Administration Guide

Nymi Connected Worker Platform 1.19.0
v1.0
2024-11-08

Contents

3 - 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.

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.

Audience

This guide provides information to NES Administrators. A NES Administrator is the person in the enterprise that manages the Connected Worker Platform for 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 08, 2024	First release of this document for the CWP 1.19.0 release.

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 SDK Developer Guide—NymiAPI(Windows)**

This document provides information about how to develop Nymi-enabled Applications by using the Nymi API(NAPI).

- **Nymi SDK Developer Guide—Webapi(Windows)**

  This document provides information about how to understand and develop Nymi-enabled Applications (NEA) on Windows by utilizing the functionality of the Nymi SDK, over a WebSocket connection that is managed by a web-based or other application.

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

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

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

  This document provides information about how to troubleshoot issues and the error messages that you might experience with the NES Administrator Console, the Nymi Enterprise Server deployment, the Nymi Band, and the Nymi Band Application.

- **Nymi Connected Worker Platform with Evidian Troubleshooting Guide**

  This document provides overview information about how to troubleshoot issues that you might experience when using the Nymi solution with Evidian.

- **Nymi Connected Worker Platform—FIDO2 Deployment Guide**

  The Nymi Connected Worker Platform—FIDO2 Deployment Guide provides information about how to configure Connected Worker Platform and FIDO2 components to allow authenticated users to use the Nymi Band to perform authentication operations.

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

  The Nymi Connected Worker Platform—POMSnet Installation and Configuration Guides provides information about how to configure the Connected Worker Platform and POMSnet components to allow authenticated users to use the Nymi Band to perform authentication operations in POMSnet.

- **Nymi Band Regulatory Guide**

  This guide provides regulatory information for the Generation 3 (GEN3) Nymi Band.

- **Third-party Licenses**

  The Nymi Connected Worker Platform—Third Party Licenses Document contains information about open source applications that are used in Nymi product offerings.

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

4 - Overview

4.1 - Nymi Band 3.0

The Nymi Band wearable is a biometric device used by companies to increase security and improve workflows.

Nymi Band Physical Features

The following figures show the front and back of the Nymi Band.
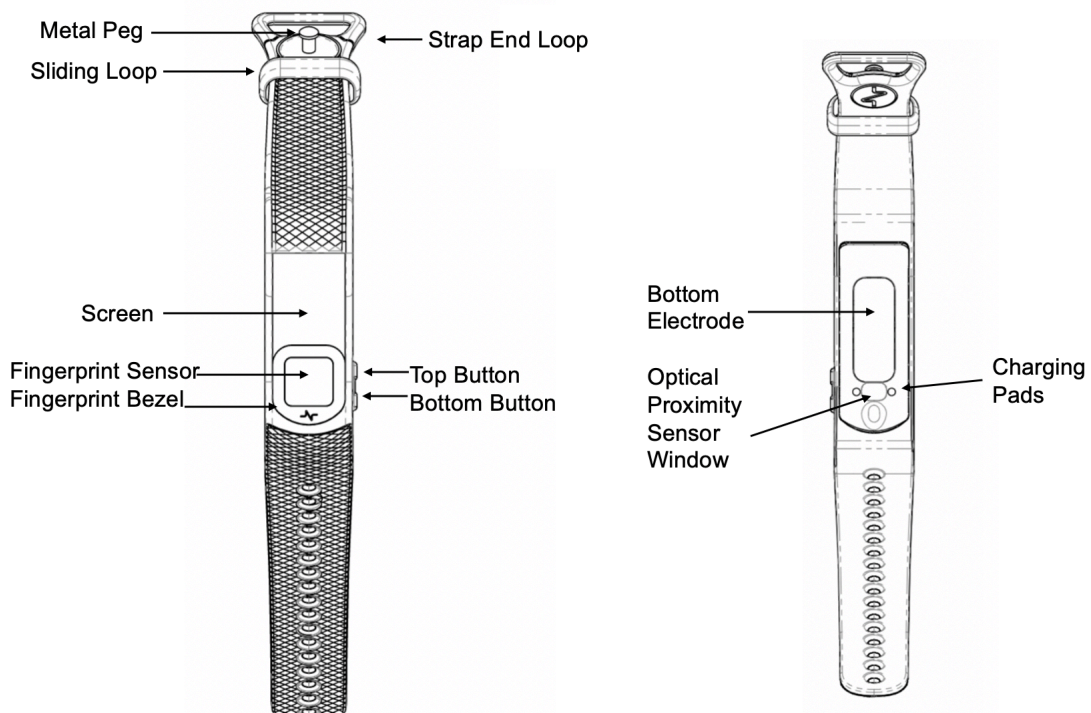
Figure 1: Nymi Band front and back

Figure 2: Nymi Band Strap

The Nymi Band is made up of the following main components:

- Screen—Visual interface on the face of the Nymi Band.
- Fingerprint Sensor—Fingerprint detection pad on the face of the Nymi Band.
- Fingerprint Bezel— Electrode that is used to capture the electrocardiogram (ECG) signal during authentication.
- Top and Bottom Buttons—Turns on the Nymi Band and allows users to navigate through screens. The buttons are also used to access administrative functions while the Nymi Band is charging.
- Charging Pads—Makes contact with the pins of the charger.
- Optical Proximity Sensor Window—Sensor that detects if the Nymi Band is on the wrist of the user.
- Bottom Electrode—Electrode that is used to capture the ECG signal during authentication. Also used to capacitively sense that the Nymi Band is on the user's wrist.
- Metal Peg—Peg that is used to secure the Nymi Band strap while it is on the wrist of the user.
- Sliding Loop—Loop used to keep any excess Nymi Band strap in place while it is on the wrist of the user.
- Strap End Loop—The loop integrated into the strap that helps the user get a good fit on their wrist. The wearer uses the strap loop in the same way that they would use a watch buckle.

The Nymi Band strap contains regulatory markings, a QR code, and the Nymi Band serial number. When scanned, the QR code displays the serial number.

Note: The Nymi Band is shipped with a protective film on the optical sensor and bottom electrode. Remove the protective film before use.

4.2 - Nymi Lock Control

Nymi Lock Control is an application that provides users with the ability to manage access to a terminal, without typing a username and password. Nymi Lock Control verifies user access through Active Directory.

When you install Nymi Lock Control on a user terminal, the following functionality is supported:

Nymi Lock Control provides users with the following functionality on their user terminal:

- Unlocking a terminal by tapping an authenticated Nymi Band on an NFC reader or bluetooth adapter that is attached to the terminal.
- Unlocking a terminal by placing an authenticated Nymi Band within the range of the Bluetooth adapter, and clicking the Submit button on the Nymi Credential Provider Login screen.
- Automatically unlocking or logging into a terminal by being placing an authenticated Nymi Band within range of the Bluetooth adapter and tapping the Enter button or space bar their keyboard.
- Locking the user terminal when the authenticated user is not within the Bluetooth range of the terminal or when the user removes their Nymi Band.
- Preventing a user terminal from locking by keeping an authenticated Nymi Band within Bluetooth range.

4.3 - NFC support

Near Field Communication (NFC) is the wireless technology that allows users to tap the Nymi Band against an NFC reader to gain access to locked terminals or provide an e-signature without typing their corporate credentials. The *Nymi Connected Worker Platform Release Notes* provides more information about supported NFC readers.

Using the NFC Reader

Connect the NFC reader into the USB port of a user terminal (the terminal must have Nymi Bluetooth Endpoint installed). The Nymi Bluetooth Endpoint automatically detects the NFC reader. A Nymi Band user taps the Nymi Band against the NFC Reader to indicate the intent to perform an operation. A user is granted or denied the ability to perform the intended action, based on the policies that are defined in the AD. For example, a user can tap an authenticated Nymi Band on an NFC Reader that is attached to a user terminal and unlock their Windows session.

Multiple Reader Support

The Nymi Bluetooth Endpoint monitors all attached and supported NFC readers and forwards events from all NFC readers (there is no preference between readers).

4.3.1 - Configuring Unverified NFC Readers

This section provides information about how to configure NFC readers that have not been verified by Nymi for use with the Connected Worker Platform.

About this task

Procedure

1. Plug the new NFC reader into a computer with the Nymi Band Application. Windows will automatically install drivers for the NFC reader.
2. After Windows installs the new drivers for the NFC reader on the computer, start the Nymi Band Application.
3. On the Login screen, press Control + Shift + Alt +F10. On some systems you must also press the Fn (function) key.
4. In the list of supported and NFC-detected NFC readers, the new reader will appear with a green plug beside it. Copy exactly the name of the NFC reader. If you do not see the reader, make sure that the device appears in Device Manager and that the driver download has completed successfully.
5. Edit the *nfc-readers.json* file in the *C:\users\Public\AppData\Nymi\unlock* directory.
6. Add an entry for the new reader by performing the following steps:
   a) At the end of the second last } add a , (comma).
   b) Add a new line and an {
   c) Add a new line and then type the name of the NFC reader as it appeared in the Nymi Band Application.
   d) Add a new line and then }
7. Save the file.

Results

The following entry is an example of the HID Omnikey 5025CL reader on Windows 10:

```
        }
        {

            "supportedReader" : "Omnikey 5x25"

        }
        }
```

4.4 - 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 *Nymi Connected Worker Platform— Administration Guide*).

4.5 - Nymi Band Enrollment Process

Enrollment is the process of associating the identity of a user with a Nymi Band. An administrator is not strictly required to be present while a new user enrolls a new Nymi Band; however, for security purposes, a corporate policy might require supervision.

The enrollment process performs the following actions:

1. Assigns the Nymi Band to the enterprise by retrieving the device ID from the Nymi Band and storing it in the Nymi Enterprise Server (NES) database. When the assigning process completes, the Nymi Band is assigned to the enterprise.
2. Creates a fingerprint template on the Nymi Band by capturing a template of the fingerprint of the user and storing the template securely on the Nymi Band. When the creation process completes, the Nymi Band is linked to the user and the user is authenticated to the Nymi Band. Only the Active Directory (AD) username of the user and the associated Nymi Band information are stored in the (NES database.

   Note: The Nymi Band securely stores the fingerprint template. The fingerprint template is never transmitted outside of protected memory.

The Nymi Connected Worker Platform provides an additional method of authentication called a corporate credential authenticator. If the enterprise policy permits it, the Nymi Band Application creates a corporate credential authenticator in addition to the fingerprint authenticator. With a corporate credential authenticator, the Nymi Band trusts the enterprise to validate the user

credentials, such as an AD username and password, before bringing the Nymi Band into an authenticated state.

4.6 - Authentication After Enrollment

Each time that a user removes an authenticated Nymi Band from their wrist, the Nymi Band deauthenticates. For day-to-day usage of the Nymi Band, each time a user puts on the Nymi Band, the user must authenticate their identity to the Nymi Band.

Depending on the defined policy, users authenticate by using one of the following methods, while the Nymi Band is on their wrist:

- By biometrics (fingerprint and optionally liveness detection)—With the Nymi Band on their wrist, the user holds their finger on the fingerprint sensor. The Nymi Band verifies that the fingerprint matches the fingerprint template that is securely stored on the Nymi Band and by default detects liveness.
- By corporate credentials (if a credential authenticator was created)—The user logs into the Nymi Band Application by using their corporate credentials as authentication and, when validation succeeds, the Nymi Band Application puts the Nymi Band into an authenticated state.

5 - Checklist for Nymi Band Distribution and Enrollment

The following checklist provides you with a list of the steps that you need to perform before users can use the Nymi Band in your environment.

Table 2: Nymi Band configuration checklist for users

Completed?	Task
	Remove the Nymi Bands and charging cradles from the box. The Nymi Band, contains enough battery charge to get you through the enrollment activities. The Nymi Band arrives in ship mode, to wake the Nymi Band, press the top bottom. After enrollment, charge the Nymi Bands for at least 2 hours for a full charge. A fully charged Nymi Band battery will typically have a 3-day battery life based on 300 BLE or NFC taps over 10 hours per day.
	Use the NES Administrator Console to Configure a group policy.
	On the enrollment terminal that you will use to enroll users: • Install the Nymi Band Application. • Plug the Nymi-provided Bluetooth Adapter (BLED112) into a USB port. • Import the root certificate into the Trusted Root Certificate Authorities store (if the certificate is not already in the store).
	On the authentication station that you will use to authenticate users by their corporate credentials, when they are experiencing issues authenticating to their Nymi Band with their biometrics: • Install the Nymi Band Application. • Plug the Bluetooth adapter (BLED112) into a USB port. • Import the root certificate into the Trusted Root Certificate Authorities store (if the certificate is not already in the store). **Note:** To use the authentication station, you must enable the Corporate Credentials option in the active group policy. *Configuring Corporate Credentials Authentication* provides more information. The Nymi Support Website provides more information about using an authentication station.
	On each user terminal: • Install the Nymi Band Application, or install Nymi Runtime and the Nymi-enabled Application. • Plug the Bluetooth adapter (BLED112) into a USB port. • Import the root certificate into the Trusted Root Certificate Authorities store (if the certificate is not already in the store).

Completed?	Task
	• Verify that the firmware version on the Nymi Band matches the version on the packing slip. The firmware version is visible when the Nymi Band is plugged into a USB charger and you press the top and bottom button on the Nymi Band. • Unplug the Nymi Band and press any button to verify that the battery icon and NO USER appears on the display of the Nymi Band.
	For Legic Advant-enabled Nymi Bands that you will use with LEGIC Advant Readers, encode the Legic credentials on each Nymi Band.
	Distribute the Nymi Band and a charging cradle to each user. If provided, distribute the Nymi Band Quick Start Guide.
	Walk each user through the Nymi Band enrollment process.

6 - Customizing the CWP Configuration

NES provides NES Administrators with the ability to customize Connected Worker Platform by using policies. Policies contain configuration settings that modify the behaviour of the Connected Worker Platform. NES Administrators can create a new group policy, with configuration settings that apply to all users, create individual user policies that apply to select users, and modify existing policies.

6.1 - Viewing Policies

Use the NES Administrator Console to view Group Polices and Individual User Policies.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing
   https://`nes_server`/`NES_service_name` or ***http://`nes_server`/`NES_service_name`***
   depending on the NES configuration, where:

   - `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
   - `NES_service_name` is the service mapping name for the NES web application. The default service mapping name is *nes.*

   For example, ***https://nes.cwp.company.com/nes***.

   Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.

2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click **Sign In**.

3. From the main window, select **Policies**.
   The `Policies` page appears with a table that displays a list of existing group and individual user policies, and summary information about each policy, as shown in the following figure.

Figure 3: Policies page

4. To view a group policy, in the `Group Policies` pane, from the **`Policy Name`** column, click the link for the policy.

By default, the `Group Policies` displays 5 group policies. Use the navigation controls to move to the between pages of policies and the list to change the number of policies to display on the pane to 10 or 20 per page.

5. To view a individual user policy, perform one of the following actions in the `Individual User Policies` pane.

- Use the expansion control to view the settings that are defined for the policy, as shown in the following figure.

Figure 4: Individual User Policy settings view

- From the **Individual User Policy Name** column, click the link for the policy. By default, the `Individual User Policies` pane displays 10 individual user policies. Use the navigation controls to move between pages of policies and the listbox to change the number of policies to display on the pane to 20 or 50 per page.

6.2 - Manage Group Policies

Use the NES Administrator Console to modify global configuration settings in a group policy, and to create and delete NES group policies.

Note: When a user is assigned to an individual policy, the configuration values in the individual policy take precedence over the value defined for the same configuration attribute in the active group policy.

6.2.1 - Modifying the Default Group Policy

After deploying NES, a default group policy, `Default Settings Set` is configured with the following settings:

About this task

- Save enrollment data to the NES database only.
- Log a user out of the Nymi Band Application after 5 minutes of inactivity.
- Always check for liveness during authentication.
- Do not allow users to re-enroll their Nymi Band or any other active Nymi Band without the need for an CWP Administrator to first delete the Nymi Band to user association in the NES Administrator Console.
- Do not allow users to use the Nymi Band to lock and unlock their user terminals.

To edit the default group policy, perform the following steps.

Procedure

1. Connect to the NES Administrator Console in a browser by typing **https://**`nes_server`**/**`NES_service_name` or **http://**`nes_server`**/**`NES_service_name` depending on the NES configuration, where:

   - `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
   - `NES_service_name` is the service mapping name for the NES web application. The default service mapping name is *nes*.

   For example, **https://nes.cwp.company.com/nes**.

   Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.

2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click **Sign In**.

3. On the `Main` page, click **Policies**.

   The `Policies` page appears. The following figure shows the `Group Policy` pane on the `Policies` page.

   Group Policies
   Applies to all users by default.

Policy Name	Is Active	Created	Modified	Modifier
Default settings set	Active	2022-01-25		EV3-UAT-LAB\EV3-UAT-SRV2$

   < 1 > 5 / Page

   Create New Group Policy

   Figure 5: Group Policies Pane

4. Select the policy that you want to change.

   The `Edit` page appears.

5. Modify the options, as required.

6. Click **Save**.

   The following figure provides an example of the `Edit Group Policy` page for the Default Settings Policy.

Figure 6: Edit Group Policy page

6.2.2 - Creating a New Group Policy

Perform the following steps to create a new group policy.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing
   ***https://*nes_server*/*NES_service_name** or ***http://*nes_server*/*NES_service_name**
   depending on the NES configuration, where:

   - `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
   - `NES_service_name` is the service mapping name for the NES web application. The default
     service mapping name is *nes.*

   For example, ***https://nes.cwp.company.com/nes***.

Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.

2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click `Sign In`.

3. Click `Policies`, and then click `Create New Group Policy`.

The following figure provides an example of the `Group Policies` pane on the Policies page.

Figure 7: Group Policy page

The `Create Group Policy` page appears with the options that are available to customize the enrollment and registration process.

Note: If the `Sign in` screen appears instead of the `Create Policy` page, the user account that you specified is not a member of the NES Administrator group.

4. Configure the options for the group policy, and then click `Save`.

6.2.3 - Changing the Active Group Policy

NES can only have one active policy.

About this task

Perform the following steps to change the policy that is active.

Procedure

1. From the navigation bar, select `Policies`.
The `Policies` page appears with a table that displays a list of existing group and individual policies.

2. In the `Group Policies` pane, in the **`Policy Name`** column, select the policy from the list. The `Edit Policy` window appears.

3. On the `Edit Group Policy` page, select the **`Is Active`** option.

4. At the bottom of the page, click **`Save`**.

6.2.4 - Deleting Group Policies

Perform the following steps to delete group policies that you no longer require.

About this task

You cannot delete an active policy.

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 `Group Policies` pane, select the policy from the list.
   The `Edit Policy` window appears.

4. If the policy that you want to delete is active, then clear the **`Is Active`** option.

5. Click **`Delete`**.

6. On the `Delete Group Policy` window, click **`Delete`**.

   Note: The **`Delete`** button is not enabled if the policy is the active policy, or if only one group policy exists.

7. Edit one of the remaining policies and select the **`Is Active`** option.

   Note: NES must always have one active policy.

8. To the right of `Policy` table, beside the policy that you want to delete, click **`Delete`**.

6.2.5 - Customizing the Enrollment / Registration

The Connected Worker Platform provides enhancements that support the following functionality:

- IT/OT support.
- Coexistence of Evidian-integrated MES applications and Nymi-enabled Applications(NEAs)
- User-driven self re-enrollment of their Nymi Band or any active Nymi Band.

