDCLCSWR
[SC] SetServiceObjectSecurity SUCCESS
```

Figure 19: InstallUtil Command

(CWP 1.9 only) Copy the Negotiate Folder

To install the Negotiate service in a CWP 1.9 environment, copy the *Negotiate* folder from the JAR zip file to the *C:\Nymi* folder on all user terminals.

Using Nymi with Rockwell PharmaSuite Solution

The following work flow describes the use case where a user uses their Nymi Band to complete authentication tasks in a Rockwell FactoryTalk PharmaSuite window.

1. User starts the Rockwell FactoryTalk PharmaSuite and navigates to a screen that requires their user credentials.
2. On the Logon screen, the user performs a left mouse click on the **Username** field.
3. User taps their authenticated Nymi Band on the NFC reader. The Desktop unlocks.
4. User navigates to screens that require the user to provide their credentials to continue.
5. The user performs a left mouse click on the **Username** field.
6. User taps their authenticated Nymi Band on the NFC reader. The authentication task completes.

Manage the Connected Worker Platform with Rockwell FactoryTalk PharmaSuite MES Environment

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

Enabling Nymi BiometricAuthentication Class Debug Mode

Enable debug mode to provide detailed messages in the *application.log* file to troubleshoot issues.

About this task

The *property.filename* parameter in the *log4j2.properties* file defines the path to the *application.log*. If required, specify an alternate path for the file.

Procedure

1. In Rockwell PharmaSuite Process Designer, export the Nymi-provided *JAR* file (*Client.jar* or *BiometricAuthentication.jar*.
2. Use an application that extracts compressed files to open the *JAR* file, and then edit *log4j2.properties* file in the compressed file, and then perform the following actions:
   - Change *rootLogger.level* parameter to ***OFF***.
   - Change the *logger.nymisdk.level* to ***debug***.
   - Change the *logger.credentialprovider.level* to ***debug***.
   - Change the *logger.credentialprovider.level* to ***debug***.

   Note: Acceptable values include:

   - *info*—Log error messages, warning messages, and informational messages.
   - *error*—Log error messages only.
   - *warn*—Log errors messages and warning messages.
   - *debug*—Log errors messages and warning messages, informational messages and debug messages.

3. For Rockwell FactoryTalk PharmaSuite MES 11.2 only, perform the changes in the previous step within the *log4j2_ftps_custom.xml* file.
4. To initialize the Rockwell FactoryTalk PharmaSuite MES with the updated *JAR* file, start the Rockwell FactoryTalk PharmaSuite MES.
5. Perform the operation that requires troubleshooting, and then review the *application.log* file.

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