Nymi with bioLock(SAP) Integration Guide

Connected Worker Platform
v1.0
2025-12-16

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 Connected Worker Platform—Nymi with bioLock(SAP) Integration Guide provides information about how to configure the Connected Worker Platform and integrate with SAP components to allow authenticated users to use the Nymi Band to perform authentication operations in the bioLock (SAP) Applications.

Audience

This guide provides information to NES and bioLock(SAP) Administrators. An NES and bioLock(SAP) Administrator is the person in the enterprise that manages the Connected Worker Platform with the Nymi-bioLock(SAP) Solution in their workplace.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	November 20, 2025	First release of this document.

Related documentation

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

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

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

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

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

- **Connected Worker Platform Release Notes**

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

How to get product help

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

How to provide documentation feedback

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

Nymi-bioLock(SAP) Solution Overview

The Nymi-bioLock(SAP) Solution is a direct integration solution that improves identity verification and access control within the bioLock SAP Integration.

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

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

Deployment Overview

The Nymi-bioLock(SAP) Solution requires you to:

- Deploy the Nymi solution with at least one instance of the Nymi Agent in a centralized location.
- Configure the user terminals to use the centralized Nymi Agent.

The following figure provides a high level overview of the components in the Nymi-bioLock(SAP) Solution.

Components in the Nymi-bioLock(SAP) Solution

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

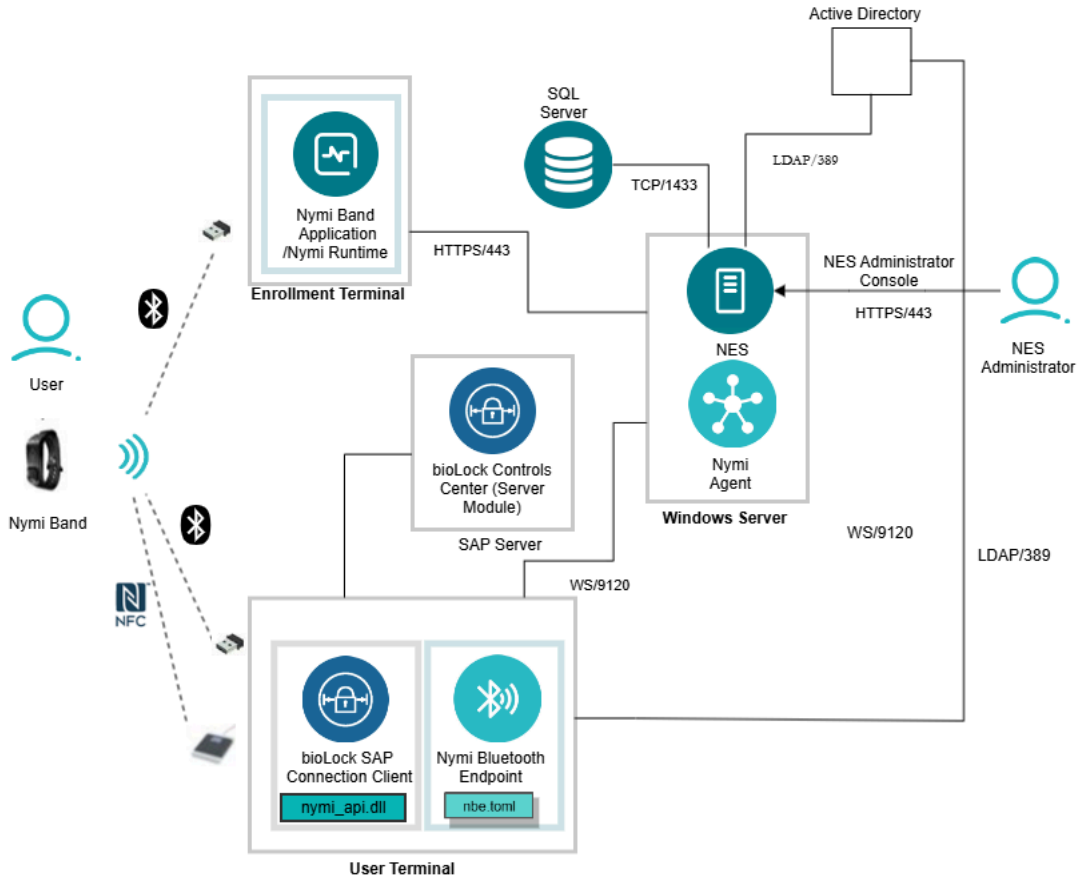

Figure 1: Nymi-bioLock(SAP) Solution components and connection ports in a Centralized Nymi Agent Configuration

The Nymi-bioLock(SAP) Solution consists of the following components.