6.2.5.1 - Configuring Nymi Enterprise Server Permissions for IT/OT

To support IT/OT environments, you can configure the Nymi Enterprise Server(NES) permissions. NES permissions restrict NES to perform Nymi Band enrollments only, Nymi Band registrations only, or both Nymi Band enrollment and registrations.

About this task

Perform the following steps to configure NES permissions for each NES server in the IT/OT environment.

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. From the **Enrollment / Registration Permissions** list, select one of the following options:
   - **Enrollment only**—Select this option to assign NES as the server on which users enroll their Nymi Bands.
   - **Registration only**—Select this option to assign NES as the server on which users register their Nymi Bands.

     Note: When you select **Registration only**, you cannot change Nymi Band-related policy settings and they appear greyed out in the `Edit Group` window.
   - **Enrollment and Registration**—Select this option when user accounts are only in the same domain as NES. For example, when there is one instance of an IT domain on which all sites connect.
5. Click **Save**.

   The following figure provides an example of the Group policies page when you select **Registration only**.

Figure 8: Registration Only Group Policy Example

6.2.5.2 - Configuring NES and Evidian Enrollment

Before you begin

By default, Connected Worker Platform supports the use of the Nymi Band to perform authentication tasks with NEAs. When you configure NES to support a Connected Worker Platform solution that is integrated with the Evidian, during the enrollment process, security settings are applied to the Nymi Band and the enrollment process results in information about the Nymi Band appearing in both the NES and Evidian EAM Controller database.

About this task

Perform the following steps to support the Nymi Band for use with Evidian-integrated MES applications and Nymi-enabled Applications.

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. From the **`Enrollment / Registration Destination`** list, select the **`NES and Evidian`** option.

5. Click **`Save`**.

Results

When the user completes the enrollment, information about the Nymi Band appears in the NES and Evidian EAM Controller database.

For existing enrolled Nymi Bands, instruct the user to log into the Nymi Band Application while wearing their authentication Nymi Band. The Nymi Band Application completes the enrollment of the user in the Evidian EAM Controller database.

Reverting to an NES only Enrollment Configuration

Perform the following actions to modify the configuration of a policy to allow users to use the Nymi Band with Nymi-enabled Applications only.

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. From the **`Enrollment /Registration Destination`** list, select the **`NES only`** option.

5. Click **`Save`**.

Results

When the user completes the enrollment, information about the Nymi Band appears in the NES database only.

If you change this option after users have enrolled their Nymi Band, Nymi Band entries for the user remain in the EAM database. The Nymi Connected Worker Platform with Evidian Guide describes how to delete the Nymi Band to user association in the EAM database.

6.2.5.3 - Configuring Self-Service Re-Enrollment and Self-Service Re-Registration

You can allow users to re-enroll; and in an IT/OT environment, re-register their own Nymi Band or any active Nymi Band without the need for a CWP Administrator to log in to the NES Administrator Console and delete the Nymi Band association with the user.

About this task

In an IT/OT environment, Nymi recommends that you define the same values for the options on the Enrollment NES and Registration NES.

Note: Users with HID SEOS-enabled Nymi Bands can only perform self-service re-enrollment and self-service re-registration with their own Nymi Band. To reuse an already enrolled SEOS-enabled Nymi Band, a CWP Administrator must disassociate the Nymi Band from the original user before another user can enroll or register the Nymi Band.

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. From the `Enrollment / Registration Settings` section, select one or both of the following options:

Option	Description
Allow a user to re-enroll / re-register their Nymi Band	Users with an active Nymi Band can re-enroll and re-register their active Nymi Band without the need for an CWP Administrator to first disassociate the Nymi Band. Users can also enroll and register to a Nymi Band that is not associated with another user.
Allow a user to re-enroll any active Nymi Band	User with an active Nymi Band can re-enroll and re-register to any Nymi Band with the exception of an HID SEOS-enabled Nymi Bands that are associated to another user in NES. When a user re-enrolls or re-registers to a non-SEOS-enabled Nymi Band that is associated with another user, the process removes the association with its previous user in NES. A user cannot re-enroll or re-register to a SEOS-enabled Nymi Band that is associated with a user, until a CWP Administrator disconnects the from the current user.

   The **Allow a user to re-enroll / re-register any active Nymi Band** option only appears after you enable the **Allow a user to re-enroll /re-register their Nymi Band** option.
5. Click `Save`.

Reverting the Self Re-Enrollment or Self Re-Registration Configuration

Perform the following actions to modify the configuration of a policy to disallow users from performing self-service re-enrollments and self-service re-registrations.

About this task

In an IT/OT configuration, Nymi recommends that the following policy setting match on the Registration NES and Enrollment NES. In an IT/OT configuration, perform the following steps on both Nymi Enterprise Servers(NES).

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. From the `Enrollment and Registration Settings` section, clear the `Allow a user to re-enroll/re-register their Nymi Band` option.
5. Click `Save`.

6.2.6 - Customizing the Nymi Band Authentication Method

The Nymi Band supports authentication by fingerprint only, a combination of fingerprint and liveness detection, and authentication by the Active Directory credentials of the user.

By default,

Policies allow you to define the methods that a user can use to authenticate to their Nymi Band. The following table summarizes the authentication method options that are available to you in a group policy and the advantages and disadvantages of each option.

Table 3: Authentication method advantages and disadvantages

Setting	Advantage	Disadvantage
Corporate Credentials = disabled Liveness Detection = disabled **Note:** This is the default configuration for new installations.	• Biometric guarantee of the identity of the user. • Authentication by fingerprint does not check for an ECG signal.	• Authentication by fingerprint does not check for an ECG signal. • User cannot authenticate by using their corporate credentials when authentication by fingerprint fails.

Setting	Advantage	Disadvantage
Corporate Credentials = disabled Liveness Detection = enabled	• Biometric guarantee of the identity of the user. • Authentication by fingerprint also checks for an ECG signal.	• Authentication might fail when the fingerprint is dirty, cut, too wet or too dry, or when the fingerprint sensor is not clean. • A small percentage of the population has difficulty providing stable ECG to the Nymi Band during authentication,which results in the liveness check and authentication to fail.
Corporate Credentials = enabled Liveness = enabled	• Authentication by fingerprint also checks for an ECG signal. • Allows a user to authenticate to authenticate by using their corporate credentials when authentication by fingerprint fails due to a fingerprint or ECG signal failure.	• A small percentage of the population has difficulty providing stable ECG to the Nymi Band during authentication,which results in the liveness check and authentication to fail. • For a user to authenticate by corporate credentials, the user must have access to the Nymi Band Application, and log into the Nymi Band Application with their corporate credentials. • Corporate Credentials Authentication does not: • Provide a biometric guarantee of the of the identity of the user. • Guarantee that the user who supplied password is the correct user.

Setting	Advantage	Disadvantage

Corporate Credentials = enabled
 	
Liveness = disabled
	• Authentication by fingerprint does not check for an ECG signal.
	• Allows a user to authenticate by using their corporate credentials when authentication by fingerprint fails.
		• Users who experience issues providing a stable ECG to the Nymi Band can authenticate the Nymi Band with their fingerprint.
		• Authentication by fingerprint does not guarantee that the user who is wearing the Nymi Band is the user that is wearing the Nymi Band.
		• Corporate Credentials Authentication does not:
		
		    • Provide a biometric guarantee of the user's identity.
		    • Guarantee that the user who supplied the password is the correct user.

6.2.6.1 - Configuring Corporate Credentials Authentication

Perform the following steps to configure the Nymi Band Application to create a corporate credential authenticator for a user during enrollment, which allows a user to authenticate the Nymi Band by Active Directory username and password.

About this task

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. From the **Enrollment Settings** section, select the option **Corporate Credentials Authentication**.
5. Click **Save**.

Results

When a user enrolls their Nymi Band, the Nymi Band Application creates a corporate credential authenticator on the Nymi Band. For subsequent authentications of the Nymi Band, if the user cannot authenticate by fingerprint, the user can log into the Nymi Band Application while wearing their Nymi Band, and the Nymi Band Application can authenticate the user to their

Nymi Band, based on the AD credentials that were used to log into the that enables users to the Nymi Band Application.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

The Nymi Band Application creates a corporate credential authenticator on the Nymi Band.

Disabling Corporate Credentials Authentication
Perform the following steps to disable corporate credentials authentication in an NES policy.

About this task

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. From the `Enrollment Settings` section, clear the option `Corporate Credentials Authentication`.
5. Click `Save`.

Results
When a user enrolls their Nymi Band, the Nymi Band Application does not create a corporate credentials authenticator on the Nymi Band and the user can only authenticate with their fingerprint.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

The Nymi Band Application removes the corporate credential authenticator from the Nymi Band.

6.2.6.2 - Configuring Liveness Detection
Perform the following steps to disable the liveness check during authentication by fingerprint.

About this task

In IT/OT environments, the Enrollment NES manages the `Liveness Detection` policy setting. The option appears greyed out on the Registration NES.

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 `Authentication Settings` section, clear the `Liveness Detection` option.
5. Click `Save`.

Results

During enrollment the Nymi Band Application updates the Nymi Band to suppress the liveness check when a user performs an authentication by fingerprint.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

Enabling Liveness Detection

Perform the following steps to enable Liveness Detection in an NES policy.

About this task

By default, Liveness Detection is disabled.

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 `Authentication Settings` section, select the `Liveness Detection` option.
5. Click `Save`.

Results

During enrollment the Nymi Band Application updates the Nymi Band to enable the liveness check when a user performs an authentication by fingerprint.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

6.2.7 - Customizing the Nymi Band Label

The Connected Worker Platform provides you with the ability to customize what a user sees on the Nymi Band screen after enrollment, for example an identifying label.

The Band Label is a text label that the enrollment process adds on the Nymi Band, which helps users to identify their Nymi Band. For example, when Nymi Bands are in the charging station, a user can identify which Nymi Band belongs to them. By default, the Band Label feature is disabled.

Nymi supports two types of band labels:

- The name of the user as it appear in Active Directory
- A customized band label that the user defines during enrollment

In IT/OT environments, the Enrollment NES manages the `Nymi Band Label` policy setting. The option appears greyed out on the Registration NES.

6.2.7.1 - Configuring a Band Label on the Nymi Band

Perform the following steps to set a label on the Nymi Band.

About this task

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 **Enrollment Settings** section, select **Display Band Label on Nymi Bands**

   The **Allow Band Label Customization** option appears.

   Perform one of the following actions:

   - Leave the **Allow Band Label Customization** cleared to display the first 12 characters of the Active Directory username for the user on the Nymi Band. The Nymi Band displays the Band Label as two rows of six characters.
   - Select **Allow Band Label Customization** to enable users to customize the Band Label that displays on their Nymi Band. Users must re-enroll to customize the Band Label on the **Set Band Label** screen during enrollment.
5. Click **Save**.

Results

During enrollment, the Nymi Band Application displays a band label screen to the user with the first 12 characters of their Active Directory username. When **Allow Band Label Customization** is enabled, the user can modify the label.

If you enable the `Display Band Label on Nymi Bands` option after enrollment has completed for users, users can apply this change to their Nymi Band by logging into the Nymi Band Application while wearing their authenticated Nymi Band. The Nymi Band Application applies changes to the Nymi Band to display the Active Directory username of the user.

If you enable the `Allow Band Label Customization` after enrollment has completed for users, the users must re-enroll their Nymi Band to set a customized band label.

6.2.7.2 - Disabling Band Label

Perform the following steps to disable the ability to create a label on a Nymi Band during enrollment.

About this task

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 `Enrollment Settings` section, perform one of the following actions:

   - To disable the creation of a customized band label during enrollment but allow the band label to contain the first 12 characters of the Active Directory name of the user, clear the `Allow Band Label Customization` option.
   - To disable the creation of a band label during enrollment, clear the `Display Band Label on Nymi Bands` option.

5. Click `Save`.

Results

The user is not provided with the option to create a band label during enrollment.

Disabling the band label option does not change the state of the band label on the Nymi Band for existing enrolled users. The users must re-enroll their Nymi Band.

6.2.8 - Customizing Connected Worker Platform to support NEAs that check AD status

The Nymi SDK allows vendors to customize applications that support the Nymi Band to complete authentication tasks.

NEAs can to respond to a request to perform an authentication task with the Nymi Band, based on the status of the account for the user in AD. For example, if a user performs an NFC tap to complete an e-sign off, and user's active directory password has expired, the e-sign off attempt does not complete.

By default, the option to support a check of the user status is disabled. If the NEA vendor programatically enables the NEA to check the status of a user in Active Directory before completing an authentication task with the Nymi Band, update the active policy to enable NES to provide NEAs with the status of a user account in Active Directory, and optionally customize the frequency with which NES contacts AD.

When you enable the option in the NES policy to determine the status of a user in AD, upon the first request for the status of a user, NES contacts AD for the information and returns the result to the NEA.

6.2.8.1 - 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.
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

Option	Description
	cache expiry value, NES contacts AD for the user status and stores the results in cache again.

6.2.9 - Customizing Nymi Lock Control Support

Nymi Lock Control is a NEA created by Nymi that supports the use of an authenticated Nymi Band to lock and unlock a Windows user terminal. By default, Nymi Lock Control support is disabled in NES

Note: If your environment uses Organization Units to limit the user terminals that use Nymi Lock Control, ensure that you add each user terminal to the Organizational Unit.

6.2.9.1 - Configuring Nymi Lock Control

Perform the following steps to enable and configure Nymi Lock Control.

About this task
By default Nymi Lock Control is not enabled.

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 options appear to customize Nymi Lock Control.

Option	Description
Lock When Away	• Configure Nymi Lock Control with the ability to lock the user terminal when Nymi Lock Control does not detect the authenticated Nymi Band. • Default: Enabled • When enabled, Nymi Lock Control locks the user terminal when a user removes an authenticated Nymi Band or when the Nymi Band is not in close proximity of the user terminal. When the Nymi Band is out of range, a 10 second timer appears on the desktop. If the Nymi Band does not return within close range of the user terminal, the terminal will lock.

Option	Description
	Ensure that your Group Policy Object(GPO) settings do not push the *Do not display the lock screen* configuration option to the Nymi Lock Control user terminals. **Note:** Edit the *nbe.toml* file to define close proximity for Nymi Lock Control. Refer to *Editing the nbe.toml File*.
Unlock When Present	• Configures Nymi Lock Control to check if the Nymi Band is in close proximity before unlocking the user terminal. If not, then unlock fails. You can define how close the Nymi Band must be to the user terminal to allow the user to unlock the terminal with the Nymi Band in the *nbe.toml* file. • Default: Enabled • When enabled, prevents an unauthorized user from unlocking the user terminal while the Nymi Band user is in Bluetooth range, but not in close proximity to the terminal. • When disabled, allows a user to unlock the user terminal by pressing the **Enter** key or space bar on the keyboard when the authenticated Nymi Band is within Bluetooth range, but not in close proximity of the user terminal.
Keep Unlocked when Present	• Provides you with the ability to define how the Nymi Band interacts with operating system screen timeouts or sleep settings that lock the user terminal. • Default: Enabled • When enabled, overrides any system screen timeouts or sleep settings, and keeps the user terminal unlocked as long as the Nymi Band is present and authenticated. • When disabled, prevents Nymi Lock Control from overriding any system screen timeouts or sleep settings.

5. Click **Save**.

Results

During enrollment the Nymi Band Application updates the Nymi Band to enable Nymi Lock Control support.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

When the Nymi Band Application updates on the Nymi Band completes, restart Nymi Lock Control.

6.2.9.2 - Disable Nymi Lock Control

You can disable Nymi Lock Control for all users or for certain user terminals.

Disabling Nymi Lock Control for All Users

Edit the active Nymi Enterprise Server(NES) group policy to disable Nymi Lock Control for all users.

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, clear the **Enable Nymi Lock Control** option.
5. Click **Save**.

Results

After a user enrolls their Nymi Band, they cannot use the Nymi Band to lock and unlock their terminal.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

Disabling Nymi Lock Control Access on User Terminals

You can use Organizational Units(OUs) to control the user terminals that use Nymi Lock Control. The *Nymi Connected Worker Platform—Deployment Guide* describes how to configure the solution to use OUs.

About this task

To disable the use of Nymi Lock Control on user terminals, perform the following steps:

Procedure

1. Edit the OU in Active Directory, and remove the user terminal.
2. Optionally, uninstall the Nymi Lock Control software.

Note: If you do not uninstall the Nymi Lock Control software, a user with a Nymi Lock Control cannot tap to unlock the user terminal, but when the user removes their Nymi Band or moves out of Bluetooth range, the desktop locks.

6.2.10 - Customizing Haptic Feedback on Nymi Bands

The Connected Worker Platform provides you with the ability to disable haptic feedback on the Nymi Bands for all users or for individual users.

Review the following sections for information about customizing haptic feedback on the Nymi Bands for all users. For information about customizing haptic feedback for individual users, refer to *Managing Individual User Policies*.

In IT/OT environments, the Enrollment NES manages the `Haptic Feedback` policy setting. The option appears greyed out on the Registration NES.

6.2.10.1 - Disabling Haptic Feedback on Nymi Bands

By default haptic feedback is enabled for all Nymi Bands.

About this task

Perform the following steps to disable haptic feedback for all Nymi Bands.

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 `Health and Safety` section, clear the option `Haptic Feedback on Nymi Bands`.
5. Click `Save`.

Results

The Nymi Bands will not vibrate upon completion of specific events. The *Nymi Band Vibration* section describes the events that trigger Nymi Bands to vibrate.

Note: Update your instructions in your Standard Operating Procedures (SOPs) to instruct the user to immediately stop using the Nymi Band if a vibration occurs when they authenticate to their Nymi Band.

6.3 - Manage Individual User Policies

After deploying NES, two default individual user policies are available.When you add a user to an individual policy, the configuration values in the individual policy take precedence over the value defined for the same configuration attribute in the active group policy.

Use the NES Administrator Console to create, and delete, and add users to an existing or new individual user policy.

User experiences the following behaviour in the existing individual group policies:

- Liveness Detection Disabled—Biometric authentication of the Nymi Band only validates that there is a fingerprint match and does not perform a liveness check. By default, haptic feedback is enabled on the Nymi Band and the user cannot perform a self-re-enrollment on their Nymi Band or another active Nymi Band.
- Corporate Credentials Authentication—Biometric authentication and corporate credential authentication is supported. By default, haptic feedback is enabled on the Nymi Band and the user cannot perform a self-re-enrollment on their Nymi Band or another active Nymi Band. To authenticate a Nymi Band by corporate credentials, the user logs into the Nymi Band Application with their username and password, while wearing their unauthenticated Nymi Band. *Customizing the Nymi Band Authentication Method* provide more information about using Corporate Credentials Authentication.

Note: In an IT/OT configuration, you can only manage liveness detection and haptic feedback from the Enrollment NES.

6.3.1 - Creating an Individual User Policy

Before you begin
Ensure that you connect to the appropriate NES to create individual user policies that manage policy options for enrolled users. The Registration NES cannot manage the `Liveness Detection` or the `Haptic Feedback` policy options. The following figure provides an example of the message that appears for `Individual User Policies` on the Registration NES.
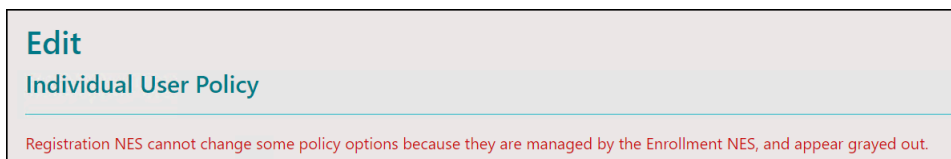
About this task
Perform the following steps to create a new individual user policy.