Table 2: Nymi-bioLock(SAP) Solution 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.

Component	Description
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.
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. Users can perform Nymi Band taps to complete authentication tasks with a supported NFC reader or the Nymi-supplied Bluetooth Adapter. **Note:** Each user terminal requires a Bluetooth Adpater.
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 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.

Component	Description
bioLock SAP Connector Client	Application that you install on the user terminals. bioLock SAP Connector Client allows non-SAP systems or custom applications to communicate with SAP systems and act as an interface to connect Nymi programs or third-party software with SAP servers, facilitating data exchange and integration. bioLock SAP Connector Client enables external systems or applications to communicate with the SAP Server to perform tasks such as data integration, automation of SAP processes, and extending the functionality of SAP applications.
SAP GUI	Standard client interface accessed on the user terminals that provides you with a graphical interface to access an interact with various SAP applications and modules. The SAP GUI provides the user access to the SAP system to perform tasks such as data entry, reporting, and transaction processing.
SAP Server	Backend component of the SAP system where all data processing and storage occur. The SAP Server is typically part of a larger SAP system environment that might include multiple servers.

Use Cases

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

- Perform multi-factor authentication in SAP applications.
- Perform SAP Digital Signatures
- Perform SAP Transaction Protection

Deploy Nymi Components in a Centralized Nymi Agent Configuration

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

Note: This guide assumes that you have deployed the bioLock SAP components on the server and user terminals.

Set Up Nymi Enterprise Server

Perform the following actions on the Nymi Enterprise Server(NES) server to support the solution.

This guide assumes that you have installed the NES software. *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 an NEAbioLock SAP.

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

Option	Description
	the status again, NES retrieves the status from cache. • When this option is disabled, NES does not cache the status of users and requires NES to check the status of users every time NES receives a request from the NEA. When you clear this option, the **`Cache Expiry`** option disappears.
Cache Expiry	• Defines the length of time that the status of the user remains valid in cache. • Default: 15 mins. • When NES receives a status request from an NEA, and the length of time that the user status has been stored in cache exceeds the cache expiry value, NES contacts AD for the user status and stores the results in cache again. Nymi suggests that you change this value to 30 seconds.

Set Up Nymi Agent Server

Install the Nymi Agent service on a server in your environment.

You can install the Nymi Agent service on the Nymi Enterprise Server(NES).

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.

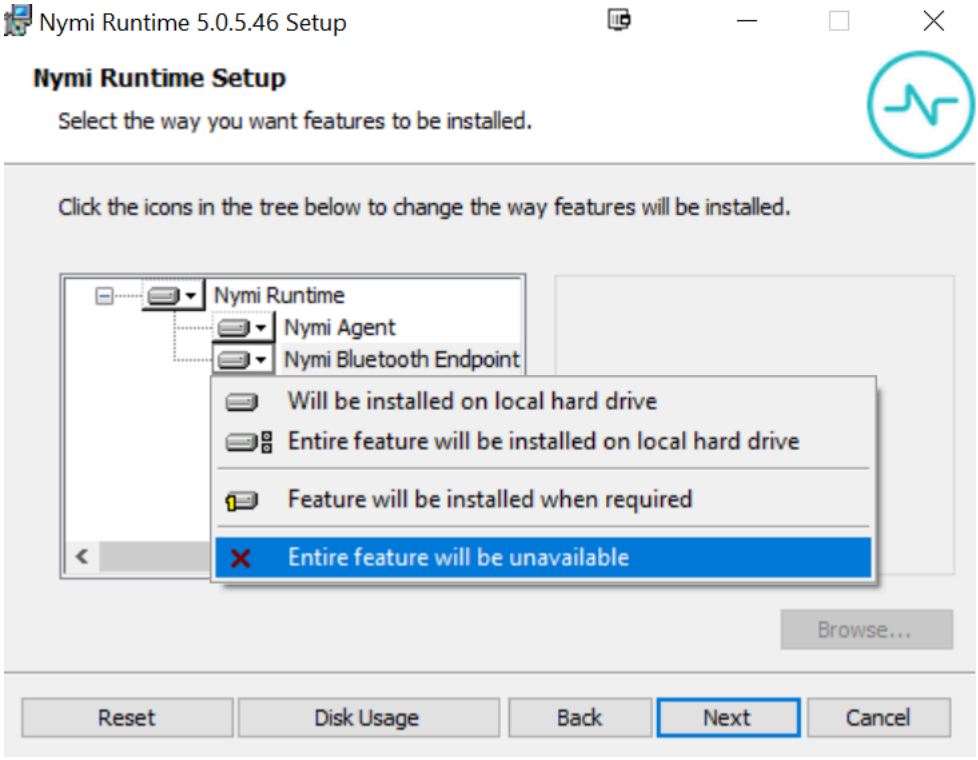

Figure 2: Nymi Bluetooth Endpoint feature will be unavailable

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

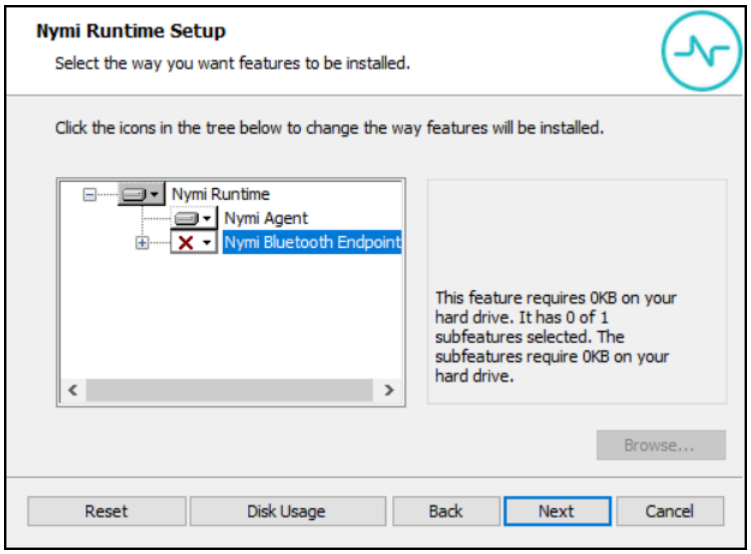

Figure 3: Nymi Bluetooth Endpoint feature is not available

10. On the `Service Account` window, 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.

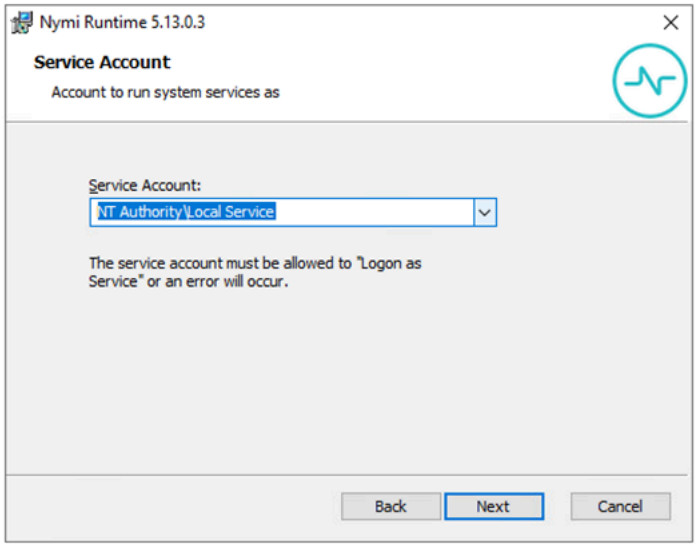

Figure 4: Nymi Runtime Service Account window

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.