Procedure

1. Connect to the NES Administrator Console in a browser by typing
   https://`nes_server`/`NES_service_name` or ***http://`nes_server`/`NES_service_name`***
   depending on the NES configuration, where:

   - `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
   - `NES_service_name` is the service mapping name for the NES web application. The default service mapping name is *nes*.

     For example, ***https://nes.cwp.company.com/nes***.

     Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables.* You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.

2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click **`Sign In`**.

3. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.

4. On the **`Individual User Policies`** pane, click **`Create New Individual User Policy`**.
   The **`Create New Individual User Policy`** page appears.

5. In the **`Individual User Policy Name`** field, type a name for the policy.

6. Select the required policy options.

7. Optionally, in the **`Notes`** field, provide some descriptive text.
   The following figure provides an example of a new individual user policy with both the **`Allow a user to re-enroll their Nymi Band`** and **`Corporate Credentials Authentication`** options are enabled, and the **`Liveness Detection`**, **`Haptic Feedback on Nymi Bands`**, and the **`Allow a user to re-enrol to any active Nymi Band`** options are disabled.

Figure 9: Create Individual Policy page

8. Click **Create**.

The new policy appears in the **Individual User Policies** pane of the `Policies` page.

What to do next

After you create the policy, add users to the policy. *Adding a User to an Individual Policy* provides more information.

6.3.2 - Creating an Individual User Policy from an Existing Individual User Policy

Perform the following steps to create an individual user policy by copying an existing policy.

Procedure

1. Connect to the NES Administrator Console in a browser by typing
https://nes_server/NES_service_name or ***http://nes_server/NES_service_name***
depending on the NES configuration, where:

- *nes_server* is the Fully Qualified Domain Name (FQDN) of the NES host.
- *NES_service_name* is the service mapping name for the NES web application. The default service mapping name is *nes*.

   For example, ***https://nes.cwp.company.com/nes***.

   Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.

2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click **`Sign In`**.

3. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.

4. On the **`Individual User Policies`** pane, select an existing policy.
   The `Edit Individual User Policy` window appears.

5. Click **`Make a Copy`**, as shown in the following figure.

Figure 10: Make a Copy button

   The `Create Individual User Policy` window appears.

6. In the **`Individual User Policy Name`** field, type a name for the policy.

7. Select the required policy options.

8. Optionally, in the **`Notes`** field, provide some descriptive text.
   The following figure provides an example of a new individual user policy with both the **`Allow a user to re-enroll their Nymi Band`** and **`Corporate Credentials Authentication`** options are enabled, and the **`Liveness Detection`**, **`Haptic Feedback on Nymi Bands`**, and the **`Allow a user to re-enrol to any active Nymi Band`** options are disabled.

Figure 11: Create Individual Policy page

9. Click **Create**.

The new policy appears in the **Individual User Policies** pane of the `Policies` page.

What to do next

After you create the policy, add users to the policy. *Adding a User to an Individual Policy* provides more information.

6.3.3 - Deleting an Individual User Policy

Perform the following steps to delete an individual user policy.

Procedure

1. Connect to the NES Administrator Console in a browser by typing ***https://***`nes_server`***/***`NES_service_name` or ***http://***`nes_server`***/***`NES_service_name` depending on the NES configuration, where:

- `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
- `NES_service_name` is the service mapping name for the NES web application. The default service mapping name is *nes*.

   For example, ***https://nes.cwp.company.com/nes***.

   Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.

2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click **Sign In**.

3. From the navigation bar, select **Policies**.

The `Policies` page appears with a table that displays a list of existing group and individual policies.

4. On the **`Individual User Policies`** pane, in the **`Individual User Policy Name`** column, select the policy.

5. Click **`Delete`**.

6. On the `Delete Individual User Policy` window, click **`Delete`**.

Results

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

6.3.4 - Adding a User to an Individual User Policy

Perform the following steps to add users to individual policy.

Procedure

1. Connect to the NES Administrator Console in a browser by typing ***https://`nes_server`/`NES_service_name`*** or ***http://`nes_server`/`NES_service_name`*** depending on the NES configuration, where:

   • `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
   • `NES_service_name` is the service mapping name for the NES web application. The default service mapping name is *nes*.

   For example, ***https://nes.cwp.company.com/nes***.

   Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.

2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click **`Sign In`**.

3. On the `Main` page, click **`Search`**.
   The `Search` page appears.

4. With the **`Users`** option selected, in the **`Search`** field type the username of the user, and then click **`Search`**.

   The `Search` page displays the results of the search. The `Search Results` window appears with a list of users. By default, the search results display 10 individual user policies. The **`Individual User Policy`** column displays the name of the individual policy that is assigned to a user. If a user is not assigned to an individual user policy, *none[group policy applied]* appears. Use the navigation controls to move between the pages of users and the list box to change the number of users to display on the pane to 20 or 50 per page.

5. In the **`Search`** results, select the user.
   The `User` properties page appears.

6. From the **`Individual User Policy`** list, select the policy.

The following figure provides an example of the `User` properties page with the Liveness Detection Enabled policy selected.
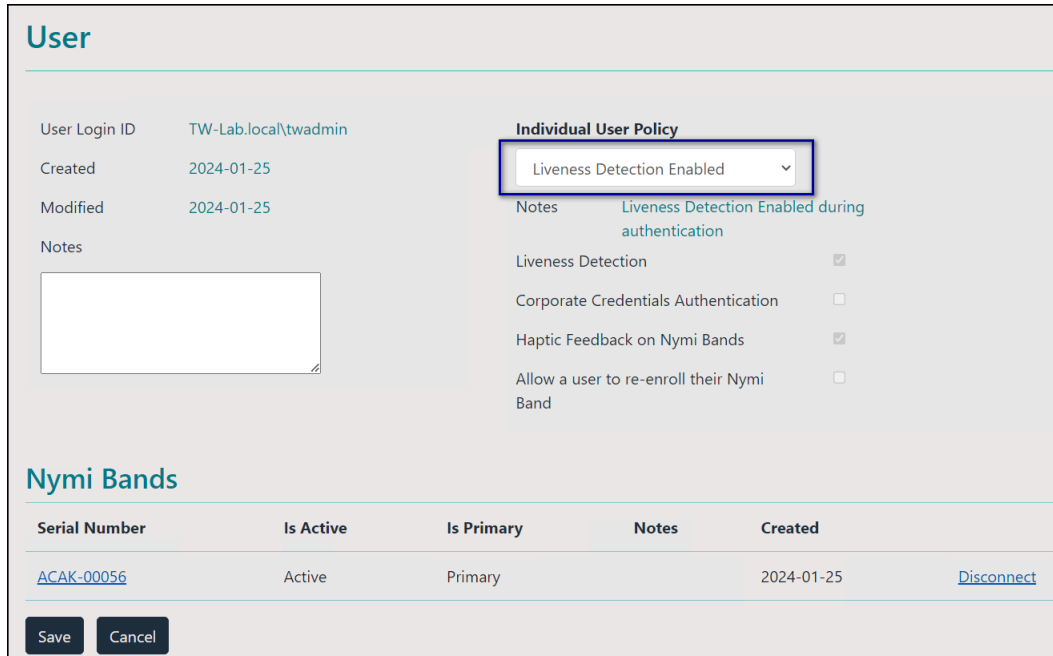
Figure 12: User Properties page

7. Click `Save`.

Results

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

6.3.5 - Displaying Individual User Policy Membership

Perform the following steps to display a list of users that are a member of an individual user policy, while on the `Policies` page.

Procedure

1. On the `Individual User Policies` pane, select the individual user policy. The `Edit Individual User Policies` appears.
2. Click the link **This individual user policy is applied to x user(s)**, as shown in the following figure.

Figure 13: Edit Individual User Policy page

The `Search` window appears and displays a list of users.

The search results include information about the status of the application of a policy to a user. There are four status types:

- No active Nymi Band—The user does not have an active Nymi Band.
- Pending—The policy on the Nymi Band does not match the policy (individual user policy or global policy) that is applied to the user. For example, the policy was applied to the user after enrollment, and the user has not signed into the Nymi Band Application while wearing their authenticated Nymi Band to activate the policy changes.

  Note: CWP 1.1 is the minimum firmware version that supports the ability to configure liveness detection. If you disable liveness detection in the NES group policy or an individual user policy and the Nymi Band firmware does not support configurable liveness detection, the policy status for the Nymi Band remains in the "Pending" state.

- Active—The policy on the Nymi Band matches the policy (individual user policy or global policy) that is applied to the user.
- Information unavailable—Enrollment occurred on an earlier version of Nymi Band Application that does not support the policy status features. Individual policy support starts with the CWP 1.3 Nymi Band Application.

The `Search Results` window appears with a list of users. By default, the search results display 10 individual user policies. The **Individual User Policy** column displays the name of the individual policy that is assigned to a user. If a user is not assigned to an individual user policy, *none[group policy applied]* appears. Use the navigation controls to move between the pages of users and the list box to change the number of users to display on the pane to 20 or 50 per page. The following figure provides an example of the `Search Results` window.

Figure 14: Individual User Policy Search Results

7 - Nymi Band Enrollment

This section provides detailed instructions about how to enroll a Nymi Band.

To enroll the Nymi Band, the user requires access to enrollment terminal. The user can enroll the Nymi Band by following the instructions that appear in the Nymi Band Application and on the Nymi Band screen. With Nymi Band 3.0, the enrollment process provides the ability to display a Band Label on the Nymi Bands screen to help users identify their Nymi Bands when the option is configured in the active policy.

7.1 - Enrollment Prerequisites

Before you enroll an HID SEOS or Legic Advant-enabled Nymi Band, review the following information.

For Legic Advant-enabled Nymi Bands that you will use with LEGIC Advant Readers, ensure that you encode the Legic credentials on each Nymi Band before enrollment.

For SEOS-enabled Nymi Bands, use the CSV file that Nymi provided to you with your purchase order to import information about the SEOS-enabled Nymi Bands in the NES database. The following section provides more information.

7.1.1 - Importing SEOS-Enabled Nymi Band information into NES

Each time you place a order for SEOS-enabled Nymi Bands, Nymi provides you a CSV that contains important information about the Nymi Bands.

About this task

Note: Ensure that you upload the information about the SEOS-enabled Nymi Bands before a user enrolls to the Nymi Band.

Nymi attaches the CSV file to the purchase order email.

Procedure

1. Copy the *CSV* file to a folder on the NES server.

   Note: Do not modify the *CSV* file. Changes to the *CSV* can prevent successful enrollment.
2. Log into the NES Administrator Console on the NES server with an NES Administrator account.
3. On the menu bar, click **Search**.

4. In the `Search` window, click **Nymi Bands**, and then click **Import**

The following figure shows the `Search` window.
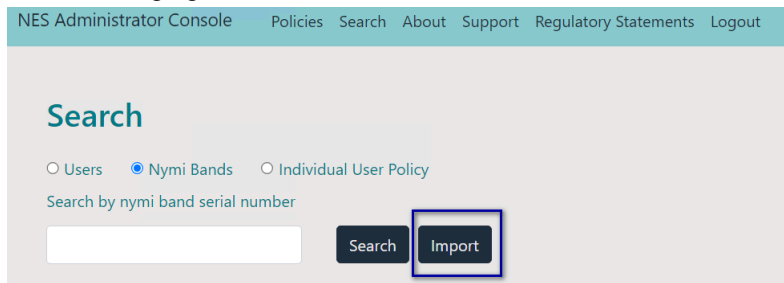
Figure 15: Import option in Search window

5. On the **Import Nymi Bands** window, click **Browse** as shown in the following figure
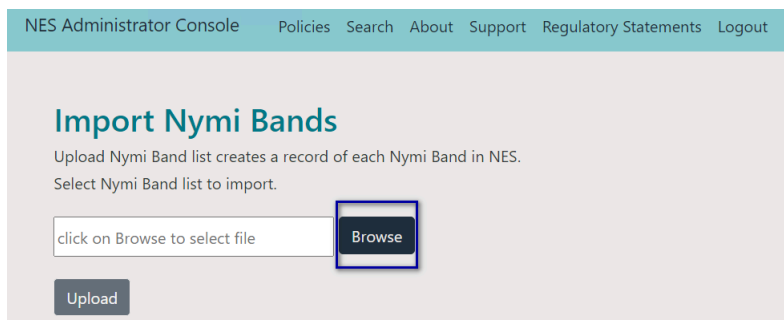
Figure 16: Browse in Import Nymi Bands window

6. In the `Open` window, navigate to the folder that contains the CSV file, select the *CSV* file, and then click **Open**.

The path and filename appear in the **Import Nymi Bands** window, as shown in the following figure.
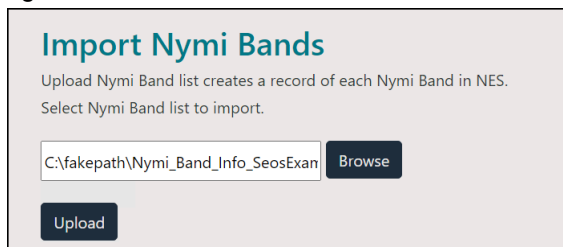
Figure 17: Import file window with filename

Note: Some browsers display the path of the file as *C:\fakepath*. It is not necessary to correct the path.

7. Click **Upload**.

The import operation completes. The import feature updates the NES database with information for new Nymi Bands. If the import detects existing Nymi Bands, the operation retains existing information and updates the database with new information only.

If the import operation encounters a problem, the `Import Nymi Bands` window indicates an error. To review error messages, click **Download records**, as shown in the following figure.
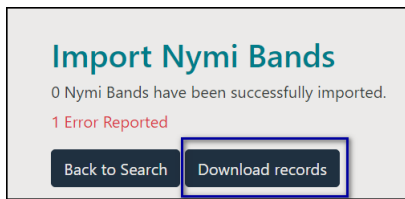
Figure 18: Nymi Band Import error

The NES Administrator Console creates a *CSV* file named *InvalidUploadsData* in the *Downloads* folder. Open the file and review the error message that appears in the last column for each that encountered an issue.

7.2 - Validating User Identity and User Intent

To ensure compliance with CFR 21 Part 11, the enrollment process includes steps that assure user identity and requires the user to acknowledge their intent to use the Nymi Band to perform e-signatures.

Before you begin
Plug the Bluetooth adapter into a USB port on the enrollment terminal. Ensure that the Bluetooth adapter is easily accessible to each Nymi Band user, as the enrollment process requires the user to tap their Nymi Band against the Bluetooth adapter. You can use a USB extension cable when a user cannot easily access the USB ports."

About this task

Instruct the user to perform the following steps on the enrollment terminal to start the enrollment process and verify the identity of the Nymi Band user.

Procedure

1. Start the Nymi Band Application by double-clicking the Nymi Band Application icon on the desktop.
2. On the `The Setting Up Your Nymi Band` screen, perform the following actions:
   a) Press the top button on the Nymi Band, wait for the Nymi Band to wake up, and then tap the Nymi Band against the Bluetooth adapter.

   The following figure shows the `Setting Up Your Nymi Band` screen and provides examples of what you might see on the Nymi Band screen when the Nymi Band is fully awake .
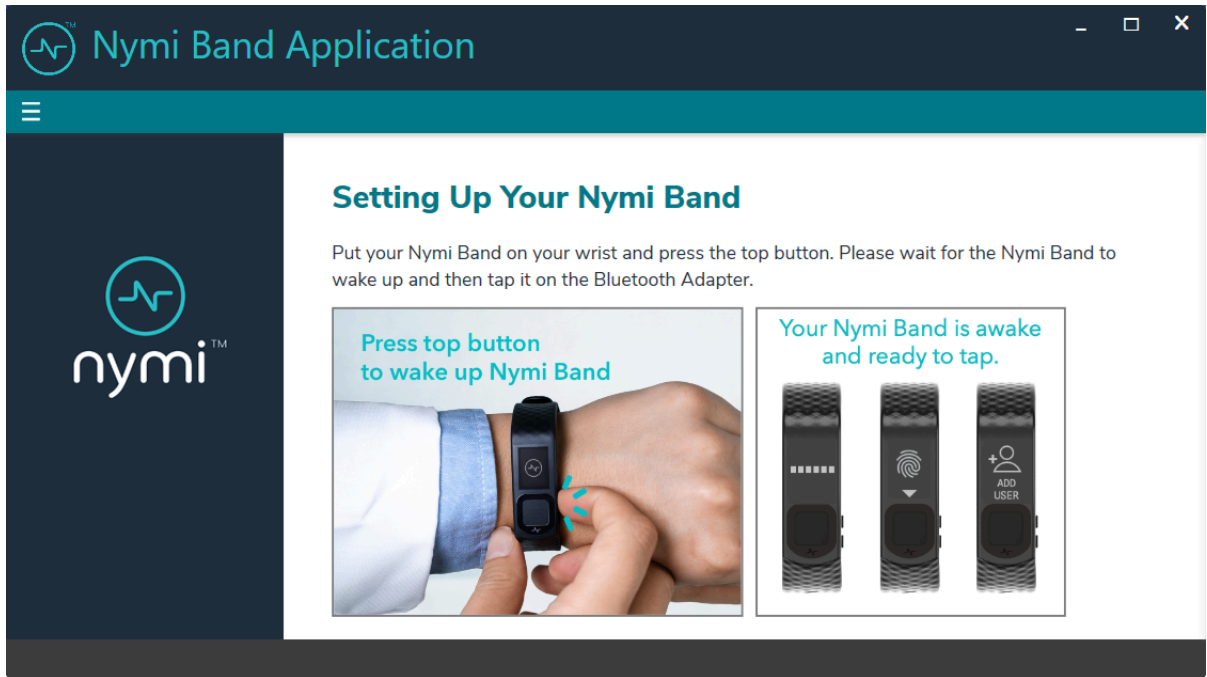
Figure 19: Setting Up Your Nymi Band

The Nymi Band Application sends information about the Nymi Band to NES and establishes a connection with the Nymi Band.

Note: If the user removes their Nymi Band or walks away from the terminal at any point after they perform the tap, the enrollment process ends, and the Nymi Band Application logs out the user. To continue the enrollment process, instruct the user to log into the Nymi Band Application again while wearing their Nymi Band.

b) Read Nymi Band statement of understanding and intent, type their Nymi Band username and password, and then click **Continue** to acknowledge that they have read and understand the statement.

The following figure provides an example of the Setting Up Your Nymi Band that shows that the application has a connection to the Nymi Band and prompts the user to provide their username and password.
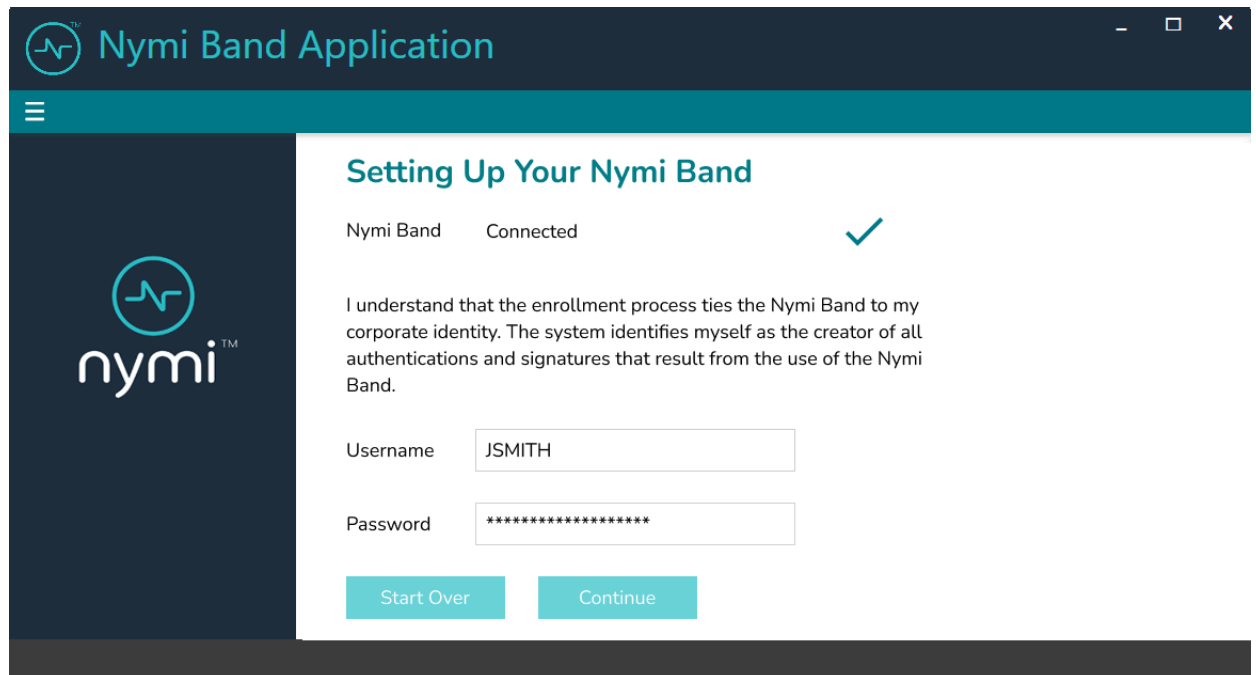
Figure 20: Setting Up Your Nymi Band

The `Setting Up Your Nymi Band` verifies the user credentials and displays an acknowledgement message.

c) When prompted, instruct the user to tap their Nymi Band to continue.

The following figure provides an example of the `Setting Up Your Nymi Band` that prompts the user to tap their Nymi Band on the Bluetooth adapter.
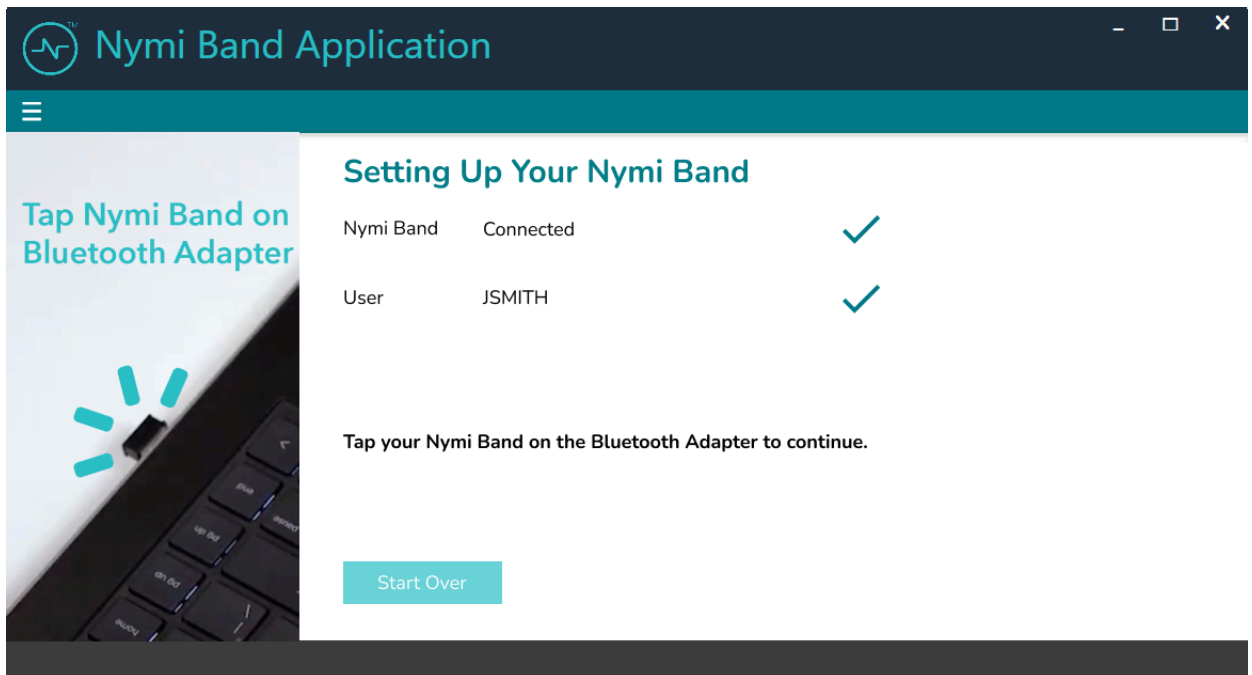
Figure 21: Setting Up Your Nymi Band

Results

In the Nymi Band Application the `Capture Fingerprint` page appears. The following section describes the fingerprint capture process.

7.3 - Capturing the Fingerprint

To uniquely identify a user as the owner of the Nymi Band, the enrollment process captures a fingerprint image on the Nymi Band and stores it as a fingerprint template. The fingerprint template never leaves the Nymi Band. The Nymi Band can only be assigned to one individual.

About this task

To increase the success of the fingerprint capture process, ensure that the fingerprint sensor on the Nymi Band is clean and dry. Additionally, ensure that the finger that the user uses:

- Is placed on the sensor only when prompted
- Is lifted from the sensor only when prompted
- Is placed on the middle of the sensor and covers as much of the sensor as possible
- Is motionless on the sensor, while the sensor is capturing the image

Instruct the user to performs the following steps to create a fingerprint template on the Nymi Band.

Procedure

1. Read the information on the `Capture Fingerprint` page.

   The following figure provides an example of the `Capture Fingerprint` page.
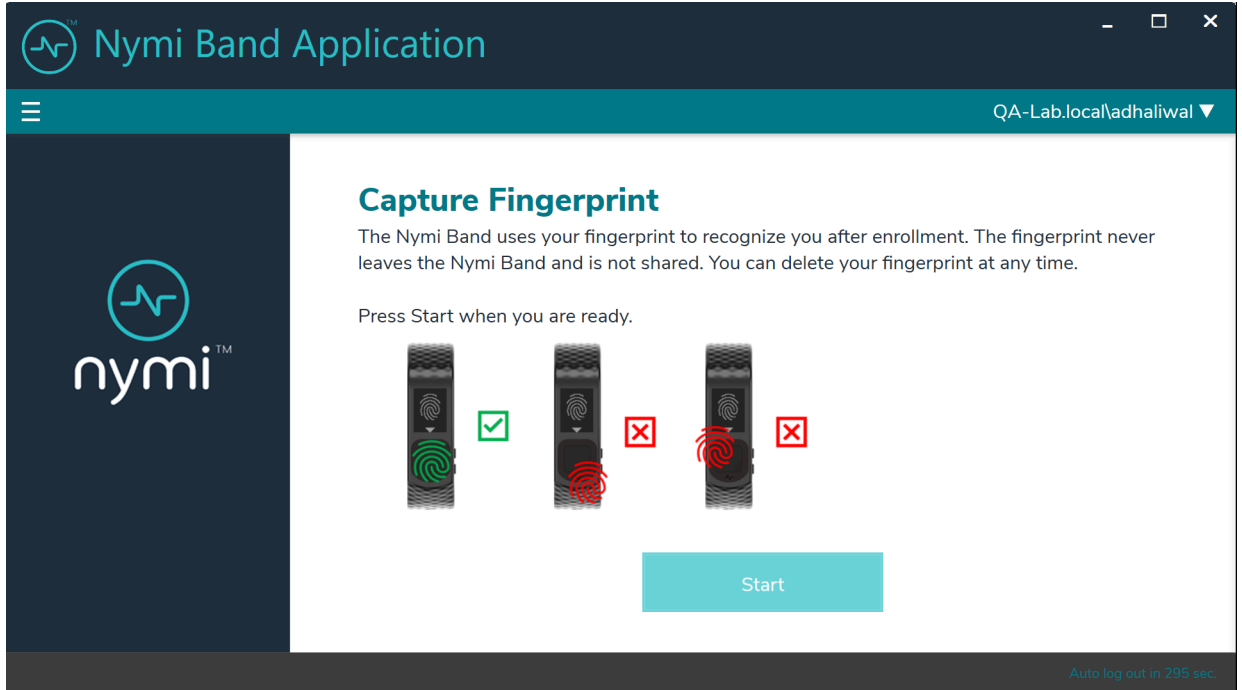
Figure 22: Capture Fingerprint

2. Click **Start**.

   The following figure provides an example of the `Capture Fingerprint` page after the user clicks **Start**.
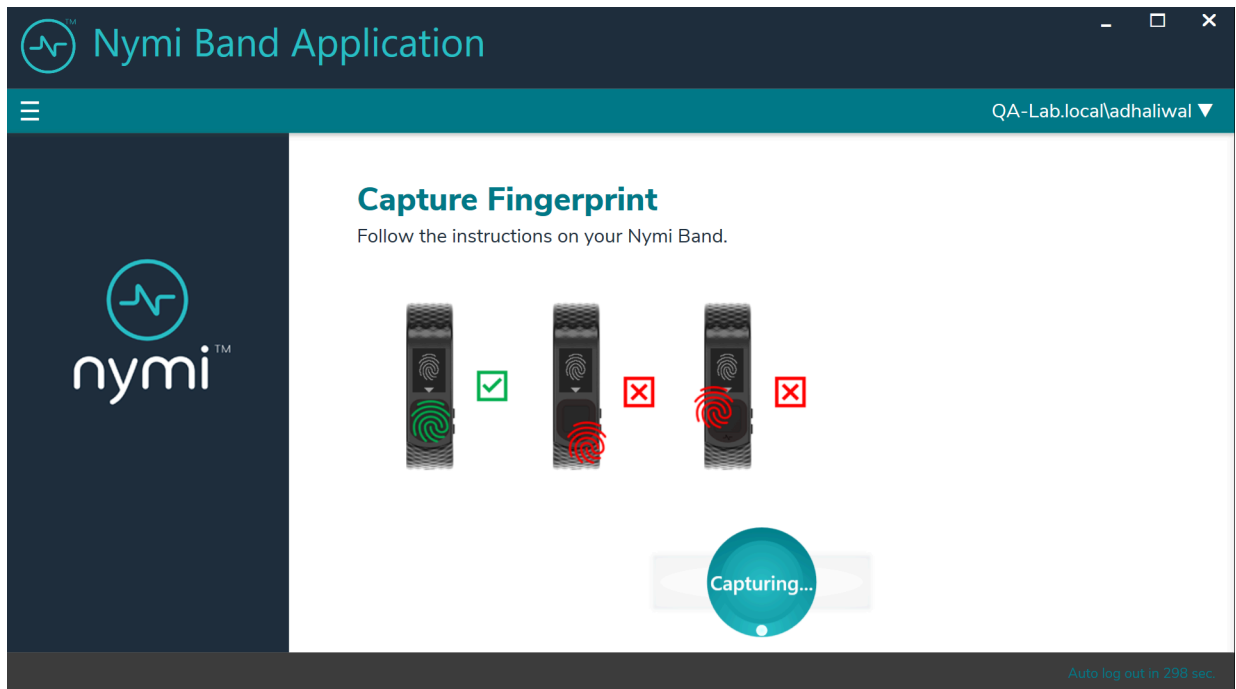
Figure 23: Capture Fingerprint In Progress

3. When the `Fingerprint` icon to appear on the Nymi Band screen, as shown in the following image, place their finger on the fingerprint sensor and the fingerprint bezel that surrounds the sensor.

Figure 24: FINGERPRINT

4. When the `LIFT FINGER` message appears on the screen, lift their finger from the sensor and bezel.

   When the `TOUCH SENSOR` message appears on the screen, place their finger on the sensor and bezel.

   The following figures show the `LIFT FINGER` and `TOUCH SENSOR` messages.

Figure 25: LIFT FINGER

Figure 26: TOUCH SENSOR

5. Repeat the steps to lift their finger and touch the sensor and bezel, as prompted.

The fingerprint process evaluates and captures 15 images of the fingerprint, and then performs one of the following actions:

- If the process determines that the images that were captured are acceptable to create a template, then the Nymi Band creates a securely-stored mathematical template of the image, and then deletes the images.
- If the process determines that the images that were captured are not acceptable to create a template, then the Nymi Band deletes all images and requires the user to repeat the fingerprint capture process.
- If the process is unable to create a template after three attempts, the process fails and the Nymi Band displays **See Admin**. In this situation, you must perform a delete user data operation on the Nymi Band, disassociate the Nymi Band from the user in the NES Administrator Console, and then repeat the enrollment process with a different Nymi Band or different finger.

  Note: *Nymi Band User Management* provides detailed information about how to delete the user data and disassociate the Nymi Band from the user.

Results

When the Nymi Band fingerprint capture process completes, the Nymi Band displays

.

The next steps in the enrollment process depends on the settings in the NES policy. If the Band Label feature is enabled, users are prompted to assign the Band Label to their Nymi Band, as described in the next section.

If the Band Label feature is disabled, the enrollment is completed after policy settings are applied. The Nymi Band vibrates twice quickly and a success message appears.

Note: The Nymi Band does not vibrate if the `Haptic Feedback on Nymi Bands` is not enabled for the user or active group policy.

7.4 - Assigning the Band Label

When an NES Administrator enables the Band Label feature in the active group policy, one of the following Band Label pages appear during the enrollment workflow:

- Preview Band Label- Provides the user with a preview of the Band Label that appears on their Nymi Band when enrollment completes. The user cannot modify the Band Label.

  Note: This page appears when the NES Administrator selects the `Display of Band Label on Nymi Bands` option in the NES active group policy.
- Customize Band Label- Provides the user with the ability to customize a Band Label that appears on their Nymi Band when enrollment completes.

  Note: This page appears when the NES Administrator selects the `Allow Band Label Customization` option in the NES active group policy.

For more information about the Band Label policy options see, *Customizing the Nymi Band Display*.

7.4.1 - Preview Band Label

The Preview Band Label page displays the first 12 characters of the username for a user on the Nymi Band screen, in two rows of six characters.

The following figure provides an example of the `Preview Band Label` page.
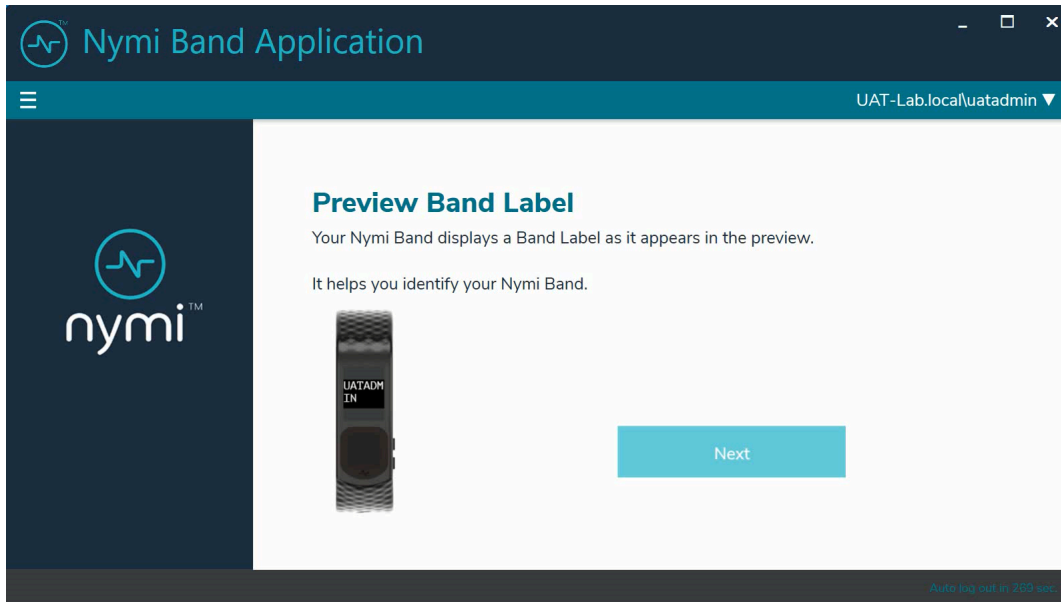
Figure 27: Preview Band Label

Instruct the user to click **Next** to continue the enrollment process.

7.4.2 - Customize Band Label

By default, the Band Label displays the corporate username for the user. When the customize option is enabled, the user can create a customized Band Label of up to 12 characters.

About this task
Instruct the user to perform the following steps to customize the Band Label.

Procedure

1. In the **Band Label** field, type the label to display on the Nymi Band.

   Supported Band Labels:

   - Contain a maximum 12 characters
   - Contain a combination of alphanumeric characters (all alpha characters display in uppercase on the Nymi Band)

• Contain a combinations of the following characters including spaces: A-Z, 0-9 and & ! " # $ % ' ( ) * + , . - \ / : ; < > = ? @ [ ] { } | ^ _ ` ~
• Do not contain leading or trailing spaces.

Note: When unsupported characters are included in the Band Label, they display as questions marks "?" on the Nymi Band screen when the enrollment process completes.