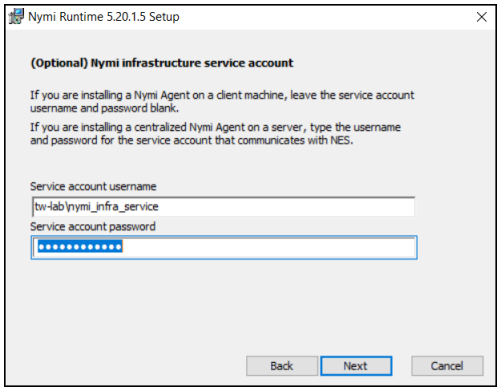

Figure 5: Nymi Infrastructure Service Account window

    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`**.

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.

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.

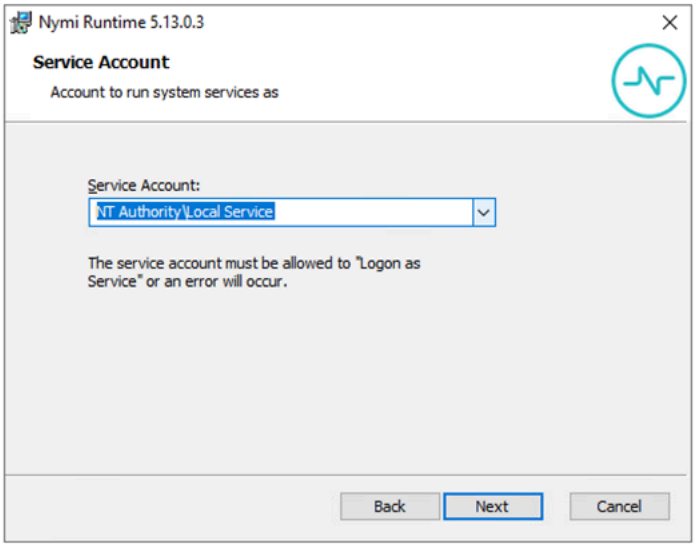

Figure 6: Nymi Runtime Service Account window

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 the User Terminals

Perform the following steps on each terminal that a user uses to access the bioLock SAP application.

Install Nymi Bluetooth Endpoint

Install Nymi Bluetooth Endpoint on each user terminal.

You can install Nymi Bluetooth Endpoint manually or silently.

Installing the Nymi Bluetooth Endpoint

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`**.