The following figure provides an example of the `Customize Band Label` page when unsupported characters are entered.
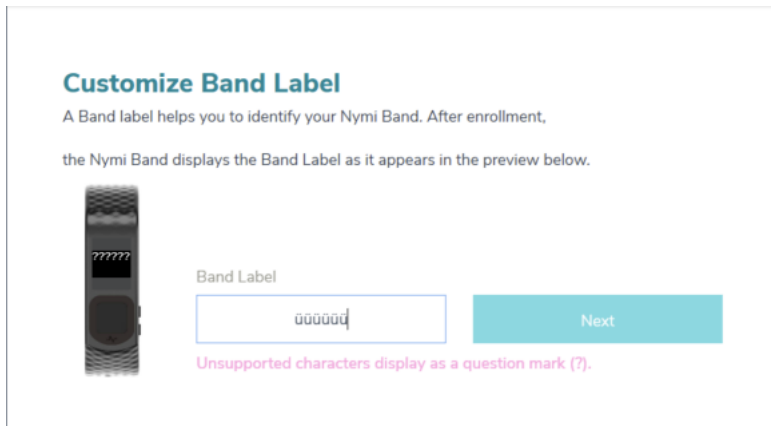
Figure 28: Custom Band Label Unsupported Characters

2. Review the Band Label in the Band Label preview.

3. Make any necessary modifications in the `Band Label` field.

4. Click `Next`, to save the Band Label and to proceed with the enrollment process.
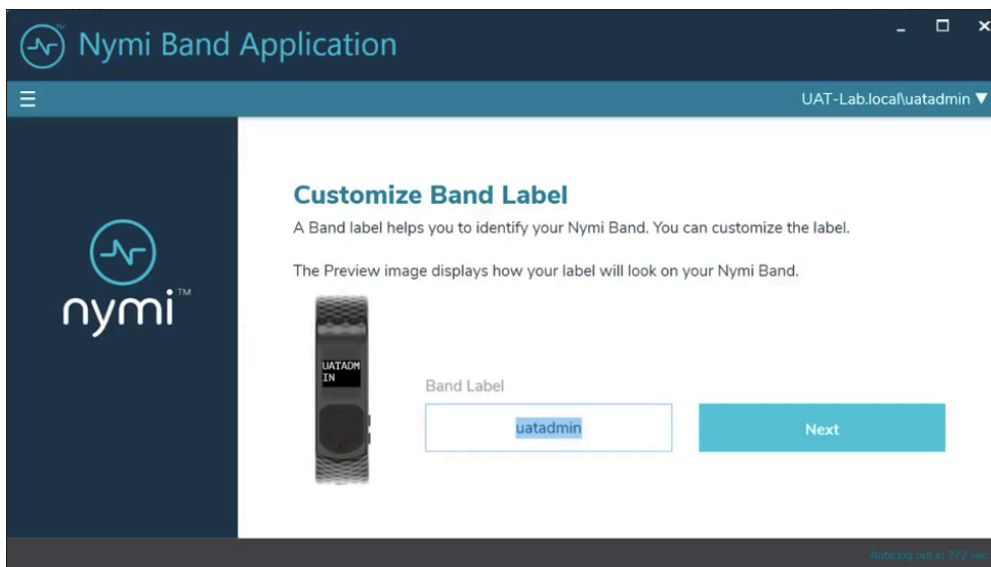
Figure 29: Custom Band Label Configuration

7.5 - Applying Policy Settings

To complete the enrollment process, the Nymi Band must apply policy settings based on the NES active policy. There is no action required from the user while configuration completes.
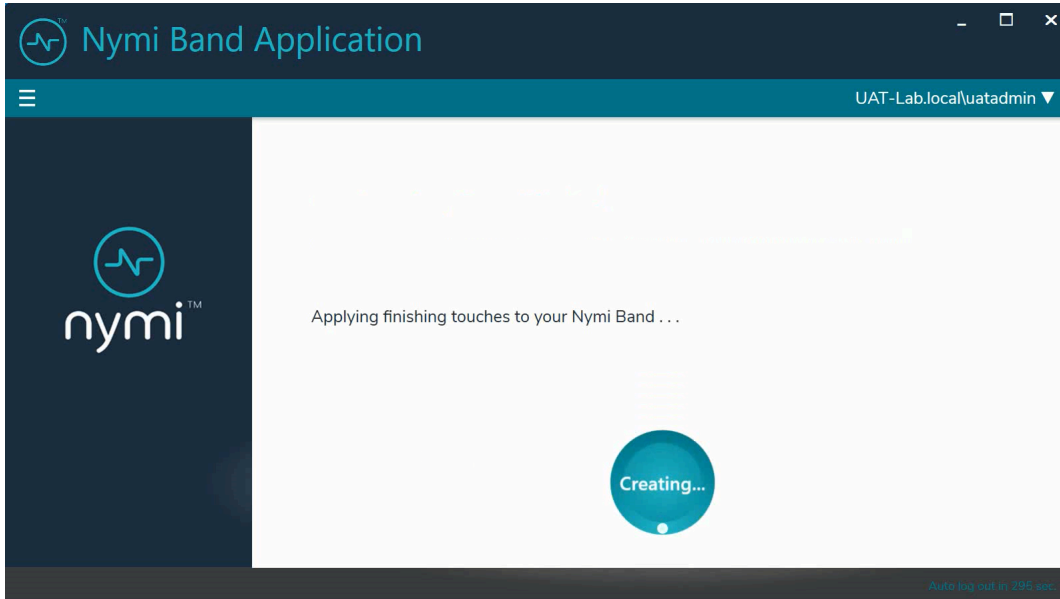
Figure 30: Applying Policy Settings

7.6 - Completing Enrollment

When the enrollment completes successfully, the `Success` page appears with a message that the enrollment succeeded and the Nymi Band is authenticated to the user.

The following figure provides an example of the `Success` page when enrollment completed successfully.
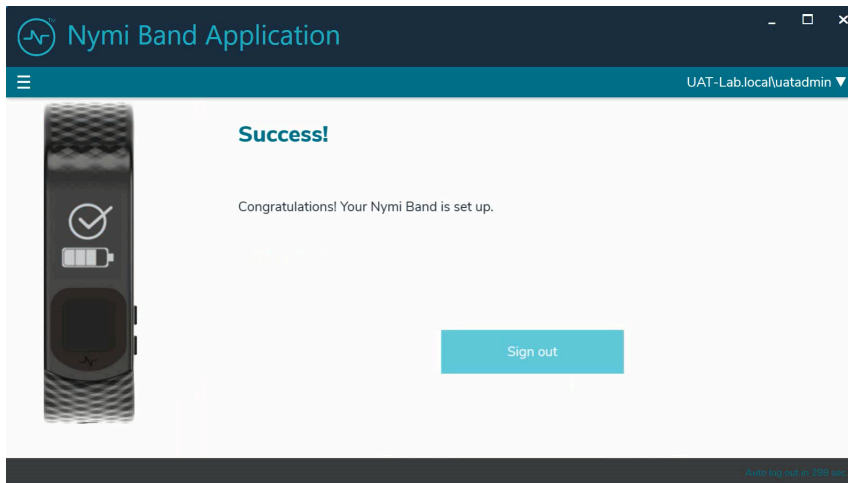
Figure 31: Success

Click `sign out`. The Nymi Band is authenticated and ready for use by the user.

The enrollment process sends information about the user and the Nymi Band, such as serial number to the NES. You can search for the information about the Nymi Band that is associated with the user. *Searching for User or Nymi Band Information* provides more information.

Note: After enrollment, Nymi recommends that each user authenticate to the Nymi Band 10 times with success. If the number of authentication attempts that are required to get 10 successful authentications exceeds 15, review the information in the Nymi Connected Worker Platform—Troubleshooting Guide for more information about how to troubleshoot Nymi Band authentication issues.

8 - (Nymi IT/OT Solution only) Nymi Band Registration

In an IT/OT configuration, users can enroll their Nymi Band in one identity domain and register their Nymi Band in another identity domain.

Before you begin
Set the active group policy setting **Enrollment / Registration** to **Registration only** or **Enrollment and Registration** on the Nymi Enterprise Server(NES) in the identity domain where users will register their Nymi Band.

About this task
When a user registers their enrolled Nymi Band in an identity domain, they can use their Nymi Band to complete authentication tasks.

Instruct the user to wear their authenticated Nymi Band and perform the following steps on the Registration Terminal.

Procedure

1. Start the Nymi Band Application by double-clicking the icon on the desktop.
2. On the `The Setting Up Your Nymi Band` screen, perform the following actions:
   a) Press the top button on the Nymi Band, wait for the Nymi Band to wake up, and then tap the Nymi Band against the Bluetooth adapter.
   b) Type your username and password, and then click **Continue**.
      Status messages appear, such as Updating user in NES and the registeration completes
3. Click **Sign out**.

Results
The user can use their Nymi Band in the identity domain to complete authentication tasks.

9 - Using the Nymi Band

The Nymi Band contains a number of screens, each providing specific images and feedback.

9.1 - Authentication After Enrollment

Each time that a user removes an authenticated Nymi Band from their wrist, the Nymi Band deauthenticates. For day-to-day usage of the Nymi Band, each time a user puts on the Nymi Band, the user must authenticate their identity to the Nymi Band.

Depending on the defined policy, users authenticate by using one of the following methods, while the Nymi Band is on their wrist:

- By biometrics (fingerprint and optionally liveness detection)—With the Nymi Band on their wrist, the user holds their finger on the fingerprint sensor. The Nymi Band verifies that the fingerprint matches the fingerprint template that is securely stored on the Nymi Band and by default detects liveness.
- By corporate credentials (if a credential authenticator was created)—The user logs into the Nymi Band Application by using their corporate credentials as authentication and, when validation succeeds, the Nymi Band Application puts the Nymi Band into an authenticated state.

9.1.1 - Authentication by Fingerprint

When the screen displays the fingerprint icon, the user holds their finger on the square fingerprint sensor and surrounding bezel. The Nymi Band displays the fingerprint authentication screen while fingerprint match and optional ECG liveness detection are in progress during authentication. The ECG liveness detection is automatically enabled for the default group policy. Refer to section *Configuring Liveness Detection* in the section *Customizing the Nymi Band Authentication Method* for information about how to disable ECG liveness detection.

Figure 32: Fingerprint Authentication screen

When the Nymi Band displays one of the following icons, the user identity was successfully authenticated, and the user can remove their finger from the fingerprint sensor and fingerprint bezel.

Figure 33: Authentication Success Screen with Band Label

Figure 34: Authentication Success Screen without Band Label

9.1.2 - Authentication by Corporate Credentials

When the screen displays the fingerprint icon, the user logs into the Nymi Band Application, and clicks the `Authenticate` button, as shown in the following figure.
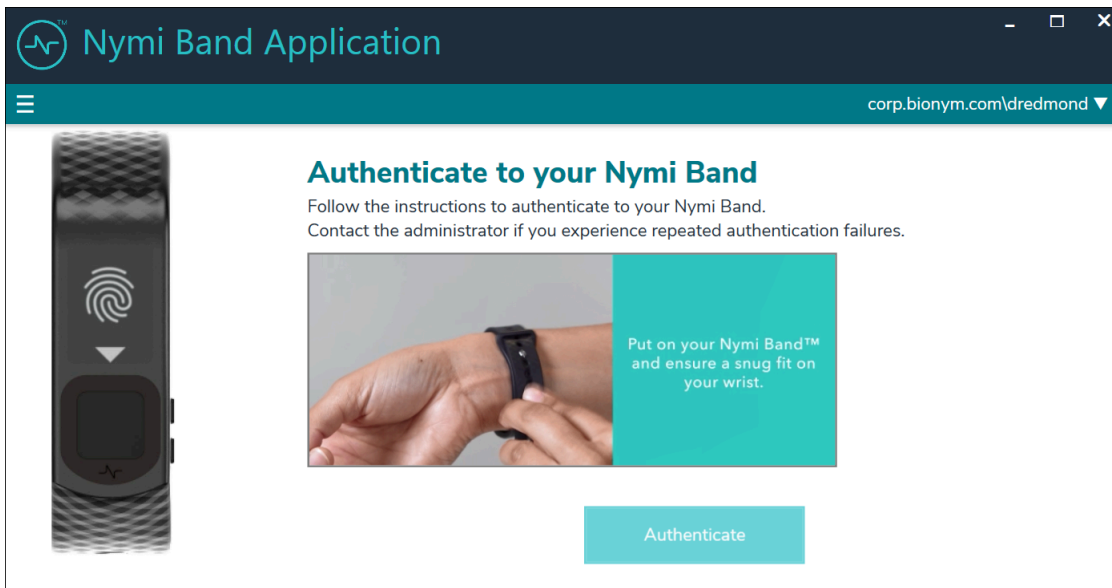
Figure 35: Authentication by Corporate Credentials

When the Nymi Band displays the success icon (checkmark), the user identity was successfully authenticated, and the user can log out of the Nymi Band Application.

9.1.3 - Authentication Failures

When authentication of the Nymi Band fails, the Nymi Band vibrates and displays a message.

Note: The Nymi Band does not vibrate if the `Haptic Feedback on Nymi Bands` is not enabled for the user or active group policy.

Nymi Band authentication failures occur for one of the following reasons:

- Fingerprint matching failure—when the authentication fails as a result of a fingerprint mismatch, the Nymi Band vibrates and displays a **No Match** message about 1 second

after the user places their finger on the fingerprint sensor and bezel. When the Nymi Band screen displays the fingerprint icon, the user can retry authentication. The message that appears on the Nymi Band screen when there are subsequent authentication failures due to fingerprint depends on the number of consecutive failures:

* When there are less than 4 consecutive fingerprint match failures, the **No Match** message appears.
* When there are more than 3 consecutive fingerprint match failures, the Nymi Band displays a message that provides advice that can result in a successful authentication. Possible messages include **Center Finger**, **Wash and Dry Hand and Wrist**, and **Clean Band**.

* Liveness failure—when the authentication fails due to the inability to detect a consistent ECG signal on the wrist, the Nymi Band vibrates and displays the **No ECG** message about 13 seconds after the user places their finger on the fingerprint sensor and bezel. When the Nymi Band screen displays the fingerprint icon, the user can retry authentication. The message that appears on the Nymi Band screen when there are subsequent authentication failures due to liveness detection issues depends on the number of consecutive failures:

* When there are less than 4 consecutive fingerprint match failures, the **No ECG** message appears.
* When there are more than 3 consecutive fingerprint match failures, the Nymi Band displays a message that provides advice that can result in a successful authentication. Possible messages include **Sit Still**, **Wash and Dry Hand and Wrist**, and **Don't Move**.

Troubleshooting Fingerprint Mismatch Failures

If the fingerprint authentication fails, ensure the following:

* Fingerprint sensor is clean and dry.

  * If the fingerprint sensor is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
  * If the fingerprint sensor is wet, dry completely with a lint-free towel, and then retry authentication.
* User does not press too hard or too softly on the fingerprint sensor.
* User's finger is clean and dry.

  * If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication.
  * If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
  * If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication
* User places their finger on the centre of the sensor, touching the surrounding bezel.
* User keeps their finger still on the sensor and bezel during the authentication period.
* User does not lift their finger off the sensor or bezel until the authentication process completes.
* User wears the Nymi Band snugly on the wrist.

- User wears their own Nymi Band.
- User attempts authentication with the same the finger that they used during enrollment.
- User finger is not damaged, for example the user has cut their finger.

  Note: If the finger that is used for authentication is damaged, consider one of the following actions:

  - Instruct the user to authenticate by corporate credentials until the finger heals.
  - Delete the user data on the Nymi Band, disassociate the user from the Nymi Band in NES and Evidian, and then perform enrollment with a different finger.

Troubleshooting Liveness Detection Failures

If the liveness detection fails, ensure the following:

- Bottom sensor is clean and dry.

  - If the bottom electrode is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
  - If the bottom electrode is wet, dry completely with a lint-free towel, and then retry authentication.
- User's finger is clean and dry.

  - If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication
  - If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
  - If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication
- User keeps their finger still on the sensor and bezel during the authentication period.
- User's wrist is not too dry. Before authentication, wash and completely dry the wrist before putting on the Nymi Band, or rub some lotion well into the wrist, and then retry authentication.
- Nymi Band bottom electrode remains in contact with the wrist during the authentication period. If the position of bottom electrode prevents contact, remove the Nymi Band, reposition the Nymi Band on the wrist, and then try authentication again.
- User does not lift their finger off the sensor or bezel until the authentication process completes.
- Nymi Band fits snugly on the wrist and does not move around during the authentication process.
- User's wrist is not tattooed where the bottom sensor makes contact.

  Note: If the user cannot use another wrist or the Nymi Band cannot make contact with an area that is not tattooed, instruct the user to authenticate by corporate credentials.

Troubleshooting Persistent Authentication Failures

Lockout policies help prevent adversarial users from gaining unauthorized access to systems through brute-force attacks.

When an authentication lockout occurs, the Nymi Band displays the **See Admin** icon and prevent the user from performing additional authentication attempts. An authentication lockout occurs in the following scenarios:

* After 50 consecutive failed authentication attempts on a previously enrolled Nymi Band due to a fingerprint mismatch.
* After 3 consecutive failed attempts to complete the fingerprint template during the enrollment due to an issue with the fingerprint imaging.

The lockout persists on the Nymi Band, even if the user removes the Nymi Band. The lockout will also persist while the Nymi Band is dead or while charging.

Clear the lockout by one of the following methods:

* Re-enroll the user to the Nymi Band.
* Authenticate the user with their credentials in the Nymi Band Application. A user can authenticate by using corporate credentials only if the `Corporate Credentials Authentication` option was enabled in the NES policy at the time of enrollment.

If the user persistently cannot authenticate to the Nymi Band, consider the following actions:

* Restart the Nymi Band and retry authentication.
* Instruct the user to log into the Nymi Band Application while wearing the Nymi Band and authenticate by corporate credentials.
* Delete the user data from the Nymi Band and then disassociate the Nymi Band from the user in NES and Evidian (if used), and then enroll with a different finger.
* Delete the user data from the Nymi Band, disassociate the Nymi Band from the user in NES and Evidian, and then enroll the user with a different Nymi Band.

For reference, use the following troubleshooting workflows.

Ensure:

-Fingerprint sensor is clean and dry.
-Finger is clean and dry.
-User does not press too hard or too softly on the fingerprint sensor.
-User places their finger on the centre of the sensor, touching the surrounding bezel.
-User keeps their finger still on the sensor and bezel during the authentication period.
-User does not lift their finger off the sensor or bezel until the authentication process completes.
-User wears the Nymi Band snugly on the wrist.
-User wears their own Nymi Band.
-User attempts authentication with the same the finger that they used during enrollment.

Fingerprint sensor not working

Finger damaged? — Yes → User uses corporate credentials

No

User retries authentication

Authentication succeeds? — Yes → User uses Nymi Band

No → Restart Nymi Band

User retries authentication

Authentication succeeds? — Yes → User uses Nymi Band

No

User deletes user data and admin dissociates Nymi Band from user in NES/Evidian → User re-enrolls Nymi Band and tries authentication

Authentication succeeds? — Yes → User uses Nymi Band

No

User deletes user data and admin dissociates Nymi Band from user in NES/Evidian → User enrolls new Nymi Band & retries authentication

Authentication succeeds? — Yes → User uses Nymi Band

No

User uses corporate credentials

9.2 - Viewing Nymi Band Text

While interacting with the Nymi Band, text can be presented on the Nymi Band screen to relay information to the user.

The below image shows the font used on the Nymi Band.

Figure 36: Nymi Band Font

9.3 - Viewing Nymi Band Screens

The Nymi Band contains a number of screens that contain images and feedback. The following table identifies screens that are typically seen by Nymi Band users.

Table 4: Nymi Band Screen

Nymi Band Screen	Nymi Band Screen Name	Description
	Blank Screen	Indicates that you need to charge the battery or that the Nymi Band is in sleep mode. Press any button to wake up the Nymi Band.
	No User	Indicates that the Nymi Band is off-body and not assigned to a user and displays the battery charging level.
	Setup code	Displays a message with letters and numbers when you wear an unenrolled Nymi Band. This is the setup code of the Nymi Band, which is used by the Nymi Band Application during the enrollment process.
	Add User	Appears after you type the setup code in the Nymi Band Application. When you see this message, follow the instructions in the Nymi Band Application to complete the enrollment process.

Nymi Band Screen	Nymi Band Screen Name	Description
	Authentication Required	Indicates that you need to authenticate your identity. Hold your fingerprint on the fingerprint sensor to initiate the authentication process.
	Authentication In Progress	Indicates that the authentication process is in progress. Hold your finger on the fingerprint sensor until the screen shows the success indicator. The screen without the progress bar indicates the authentication process with **Liveness Detection** disabled.
	Success	Indicates a success based on user enrollment or user authentication. The top image is when Band Label is enabled and the bottom image is when the Band Label is disabled.
	Authenticated	Indicates that the Nymi Band is on-body and authenticated. The top image is when the Band Label is enabled and the bottom image is when the Band Label is disabled. The Nymi Band is ready to use.
	No Match	Indicates that authentication failed as a result of a fingerprint mismatch.
	Center Finger	Appears when there has been more than 3 consecutive authentication failures as a result of a fingerprint mismatch.
	Center Finger	Appears when there has been more than 3 consecutive authentication failures as a result of a fingerprint mismatch or liveness detection issue.

Nymi Band Screen	Nymi Band Screen Name	Description
CLEAN BAND	Clean Band	Appears when there has been more than 3 consecutive authentication failures as a result of a fingerprint mismatch.
SIT STILL	Sit Still	Appears when there has been more than 3 consecutive authentication failures as a result of a liveness detection issue.
DON'T MOVE ARMS	Don't Move	Appears when there has been more than 3 consecutive authentication failures as a result of a liveness detection issue.
SEE ADMIN	Authentication Lockout	Indicates that the user is locked out of the Nymi Band. The lockout prevents the user from authenticating with their fingerprint.
JSMITH DAYL08	Deauthenticated	Indicates that the Nymi Band is deauthenticated. The top image is when Band Label is enabled, and the bottom image is when the Band Label is disabled or when authentication fails.
JSMITH DAYL08	Unauthenticated Band	Indicates that the Nymi Band is off-body. The top image is when Band Label is enabled and the bottom image is when the Band Label is disabled.
DELETE USER DATA	Delete User Data	Indicates that the process of deleting user data is running. Deleting user data on a Nymi Band removes all the data for the currently enrolled user from the Nymi Band.
USER DATA DELETED	User Data Deleted	Indicates that the user data on a Nymi Band has been removed.

9.4 - Viewing the Band Label

When you configure the policy to assign a Band Label during enrollment, the label appears on a Nymi Band that is:

- On-body and authenticated (on your body and fingerprint accepted)
- Off body and deauthenticated (not on your body and the band did not accept the fingerprint)
- Off body and on the charger

On-Body and authenticated

While on-body and authenticated, when a user presses the top button twice on the Nymi Band, the screen scrolls to the `Band Label` screen. The screen displays for two seconds and then dims for 15 seconds before it turns off.

The following image provides an example of the `Band Label` screen.

Figure 37: Band Label on an enrolled and authenticated Nymi Band

Note: After the Band Label is set during the enrollment workflow, the user cannot modify the Band Label without performing the `Delete User Data` process. For more information see, *Deleting User Data* .

Deauthenticated

While an enrolled Nymi Band is off body (not being worn and therefore not authenticated), the Nymi Band screen displays the Band Label above the battery status icon.

The following image provides an example of the Band Label on an unauthenticated Nymi Band

Figure 38: Band Label on an unauthenticated Nymi Band

Enrolled and Charging, or on the Charger

When an enrolled Nymi Band is charging, the Nymi Band screen displays the Band Label above the charging icon.

The following figure provides an example of the Band Label while the Nymi Band is charging.

Figure 39: Band Label on a charging Nymi Band

9.5 - Nymi Band Dashboard

The Nymi Band Dashboard is a on band carousel that enables users to navigate through screens that provide you with information. The dashboard is only available on an authenticated Nymi Band if a Band Label has been assigned to the Nymi Band. By pressing the top and bottom buttons of the Nymi Band, users can navigate through screens that provide information, such as the Band label and SEOS status.

When you wake up an authenticated Nymi Band, the main dashboard screen appears.

When the Nymi Band has a band label, an arrow at the top of the dashboard screen appears and you can press the top button to display the band label. At the bottom of the band label screen, an arrow appears and you can press the bottom button to return to the dashboard screen.

The following figure provides an overview of the Nymi Band Dashboard carousel.
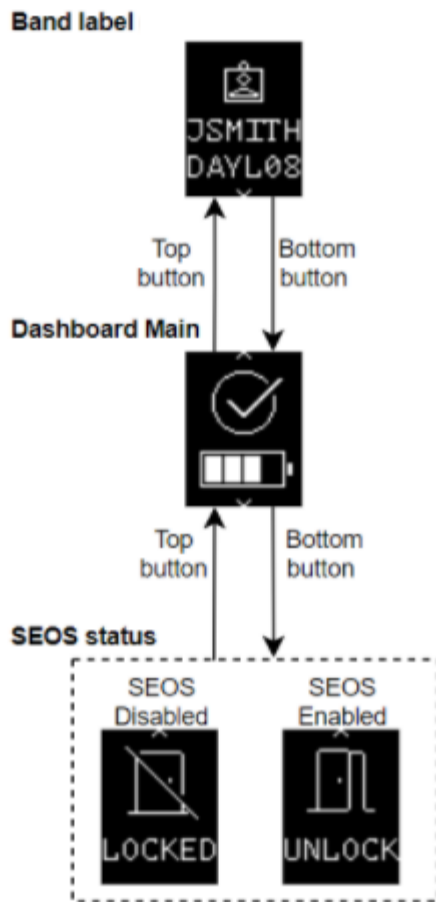
Figure 40: Nymi Band Dashboard carousel

9.6 - Nymi Band Vibration

By default the Nymi Band provides haptic feedback, specifically a vibration, that is triggered by specific events.

Note: You can disable haptic feedback on the Nymi Band for certain users or all users. *Customizing the CWP Configuration* provides more information.

Vibration Event	Details	When is it occurs
Acknowledgement	One short vibration. Used when the Nymi Band acknowledges that the user input has been received or to prompt the user to pay attention to the Nymi Band	• Nymi Band detects user's finger at the beginning of an authentication • Nymi Band starts charging

Vibration Event	Details	When is it occurs
Success	Two short vibrations in quick succession. Used when the Nymi Band confirms an operation is successfully completed	• Nymi Band's authentication success • Fingerprint enrollment success • Start of restart or security wipe sequence
Warning	Long vibration. Used when the Nymi Band confirms that an operation is successfully completed	• Failed authentication • Nymi Band transition from authenticated state to deauthenticated state
Reset	Three short vibrations in quick succession. Used when the Nymi Band encounters an internal issue and restarts in an attempt to correct the problem.	Nymi Band encounters an internal issue. The Nymi Band performs up to three consecutive reset attempts. • If the recovery succeeds in one of the attempt, instruct the user to authenticate to their Nymi Band • If the recovery fails, the Nymi Band displays a fault code. Contact Nymi Support to start the RMA process.

9.7 - Tapping the Nymi Band

Many uses for the Nymi Band involve tapping it to a compatible BLE adapter or NFC reader to perform a task.

Note: The section *Editing the nbe.toml File* in the *Nymi Connected Worker Platform— Deployment Guide* provides information about how to configure BLE tap.

Tips for tapping your Nymi Band

• For tapping to work, users must first authenticate their identity to the Nymi Band. If the screen on the Nymi Band is blank, press any button on the Nymi Band to wake it from sleep. If the screen remains blank, users need to charge the Nymi Band. If the screen displays the fingerprint image, users need to authenticate their identity.
• Users do not need to touch the face of the Nymi Band directly to the reader. Keep it just above the surface of the NFC reader (approximately 1 cm) or BLE adapter (within 10 cm).
• If tapping fails, move the Nymi Band away from the reader (30 cm or more) and then try again.

- Users may need to adjust the tapping speed. It should take approximately 1 second to move the Nymi Band towards and away from the reader.

9.8 - SEOS Access

By default, an authenticated Nymi Band provides users with the ability to gain access to SEOS-enabled doors.

When the user removes their authenticated SEOS-enabled Nymi Band, the Nymi Band deauthenticates and SEOS is disabled.

10 - Using the Nymi Application

The Nymi Application allows you to perform authentication tasks, such as e-signatures by tapping the Nymi Band on the iPad.

When a user launches a web-based Nymi-enabled Application (NEA) and performs an authentication task, the Nymi Application appears on the screen and prompts the user to tap their Nymi Band to complete the operation. The following figure show the Nymi Application window.
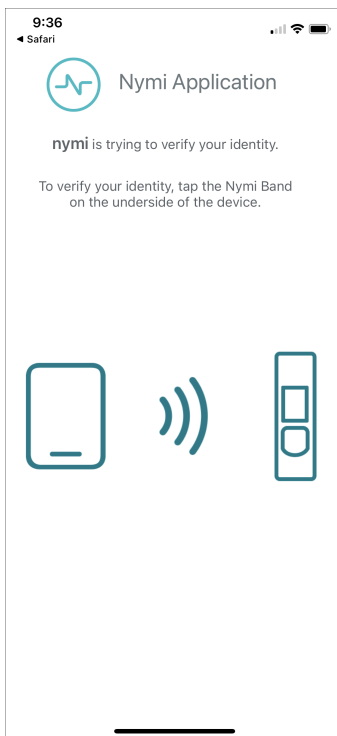
Figure 41: Nymi Application

Note: The Nymi Application might reference a different company name instead of *nymi*.

If the Nymi Application detects that a configuration issue, a status panel appears in the lower left corner of the screen and displays the problem to the user. The following figure provides an example of the status panel when the Nymi Application cannot access Bluetooth adapter
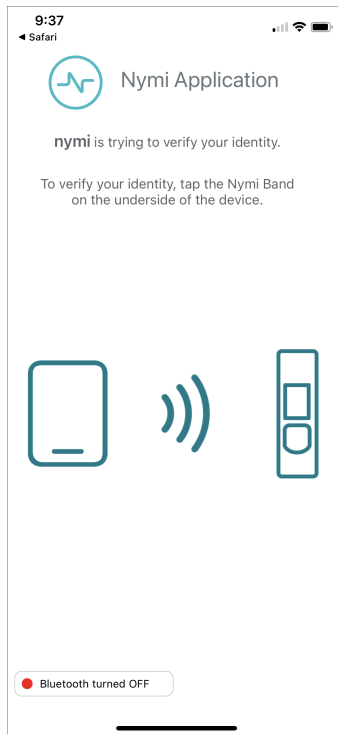
Figure 42: Nymi Application - Cannot Access Bluetooth Adapter

The Nymi Application waits about 10 seconds for the user to tap their Nymi Band. If user does not tap the Nymi Band and the request times out, the Nymi Application prompts the user to retry or cancel, as shown in the following figure.
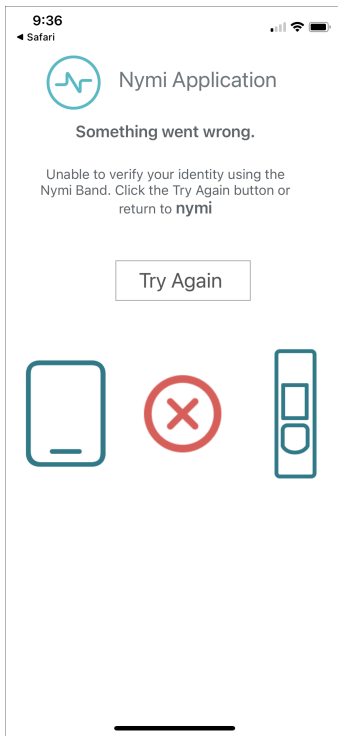
Figure 43: Nymi Application Timeout

When the tap operation completes successfully, the Nymi Application prompts the user to tap the application link on the navigation bar to return to the web-based NEA.
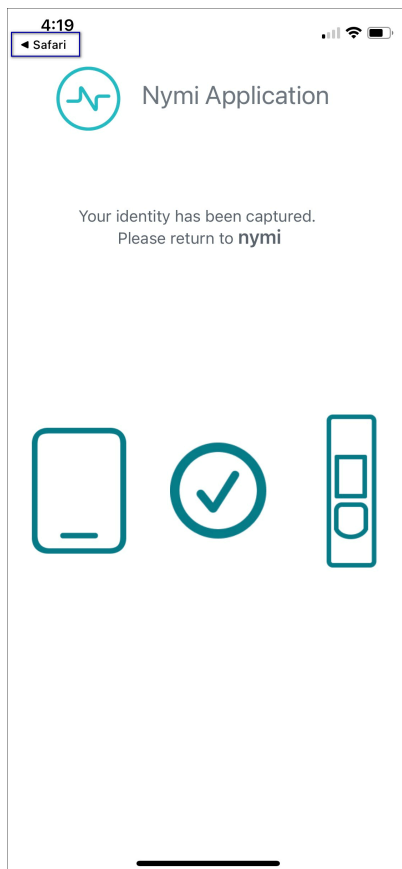
Figure 44: Nymi Application Success

10.1 - Overriding the Nymi Band Tap Configuration

The MDM device profile defines the positioning of the Nymi Band near the Bluetooth adapter that the Nymi Application requires to complete an authentication task.

About this task

If your configuration allows users to override the settings directly on the iOS device, perform the following steps.

Procedure

1. On the iOS device, navigate to `Settings > Nymi`

2. In the `Profile Settings` section, touch `Nymi Band Tap`, as shown in the following figure.

1:10

⟨ Settings   **Nymi**

ALLOW NYMI TO ACCESS

* Bluetooth	⬤
Local Network	⬤
Siri & Search	›
⚙ Background App Refresh	⬤

NYMI SETTINGS

| Version | 0.2.24 |
| Logs | ⬤ |

PROFILE SETTINGS

| Nymi Band Tap   Profile 1 (Far) › |

Adjust how much distance the Nymi
Band has to come to the device for a
tap.

---
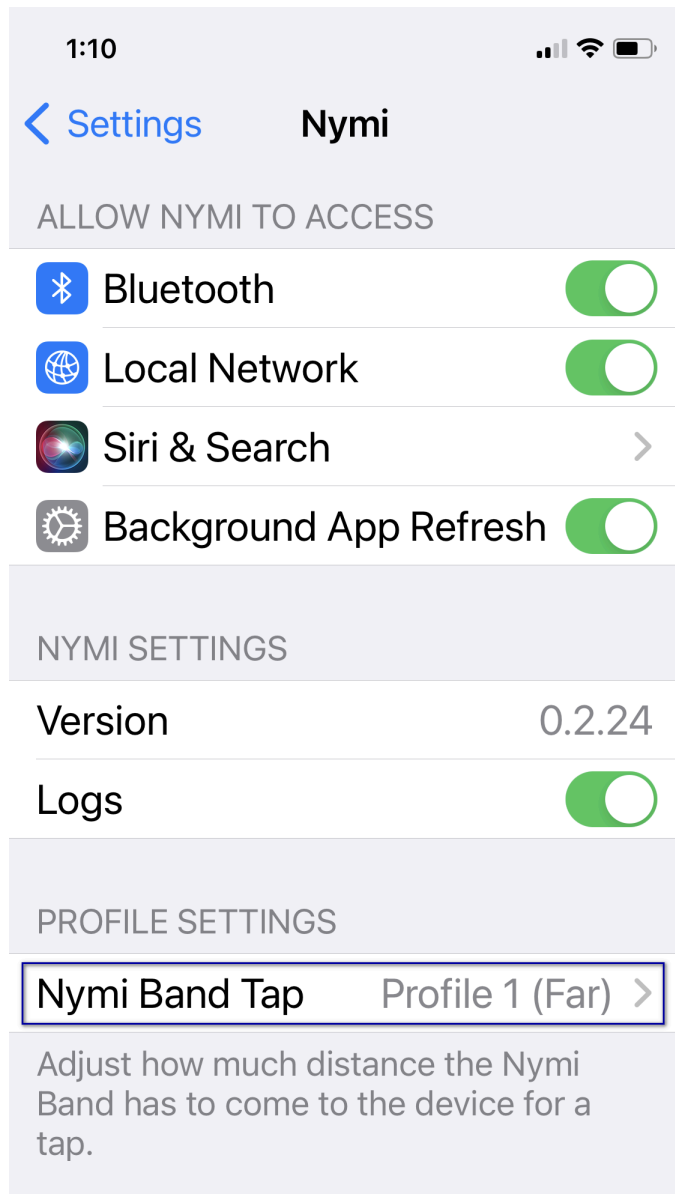
3. On the `Nymi Band Tap` screen, adjust the profile setting.

   Note: You can use the Nymi Calibration tool to determine the optimal profile setting. The *Nymi Connected Worker Platform—Deployment Guide* provides more information.

   - To increase the detection sensitivity of the Nymi Band, select a smaller profile value. Lower values reduce the distance between the Nymi Band and Bluetooth adapter that the Nymi Application requires to complete an authentication task.
   - To decrease the detection sensitivity of the Nymi Band, select a higher profile value. Higher values increase the distance between the Nymi Band and Bluetooth adapter that the Nymi Application requires to complete an authentication task.

4. Retest the Nymi Band tap.

11 - Using Nymi Lock Control

A user can unlock a Nymi Lock Control user terminal by tapping their authenticated Nymi Band against an attached NFC reader, BLE adapter (BLED112), or by using the Nymi Credential Provider to log in without typing a password.

A terminal on which Nymi Lock Control is installed has a modified Windows login screen that displays Nymi Credential Provider below the username. The Nymi Credential Provider is the application that validates user credentials for Nymi Lock Control.

The following image provides an example of the login screen when Nymi Lock Control is installed on the terminal.
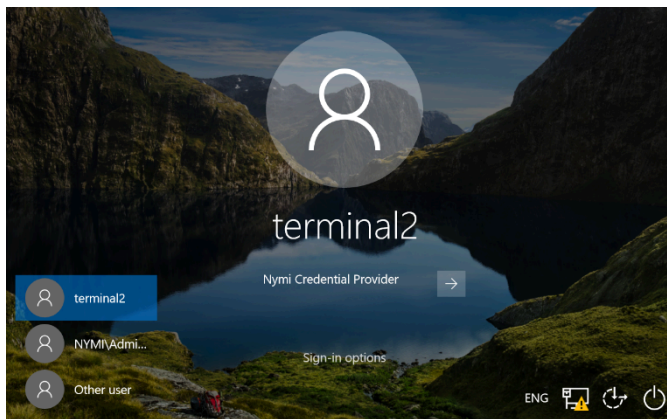
Figure 45: User Terminal Log in Screen with Nymi Lock Control

11.1 - Configuring Nymi Lock Control

Perform the following steps to enable and configure Nymi Lock Control.

About this task
By default Nymi Lock Control is not enabled.

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 options appear to customize Nymi Lock Control.

Option	Description
Lock When Away	• Configure Nymi Lock Control with the ability to lock the user terminal when Nymi Lock Control does not detect the authenticated Nymi Band. • Default: Enabled • When enabled, Nymi Lock Control locks the user terminal when a user removes an authenticated Nymi Band or when the Nymi Band is not in close proximity of the user terminal. When the Nymi Band is out of range, a 10 second timer appears on the desktop. If the Nymi Band does not return within close range of the user terminal, the terminal will lock. Ensure that your Group Policy Object(GPO) settings do not push the *Do not display the lock screen* configuration option to the Nymi Lock Control user terminals. **Note:** Edit the *nbe.toml* file to define close proximity for Nymi Lock Control. Refer to *Editing the nbe.toml File*.
Unlock When Present	• Configures Nymi Lock Control to check if the Nymi Band is in close proximity before unlocking the user terminal. If not, then unlock fails. You can define how close the Nymi Band must be to the user terminal to allow the user to unlock the terminal with the Nymi Band in the *nbe.toml* file. • Default: Enabled • When enabled, prevents an unauthorized user from unlocking the user terminal while the Nymi Band user is in Bluetooth range, but not in close proximity to the terminal. • When disabled, allows a user to unlock the user terminal by pressing the **Enter** key or space bar on the keyboard when the authenticated Nymi Band is within Bluetooth range, but not in close proximity of the user terminal.
Keep Unlocked when Present	• Provides you with the ability to define how the Nymi Band interacts with operating system screen timeouts or sleep settings that lock the user terminal.

Option	Description
	• Default: Enabled • When enabled, overrides any system screen timeouts or sleep settings, and keeps the user terminal unlocked as long as the Nymi Band is present and authenticated. • When disabled, prevents Nymi Lock Control from overriding any system screen timeouts or sleep settings.

5. Click **Save**.

Results

During enrollment the Nymi Band Application updates the Nymi Band to enable Nymi Lock Control support.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

When the Nymi Band Application updates on the Nymi Band completes, restart Nymi Lock Control.