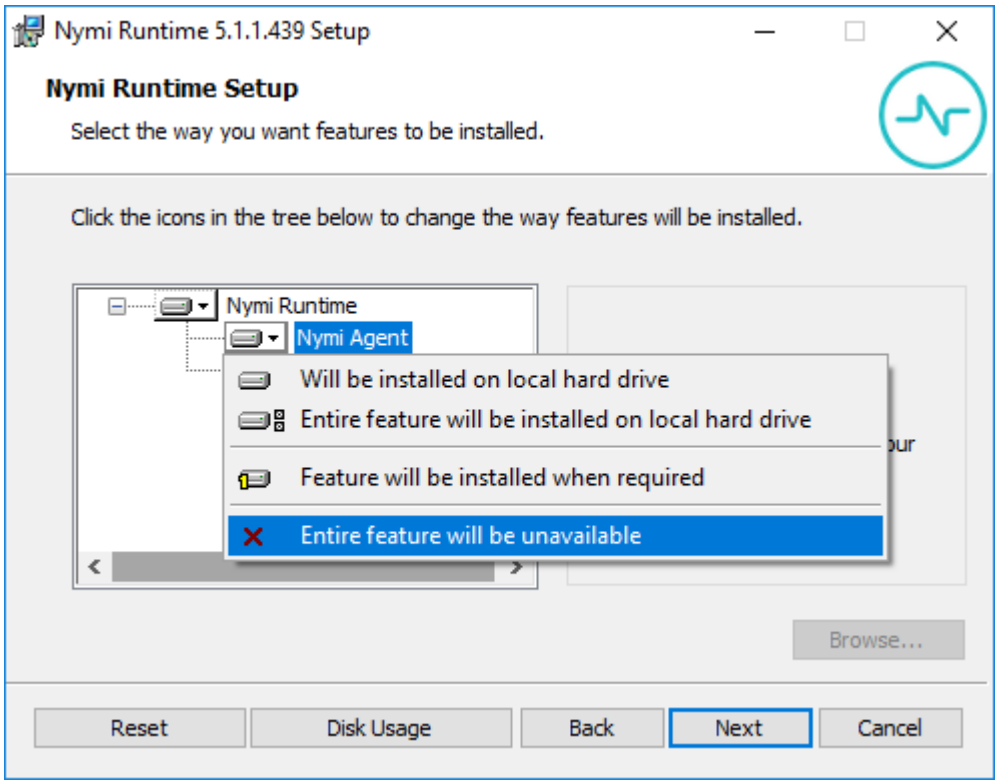

Figure 7: Nymi Agent feature will be unavailable

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

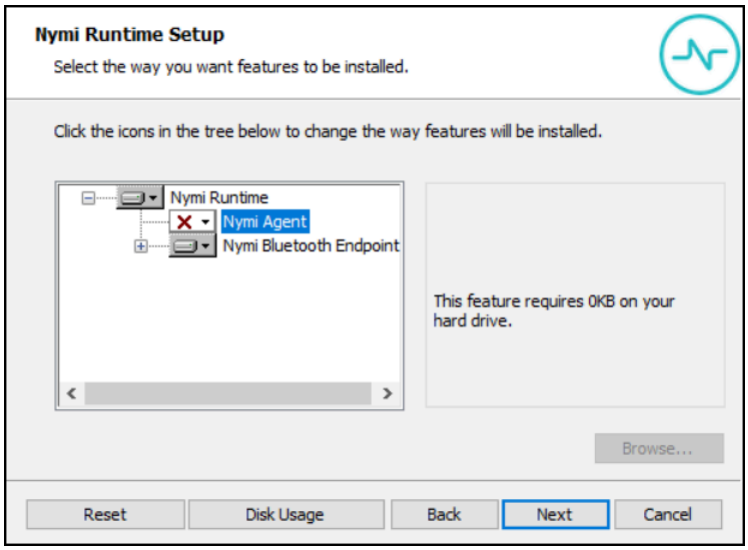

Figure 8: Nymi Agent feature is not available

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

    - Accept the default service account NTAuthority\LocalService, click **`Next`**.
    - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.

    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.

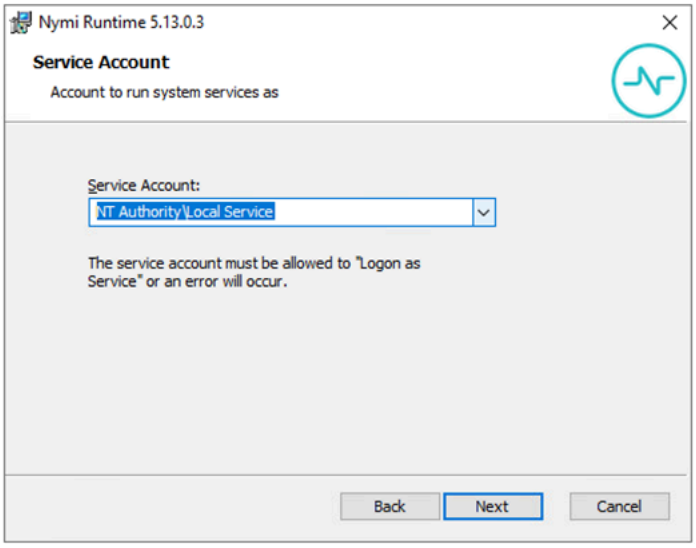

Figure 9: Nymi Runtime Service Account window

12. On the `Ready to install` page, click **`Install`**.

13. Click **`Finish`**.

14. On the `Installation Completed Successfully` page, click **`Close`**.

What to do next

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

Installing Nymi Bluetooth Endpoint Silently

Procedure

Run a Command Prompt as administrator.

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

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

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

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

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

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

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

What to do next

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

Editing the Nymi Bluetooth Endpoint Configuration File

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

About this task

Perform the following steps on each user terminal.