11.2 - Initializing Nymi Lock Control

Perform the following while wearing an authenticated Nymi Band.

About this task

Procedure

1. Lock the desktop.

2. Press any key to display the Windows Login screen.

3. Click **Other User**.

4. Click **Sign-in options**.

5. Click the **Nymi Credential Provider** button, as shown in the following figure.
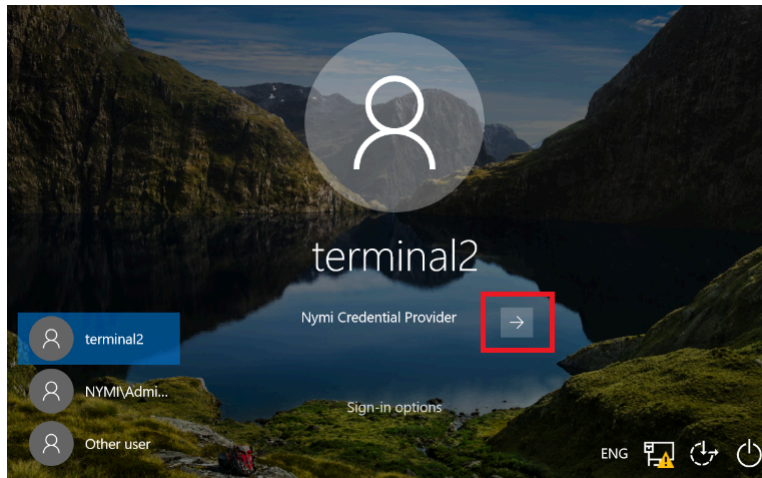
Figure 46: Nymi Credential Provider button

6. Tap the Nymi Band against the NFC reader or Bluetooth Adapter to unlock the desktop.

11.3 - Confirming Nymi Lock Control Recognizes the Nymi Band

After a user enrolls their Nymi Band, perform the following steps on a user terminal to confirm that Nymi Lock Control recognizes the Nymi Band user.

About this task

To confirm that Nymi Lock Control recognizes the Nymi Band, the Nymi Band user should perform the following steps:

Procedure

1. Log into the user terminal with your username and password.

Note: Nymi Lock Control will NOT detect changes to a user's corporate credentials in the Nymi Band. If a user changes their corporate credentials or the password has expired while Nymi Lock Control is enabled, Nymi Lock Control will not unlock the terminal. To update the Nymi Band with the encrypted password, the user must first sign into the Nymi Band Application and re-authenticate their Nymi Band. Refer to Resetting an Expired Password for information on resetting an expired password.

2. From the system tray, hover over the Nymi Lock Control icon.
When Nymi Lock Control detects the Nymi Band, the icon displays a green checkmark.

Hover text also appears to indicate that the Nymi Band is present.

11.4 - Unlocking or Logging On With an NFC or BLE Tap

Perform the following actions to unlock a user terminal by tapping the Nymi Band against an attached bluetooth adapter or an attached NFC reader.

Procedure

1. Press any key to display the Windows Login screen.
2. Tap the authenticated Nymi Band against the bluetooth adapter or NFC reader. Desktop unlocks.

11.5 - Unlocking with Nymi Credential Provider

When Nymi Lock Control is installed on a terminal, the log in screen displays Nymi Credential Provider below the username of an enrolled user.

About this task

A user with an authenticated Nymi Band can use the Nymi Credential Provider to unlock a user terminal that does not have an attached NFC reader.

Procedure

1. Press any key to display the Windows Login screen.
2. Select the username on the Login screen. If the username does not appear, perform the following actions:
   a) Click `Other User`.
   b) Click `Sign-in options`, and then select the Nymi icon.
   c) Type the username.
3. Click the `Submit` button.
   The following figure provides an example of the Login screen with the `Submit` button.
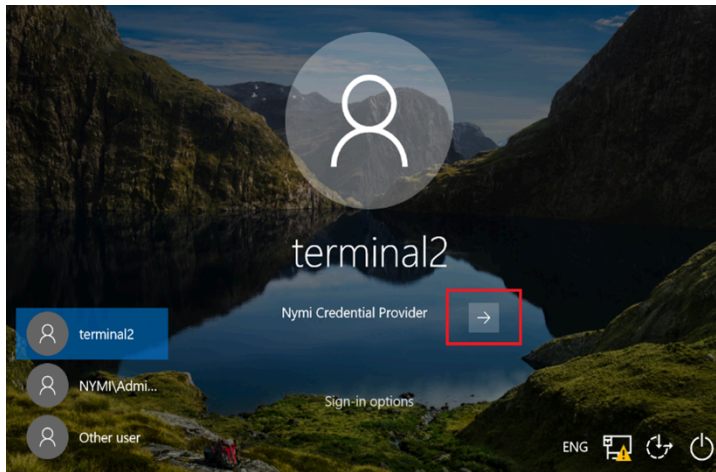
Figure 47: Nymi Credential Provider Submit button

The Nymi Credential Provider validates the authorization of the user. If the user has permission to access the user terminal, the user terminal unlocks.

11.6 - Unlocking a Nymi Lock Control User Terminal Without a Nymi Band

Nymi Credential Provider provides sign in options that allow users to log into the user terminal without an authenticated Nymi Band.

About this task

A user that does not have an enrolled Nymi Band can unlock a terminal that has Nymi Lock Control installed by clicking `Sign-in` options, and then selecting password credentials or smart card.

Procedure

1. Press any key to display the Windows login screen.
2. Click `Sign-on Options`, and then select the `Password` icon, as shown in the following figure.
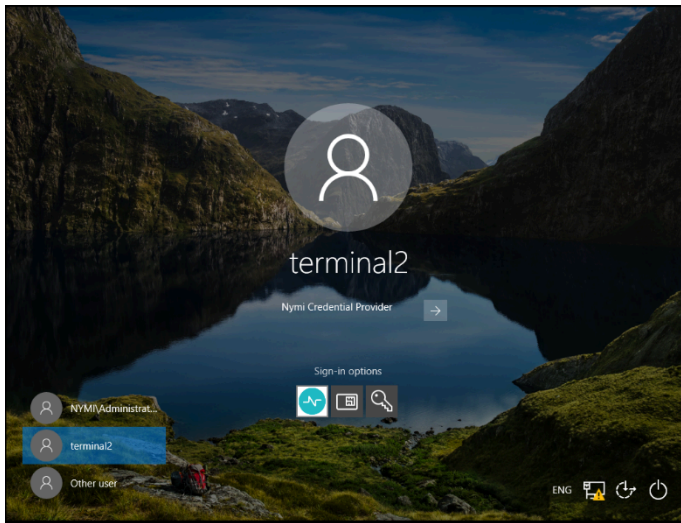
Figure 48: Sign-on Options screen

11.7 - Locking the User Terminal

The user can manually lock the terminal or the terminal automatically locks in the following situations:

- When the user removes the Nymi Band from their wrist.
- When the Nymi Band is out of Bluetooth range of the user terminal for more than 30 seconds.

11.8 - Stopping Nymi Lock Control

By default, Nymi Lock Control starts when the user terminal starts.

About this task
Perform the following steps to stop the Nymi Lock Control application on the user terminal.

Procedure

1. Log into the user terminal.
2. On the System Tray, right-click the Nymi Lock Control icon, and select `Quit`.

12 - Nymi Band Management

This chapter provides information about to how manage and maintain the Nymi Band.

12.1 - Removing the Nymi Band

When their shift ends, the user should remove and safely store their Nymi Band.

Nymi recommends that the user charges their Nymi Band at the end of each shift. When the user removes the Nymi Band, it vibrates once to indicate that deauthentication has occurred.

Note: The Nymi Band does not vibrate if the `Haptic Feedback on Nymi Bands` is not enabled for the user or active group policy.

Figure 49: Deauthentication with Band Label enabled

Figure 50: Deauthentication with Band Label disabled

When the user places the Nymi Band on their wrist again, the screen displays the fingerprint icon. The user cannot perform any tasks with the Nymi Band until they authenticate their identity. See the section *Authenticating User Identity to the Nymi Band* for information about how the user can re-authenticate to the Nymi Band.

12.2 - Storing the Nymi Band

This section provides recommendations for storing the Nymi Band when it is not in use.

- Store the Nymi Band in a dry and temperature controlled environment inside the range of 0°C to 45°C.
- Remove the Nymi Band from storage every 10 months and perform a full charge, to ensure that the battery does not discharge to very low levels and improve overall battery life.
- Apply a label near or on the Nymi Band charger to allow users to quickly identify their Nymi Band when charging in mass charging configurations. The *Nymi Band Charging Recommendations Guide* provides information and references designs for charging station configurations.

12.3 - Charging the Nymi Band

The Nymi Band is charged by placing it on a Nymi Band charger. The Nymi Band charger receives power from standard USB ports. It takes up to two hours to charge a fully depleted Nymi Band. A fully-charged Nymi Band typically has a 3-day battery life based on 300 BLE or NFC taps over 10 hours per day. Charging must occur in a temperature controlled environment inside the range of 15 to 30°C (59 to 86°F). This will ensure the Nymi Band charges in a timely manner and will maintain the longevity of the battery.
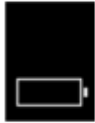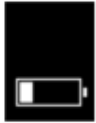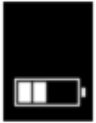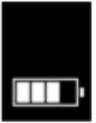
Before you begin
Nymi provides a custom charging cradle for charging the Nymi Band.

Figure 51: Battery Charger

The Nymi Band provides battery screens that indicate the charge level of the Nymi Band. When the user connects the charger to the Nymi Band, the Nymi Band vibrates and the battery icon changes to indicate the Nymi Band is being charged. A blue LED on the charger lights up indicating that the Nymi Band is charging.

Note: The Nymi Band does not vibrate if the `Haptic Feedback on Nymi Bands` is not enabled for the user or active group policy.

0% - 4%	5% - 25%	26% - 50%	51% - 75%	76% - 100%

About this task

To charge a Nymi Band, perform the following steps:

Procedure

1. Plug the charging cradle into the USB port on your computer or a USB charging hub. A red LED indicator appears in near the top of the charging cradle indicating that it is receiving power.

2. Hold the cradle side of the Nymi Band charger close to the underside of the Nymi Band until it attaches magnetically. Make sure the pins on the charging cradle align with the port on the back of the Nymi Band. The Nymi Band vibrates indicating that it is receiving power. A blue indicator light appears on the side of the charging cradle to indicate that the user successfully connected the Nymi Band to the charging cradle and the Nymi Band is receiving power.

   Note: The Nymi Band does not vibrate if the `Haptic Feedback on Nymi Bands` is not enabled for the user or active group policy.

3. Push the bottom button on the Nymi Band to view the amount of battery charge that is on the Nymi Band.

   Figure 52: Charging battery indicator

4. When the Nymi Band is fully charged, disconnect the charging cradle from the Nymi Band.

   Figure 53: Full battery indicator

12.4 - Managing Battery Life

If the battery reaches a critically low level, the screen displays the critically low charge image, and then Nymi Band vibrates and shuts down.

Note: The Nymi Band does not vibrate if the `Haptic Feedback on Nymi Bands` is not enabled for the user or active group policy.

To use the Nymi Band again, the user will need to charge it for at least 30 minutes. While charging, the screen might show the critically low charge image for several minutes, and then displays the charging battery indicator.

The typical battery life of the Nymi Band depends on how the Nymi Band is used. The following table summarizes the usage scenarios, activities, and the typical battery life in each scenario.

Table 5: Typical Battery Life

Usage Scenario	Daily Activities	Typical Battery Life
Pharmaceutical Manufacturing	Nymi Band is off body for 14 hours and on body for 10 hours. 300 Tap-to-Authenticate operations (non-SEOS) 20 physical access transactions	3 days
General Enterprise	Nymi Band is off body for 14 hours and on body for 10 hours. 25 physical access transactions 20 print job releases 20 terminal unlocks	3 days

The Nymi Band screen displays icons that indicate the current battery life availability.

- High battery life - an icon with four bars.
- Medium battery life - an icon with two or three bars.
- Low battery life - an icon with one bar.

Additional icons display when the Nymi Band is:

- plugged into a charger.
- charging.
- fully charged.

12.5 - Exiting Sleep Mode

To conserve battery life, the Nymi Band goes into sleep mode in the following situations:

- When a user removes the Nymi Band
- When the battery level of the Nymi Band is low
- About 30 seconds after a user authenticates to the Nymi Band

When in sleep mode, the screen on the Nymi Band is blank. To exit sleep mode, the user must charge the Nymi Band if required, and then press any button on the Nymi Band.

12.6 - Authenticating User Identity to the Nymi Band

Each time the user removes the Nymi Band, the Nymi Band deauthenticates. To use the Nymi Band to perform tasks, the user must authenticate to the Nymi Band. How the user authenticates depends on the group policy configuration.

12.6.1 - Authentication by Fingerprint

When the screen displays the fingerprint icon, the user holds their finger on the square fingerprint sensor and surrounding bezel. The Nymi Band displays the fingerprint authentication screen while fingerprint match and optional ECG liveness detection are in progress during authentication. The ECG liveness detection is automatically enabled for the default group policy. Refer to section *Configuring Liveness Detection* in the section *Customizing the Nymi Band Authentication Method* for information about how to disable ECG liveness detection.

Figure 54: Fingerprint Authentication screen

When the Nymi Band displays one of the following icons, the user identity was successfully authenticated, and the user can remove their finger from the fingerprint sensor and fingerprint bezel.

Figure 55: Authentication Success Screen with Band Label

Figure 56: Authentication Success Screen without Band Label

12.6.1.1 - Authentication Failures

When authentication of the Nymi Band fails, the Nymi Band vibrates and displays a message.

Note: The Nymi Band does not vibrate if the `Haptic Feedback on Nymi Bands` is not enabled for the user or active group policy.

Nymi Band authentication failures occur for one of the following reasons:

* Fingerprint matching failure—when the authentication fails as a result of a fingerprint mismatch, the Nymi Band vibrates and displays a **No Match** message about 1 second after the user places their finger on the fingerprint sensor and bezel. When the Nymi Band screen displays the fingerprint icon, the user can retry authentication. The message that appears on the Nymi Band screen when there are subsequent authentication failures due to fingerprint depends on the number of consecutive failures:

    * When there are less than 4 consecutive fingerprint match failures, the **No Match** message appears.
    * When there are more than 3 consecutive fingerprint match failures, the Nymi Band displays a message that provides advice that can result in a successful authentication. Possible messages include **Center Finger**, **Wash and Dry Hand and Wrist**, and **Clean Band**.

* Liveness failure—when the authentication fails due to the inability to detect a consistent ECG signal on the wrist, the Nymi Band vibrates and displays the **No ECG** message about 13 seconds after the user places their finger on the fingerprint sensor and bezel. When the Nymi Band screen displays the fingerprint icon, the user can retry authentication. The message that appears on the Nymi Band screen when there are subsequent authentication failures due to liveness detection issues depends on the number of consecutive failures:

    * When there are less than 4 consecutive fingerprint match failures, the **No ECG** message appears.
    * When there are more than 3 consecutive fingerprint match failures, the Nymi Band displays a message that provides advice that can result in a successful authentication. Possible messages include **Sit Still**, **Wash and Dry Hand and Wrist**, and **Don't Move**.

Troubleshooting Fingerprint Mismatch Failures

If the fingerprint authentication fails, ensure the following:

* Fingerprint sensor is clean and dry.

    * If the fingerprint sensor is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
    * If the fingerprint sensor is wet, dry completely with a lint-free towel, and then retry authentication.
* User does not press too hard or too softly on the fingerprint sensor.
* User's finger is clean and dry.

    * If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication.
    * If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
    * If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication

- User places their finger on the centre of the sensor, touching the surrounding bezel.
- User keeps their finger still on the sensor and bezel during the authentication period.
- User does not lift their finger off the sensor or bezel until the authentication process completes.
- User wears the Nymi Band snugly on the wrist.
- User wears their own Nymi Band.
- User attempts authentication with the same the finger that they used during enrollment.
- User finger is not damaged, for example the user has cut their finger.

   Note: If the finger that is used for authentication is damaged, consider one of the following actions:

   - Instruct the user to authenticate by corporate credentials until the finger heals.
   - Delete the user data on the Nymi Band, disassociate the user from the Nymi Band in NES and Evidian, and then perform enrollment with a different finger.

Troubleshooting Liveness Detection Failures

If the liveness detection fails, ensure the following:

- Bottom sensor is clean and dry.

   - If the bottom electrode is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
   - If the bottom electrode is wet, dry completely with a lint-free towel, and then retry authentication.
- User's finger is clean and dry.

   - If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication
   - If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
   - If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication
- User keeps their finger still on the sensor and bezel during the authentication period.
- User's wrist is not too dry. Before authentication, wash and completely dry the wrist before putting on the Nymi Band, or rub some lotion well into the wrist, and then retry authentication.
- Nymi Band bottom electrode remains in contact with the wrist during the authentication period. If the position of bottom electrode prevents contact, remove the Nymi Band, reposition the Nymi Band on the wrist, and then try authentication again.
- User does not lift their finger off the sensor or bezel until the authentication process completes.
- Nymi Band fits snugly on the wrist and does not move around during the authentication process.
- User's wrist is not tattooed where the bottom sensor makes contact.

Note: If the user cannot use another wrist or the Nymi Band cannot make contact with an area that is not tattooed, instruct the user to authenticate by corporate credentials.

Troubleshooting Persistent Authentication Failures

Lockout policies help prevent adversarial users from gaining unauthorized access to systems through brute-force attacks.

When an authentication lockout occurs, the Nymi Band displays the **See Admin** icon and prevent the user from performing additional authentication attempts. An authentication lockout occurs in the following scenarios:

* After 50 consecutive failed authentication attempts on a previously enrolled Nymi Band due to a fingerprint mismatch.
* After 3 consecutive failed attempts to complete the fingerprint template during the enrollment due to an issue with the fingerprint imaging.

The lockout persists on the Nymi Band, even if the user removes the Nymi Band. The lockout will also persist while the Nymi Band is dead or while charging.

Clear the lockout by one of the following methods:

* Re-enroll the user to the Nymi Band.
* Authenticate the user with their credentials in the Nymi Band Application. A user can authenticate by using corporate credentials only if the `Corporate Credentials Authentication` option was enabled in the NES policy at the time of enrollment.

If the user persistently cannot authenticate to the Nymi Band, consider the following actions:

* Restart the Nymi Band and retry authentication.
* Instruct the user to log into the Nymi Band Application while wearing the Nymi Band and authenticate by corporate credentials.
* Delete the user data from the Nymi Band and then disassociate the Nymi Band from the user in NES and Evidian (if used), and then enroll with a different finger.
* Delete the user data from the Nymi Band, disassociate the Nymi Band from the user in NES and Evidian, and then enroll the user with a different Nymi Band.

For reference, use the following troubleshooting workflows.

Ensure:

-Fingerprint sensor is clean and dry.
-Finger is clean and dry.
-User does not press too hard or too softly on the fingerprint sensor.
-User places their finger on the centre of the sensor, touching the surrounding bezel.
-User keeps their finger still on the sensor and bezel during the authentication period.
-User does not lift their finger off the sensor or bezel until the authentication process completes.
-User wears the Nymi Band snugly on the wrist.
-User wears their own Nymi Band.
-User attempts authentication with the same the finger that they used during enrollment.