Procedure

1. Edit the *nbe.toml* file with a text editor in administrator mode.
2. Edit the default *agent_url* parameter and perform the following changes:
  ```

- For WSS:
  - Change the protocol from ws to wss
  - Replace ***127.0.0.1*** with the FQDN of the centralized Nymi Agent machine.
- For WS, replace ***127.0.0.1*** with the IP address of centralized Nymi Agent machine.

For example, for WSS:

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

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

Note: Optionally, you can also change the communication port from the default value 9120.

3. Optionally, at the end of a file create a new parameter to specify the endpoint ID in the following format:

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

Configuring the Connected Worker Platform Communication Protocol

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

About this task

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

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

Procedure

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

   The following figure provides an example of the new variable.

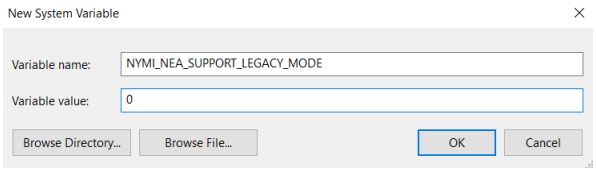

Figure 10: New System Variable window

c) Click **OK**.

Using the Nymi Band with bioLock SAP

Use the Nymi Band to perform e-signatures.

About this task

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

Procedure

1. Open the bioLock SAP application.
2. On the Fetch Token from Nymi Server popup, specify the FQDN of the Nymi Enterprise Server(NES), and then click OK.
3. On the Login popup, type your username and password.

   The following figure provides an example of the login page, when the bioLock SAP application is configured to use support the Nymi Band.

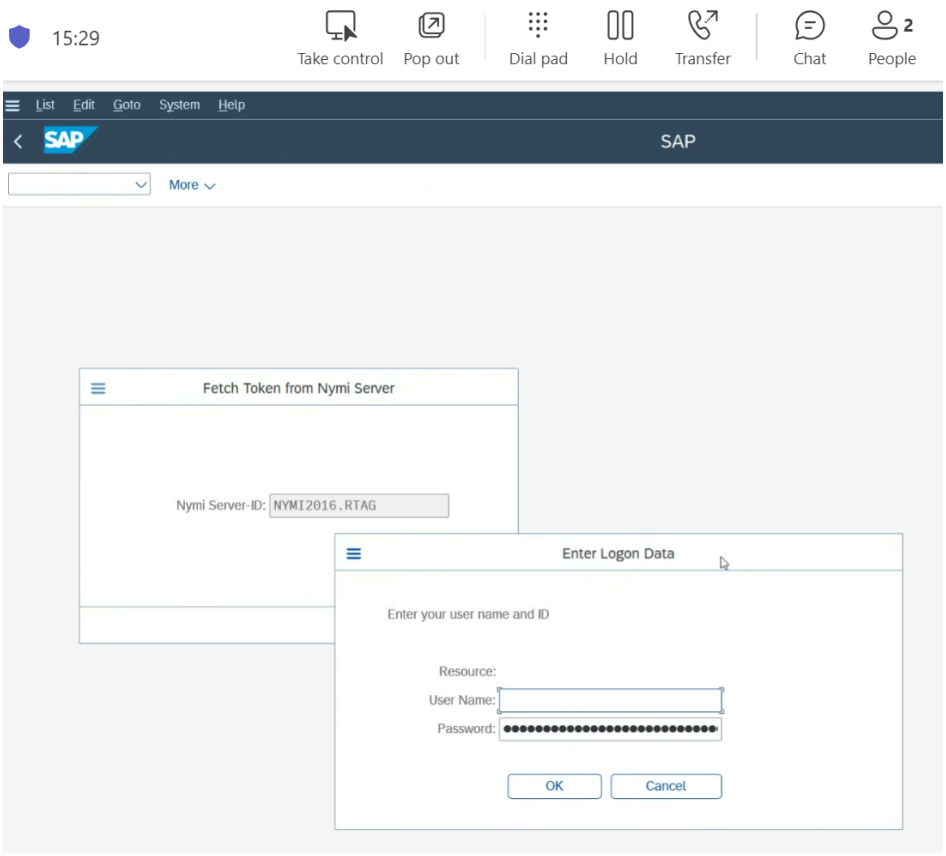

Figure 11: bioLock Login page

When the login completes, you can complete authentication tasks such as e-signatures with a Nymi Band.

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