12.6.2 - Authentication by Corporate Credentials

When the screen displays the fingerprint icon, the user logs into the Nymi Band Application, and clicks the **Authenticate** button, as shown in the following figure.
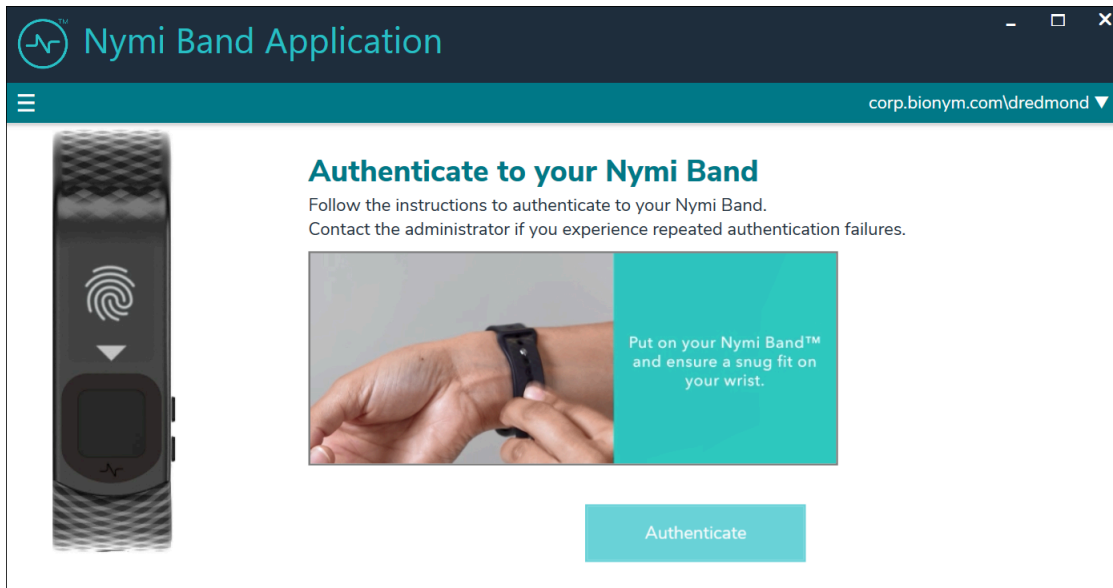
Figure 57: Authentication by Corporate Credentials

When the Nymi Band displays the success icon (checkmark), the user identity was successfully authenticated, and the user can log out of the Nymi Band Application.

12.7 - Cleaning the Nymi Band

For recommendations on cleaning the Nymi Band, refer to the *Nymi Band 3.0 Cleaning Recommendations Guide.*

12.8 - Restarting the Nymi Band

While troubleshooting an issue, you might be required to restart, or reboot, the Nymi Band.

About this task

Note: A restart does not change any data on the Nymi Band. The Nymi Band remains registered to the user and enrolled in the enterprise.

Perform the following steps to restart the Nymi Band.

Procedure

1. Ask the user to remove the Nymi Band.
2. Plug the Nymi Band into a charger.
3. Press and hold the top button, the word **RESTART** and a countdown progress bar appears on the screen. Continue to hold the top button for 10 seconds to complete the countdown,

and initiate the restart procedure. The following figure shows the **RESTART** message with countdown.

Figure 58: RESTART message

Results

The Nymi Band restarts and startup messages appear on the screen. The restart process takes about 20 seconds to complete.

12.9 - Determining the Nymi Band Firmware Version

When troubleshooting an issue, you might require the Nymi Band firmware version. Perform the following steps to determine the firmware version on a Nymi Band.

About this task

This procedure requires you to use the Nymi Band charging cable to put the Nymi Band on charge.

Procedure

1. Remove the Nymi Band from the wrist of the user.

2. Put the Nymi Band on the charger.

3. Press and release the top and bottom button.
   The firmware version appears on the screen, as shown in the following figure.

Figure 59: Nymi Band firmware version

12.10 - Determining Enrollment Location

The `Nymi Band Properties` page in the NES Administrator Console provides you with an information to help you determine which Nymi Enterprise Server(NES) the user accessed to complete their enrollment in an IT/OT configuration.

About this task

Perform the following steps with a NES Administrator account.

Procedure

1. In the `Search` page, select the `Users` Option.
2. In the `Search` field, type the full or partial username, first name, or last name of the user.
3. Click `Search`. The `Search` page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the `User Details` page.
5. In the `Nymi Band` section, select the Nymi Band.
   The `Nymi Band` page appears with details about the Nymi Band. The `Is Nymi Band Enrolled Here` option provides you with the enrollment location. One of the following values appear:

   • Yes—When the Nymi Band enrollment completed on the current NES.
   • No—When the Nymi Band enrollment completed on another NES an the IT/OT environment.

   The following image provides an example where the Nymi Band enrollment completed on the current NES.

Figure 60: Nymi Band properties page

13 - Nymi Band User Management

Nymi Bands for each user can be managed through the NES Administrator Console.

There are circumstances where you need to change the status of your Nymi Band.

Select Search from the NES Administrator Console to perform the following actions:

* Searching for User or Nymi Band Information
* Issuing a temporary Nymi Band to a user
* Replacing the Nymi Band for a user
* Suspending a Primary Nymi Band for a user
* Deleting a Nymi Band from a user
* Deleting User Data
* Reassigning a Nymi Band
* Restoring the Nymi Band

13.1 - NFC (Unique Identifier) UID Management

When the Nymi Band is unenrolled, a randomly generated NFC UID is available each time it is tapped on an NFC reader when on charger or on-body. This randomly generated NFC UID differs in length from the static NFC UID available when the Nymi Band is authenticated.

About this task

13.2 - Searching for User or Nymi Bands Information

The Search page enables Administrators to search the NES database for information about users, individual user policy membership, or Nymi Bands.

Searching for Nymi Band information is particular useful for:

* locating a specific Nymi Band during inventory
* disassociating a user from a Nymi Band
* locating the user of a misplaced Nymi Band

The Search page provides Administrators with two types of search options:

- Users - Search for Active Directory users that are in the domain(s) managed by NES and display information about the Nymi Band(s) that are assigned to the user account
- Nymi Bands - Search for Nymi Band details by using the Nymi Band serial number
- Individual User Policies - Search for users that are a member of an individual user policy or are not a member of any individual user policy.

13.2.1 - Searching for Users

The `Search` page enables NES Administrators to search for enrolled Nymi Band users by first name, last name, or username.

About this task

Procedure

1. From the NES Administrator Console, select **Search**.

   The Search page appears.

2. In the `Search` page, select the **Users** option.

3. In the **Search** field, type the full or partial criteria for the following:

   - First name, last name of the user that logs in to the network terminal (space between first name and last name)
   - Username, as the value appears in AD

4. Click **Search**.

   The `Search` page provides a list of matching users, and provides summary information about Individual User Policy or Group policy membership and the status of the application of a policy to a user. There are four status types:

   - No active Nymi Band—The user does not have an active Nymi Band.
   - Pending—The policy on the Nymi Band does not match the policy (individual user policy or global policy) that is applied to the user. For example, the policy was applied to the user after enrollment, and the user has not signed into the Nymi Band Application while wearing their authenticated Nymi Band to activate the policy changes.

     Note: CWP 1.1 is the minimum firmware version that supports the ability to configure liveness detection. If you disable liveness detection in the NES group policy or an individual user policy and the Nymi Band firmware does not support configurable liveness detection, the policy status for the Nymi Band remains in the "Pending" state.

   - Active—The policy on the Nymi Band matches the policy (individual user policy or global policy) that is applied to the user.
   - Information unavailable—Enrollment occurred on an earlier version of Nymi Band Application that does not support the policy status features. Individual policy support starts with the CWP 1.3 Nymi Band Application.

   The following figure provides an example of the `Search` page when multiple users are found based on the search criteria.

Figure 61: Users Search Results Page

By default, the search result displays 10 users. Use the navigation controls to move between the pages of users and the list box to change the number of users to display on the pane to 20 or 50 per page.

5. Select a user by clicking the `Domain\username` link.

13.2.1.1 - User Details Page

When you select a user in the `User Search Results` page, the `User Details` page appears, which provides information about user account settings.

The following figure provides an example of the `User Details` window.
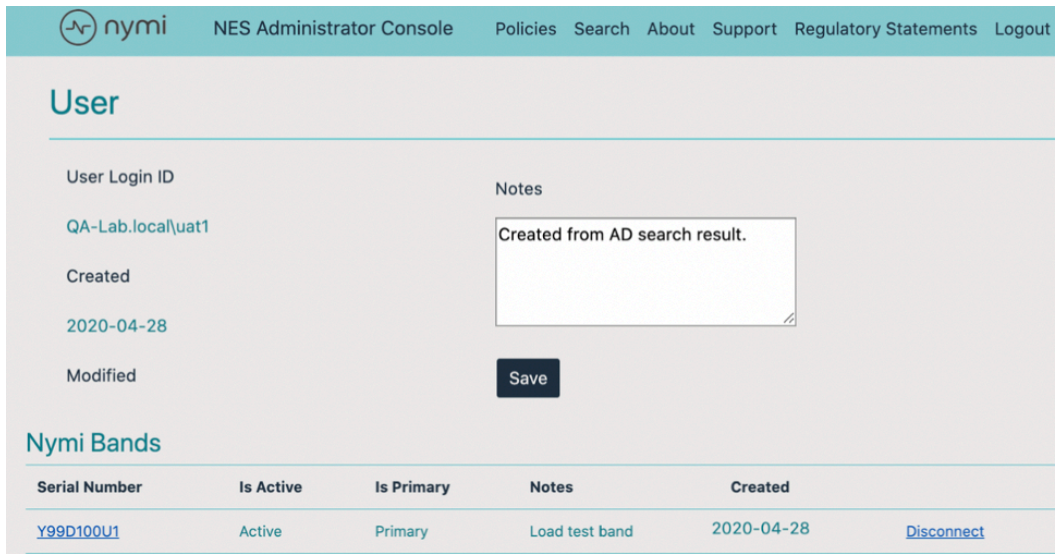
Figure 62: User Details Page

Table 6: User Details Summary

Field	Description
Serial Number	Provides the serial number of the Nymi Band.
Is Active	Displays Active when the Nymi Band is active, and is blank when the Nymi Band is disabled.
Is Primary	Displays Primary when the user has at least one Nymi Band assigned, and the Nymi Band is the primary Nymi Band. Appears empty when the Nymi Band is a temporary Nymi Band.
Notes	Displays an informative message about the Nymi Band that was supplied by the administrator.
Created	Displays the date that the Nymi Band was registered to the user or the date that an Administrator first searched for a user.
Disconnect	Deletes the Nymi Band association with the user. Use this option to disassociate the Nymi Band from a user as a part of the Delete User Data process.

13.2.2 - Searching for Nymi Bands

The `Search` page enables NES Administrators to search by a serial number for an enrolled or registered Nymi Band.

About this task

In an IT/OT environment, a Nymi Band that a user enrolled on an Enrollment NES does not appear for the user on the Registration NES until the user logs into the Registration Terminal to complete the registration process.

Procedure

1. In the NES Administrator Console, select **Search**.

2. In the Search page, select the **Nymi Bands** option.

3. In the **Search** field, type the serial number of the Nymi Band (located on the back of the Nymi Band).

4. Click **Search**.

   The following figure provides an example of the Search page when searching by the Nymi Band serial number.

Figure 63: Nymi Band Search Results Page

By default, the search results display 10 Nymi Bands. Use the navigation controls to move between the pages of Nymi Bands and the list box to change the number of users to display on the pane to 20 or 50 per page

5. Do one of the following:

- In the returned search list, click the **`Domain\username`** link. The `User Details` page displays with the user's information.
- In the returned search list, click the `Serial Number` link. The `Nymi Band` details page displays with information about a Nymi Band.

13.2.2.1 - Nymi Band Details Page

The `Nymi Band` details page displays information about a Nymi Band.

Table 7: Nymi Band Details Summary

Field	Description
Domain\Username	Provides the domain and username of the Nymi Band user. The domain is the AD server that stores this information about the user.
Band ID	Displays the MAC address number of the Nymi Band.
NFC UID	Displays the ID that is readable by Near Field Communication (NFC) technology when the Nymi Band is authenticated.
Security App Key	Displays the status of the symmetric key ID of the Nymi Band. • If the policy is configured to support the creation, ID is created the field displays, **`Created`** • If the ID is not created the field displays, **`Not Created`**
Corp Credentials Auth	Displays the status of the External Authenticator creation. • If a policy enables the use of External Authenticator, the field displays **`Created`** • If a policy is not configured to enable the use of an External Authenticator, the field displays **`Not Created`**
Serial Number	Displays the unique value that is located on the back of the Nymi Band.
Encrypted Password	Indicates if the user's password was encrypted and saved in NES database. • If the password was encrypted and saved, the field displays **`Stored`** • If the password was not encrypted and not saved, the field displays **`Missing`**

Field	Description
Has Fingerprint	Indicates if the user's fingerprint step was performed during enrollment. • If the fingerprint step was performed, the field displays `Yes` • If the fingerprint step was not performed, the field displays `No`
Band Label	Displays the Band Label assigned to the Nymi Band. Band Labels can only be assigned to Nymi Band 3.0, when the active policy is configured to support the option.
Firmware Version	Displays the version of the Nymi Band firmware at the time of enrollment.
Is Band Enrolled Here	Displays the enrollment status of the Nymi Band on NES. One of the following values appears" • Yes-The user enrolled the Nymi Band to this NES. • No-The user registered the Nymi Band to this NES and enrolled the Nymi Band to another NES in the IT/OT environment. If the user registered the Nymi Band on this NES, the following message also appears: "NES does not manage the policy on this Nymi Band. Connect to the Enrollment NES to manage the policy. "
Created	Displays the date that the Nymi Band was registered to the user or the first time that an NES Administrator searched for the user.
Modified	Displays the date that the Nymi Band assignment was modified.
Is Active	Displays Active when the Nymi Band is active and is empty when the Nymi Band is disabled.
Is Primary	Displays Primary when the user has at least one Nymi Band assigned, and the Nymi Band is the primary Nymi Band. Appears empty when the Nymi Band is a temporary Nymi Band.
Notes	Displays an informative message that an CWP Administrator typed about the Nymi Band.

The following figure provides an example of the `Nymi Band Details` window.

Figure 64: Nymi Band Details page

13.2.3 - Searching for Individual User Policy Membership

The `Search` page enables NES Administrators to display all users that are a member of an individual user policy.

About this task

Procedure

1. From the NES Administrator Console, select `Search`.

   The Search page appears.

2. In the `Search` page, select the `Individual User Policy` option.

3. From the policy list, select the Individual User Policy, and then click `Search`.

Results

The `Search Results` window appears with a list of users. By default, the search results display 10 individual user policies. The **`Individual User Policy`** column displays the name of the individual policy that is assigned to a user. If a user is not assigned to an individual user policy, `none[group policy applied]` appears. Use the navigation controls to move between the pages of users and the list box to change the number of users to display on the pane to 20 or 50 per page. The following figure provides an example of the Search Results window.

Figure 65: Individual User Policy Search Results

The search results include information about the status of the application of a policy to a user. There are four status types:

- No active Nymi Band—The user does not have an active Nymi Band.
- Pending—The policy on the Nymi Band does not match the policy (individual user policy or global policy) that is applied to the user. For example, the policy was applied to the user after enrollment, and the user has not signed into the Nymi Band Application while wearing their authenticated Nymi Band to activate the policy changes.

  Note: CWP 1.1 is the minimum firmware version that supports the ability to configure liveness detection. If you disable liveness detection in the NES group policy or an individual user policy and the Nymi Band firmware does not support configurable liveness detection, the policy status for the Nymi Band remains in the "Pending" state.
- Active—The policy on the Nymi Band matches the policy (individual user policy or global policy) that is applied to the user.
- Information unavailable—Enrollment occurred on an earlier version of Nymi Band Application that does not support the policy status features. Individual policy support starts with the CWP 1.3 Nymi Band Application.

13.3 - Determining Enrollment Location

The `Nymi Band Properties` page in the NES Administrator Console provides you with an information to help you determine which Nymi Enterprise Server(NES) the user accessed to complete their enrollment in an IT/OT configuration.

About this task
Perform the following steps with a NES Administrator account.

Procedure

1. In the **Search** page, select the **Users** Option.
2. In the **Search** field, type the full or partial username, first name, or last name of the user.
3. Click **Search**. The `Search` page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the **User Details** page.
5. In the **Nymi Band** section, select the Nymi Band.
   The `Nymi Band` page appears with details about the Nymi Band. The **Is Nymi Band Enrolled Here** option provides you with the enrollment location. One of the following values appear:

   - Yes—When the Nymi Band enrollment completed on the current NES.
   - No—When the Nymi Band enrollment completed on another NES an the IT/OT environment.

   The following image provides an example where the Nymi Band enrollment completed on the current NES.

Figure 66: Nymi Band properties page

13.4 - Deleting User Data

The Delete User Data process clears personal information, such as the fingerprint template and credentials, from the Nymi Band that is currently enrolled to a user. This process also clears the lockout during a failed authentication lockout.

About this task

Before you can re-enroll a Nymi Band, you must perform the delete user data operation.

Procedure

1. Remove the Nymi Band from the wrist of the user, and then attach the Nymi Band to a charger.

2. On the Nymi Band, hold the bottom button. The Delete User Data message displays on the screen, as shown in the following figure.

   Note: The Nymi Band does not vibrate if the `Haptic Feedback on Nymi Bands` is not enabled for the user or active group policy.

Figure 67: Delete User Data

3. Continue to hold the bottom button until the Nymi Band vibrates quickly twice and the **USER DATA DELETED** message displays on the screen (after about 10 seconds), as show in the following figure.

Figure 68: User Data Deleted

Results

Biometric authentication does not work for the user after you perform a delete user data operation. To use the Nymi Band again, the user must enroll the Nymi Band by using the Nymi Band Application.

Note: If you delete the user data on a Nymi Band and attempt to re-enroll it, you will see the following message,

A Nymi Band has been assigned to (user name), however it cannot be found.

To proceed, you need to delete the Nymi Band association with the user in the NES Administrator Console.

13.5 - Replacing, Re-Enrolling or Re-Registering the Nymi Band for a User

After a user enrolls to a Nymi Band, there are several reasons that a user might need to repeat enrollment:

- User might need to temporarily enroll to another Nymi Band when they have forgotten their Nymi Band at home.
- User might need to permanently enroll to another Nymi Band when they have lost their Nymi Band or the Nymi Band does not function correctly.
- User might need to re-enroll their Nymi Band when the characteristics of their fingerprint change, for example, when their finger has a cut.
-

Nymi provides you with configuration options that allow users to perform self-service re-enrollment without the assistance of an CWP Administrator. Alternatively, you can ensure that users only complete re-enrollment with the assistance of a CWP Administrator.

The steps to replace or re-enroll a Nymi Band differ depending on your configuration.

13.5.1 - Managing Nymi Band Re-Enrollments and Re-registrations with Self-Service

When you enable the self-service enrollment and self-service registration feature in the active Nymi Enterprise Server(NES) administration policy, users can re-enroll and re-register their own Nymi Band or optionally a Nymi Band that is currently assigned to another user without the assistance of an CWP Administrator.

Before you begin

Customizing Self-Service Re-Enrollment and Self_service Re-Registration provides detailed information about how to configure the NES active policy to allow a user to self-enroll and self-register their own Nymi Band or to the Nymi Band of another user.

Note: User with SEOS-enabled Nymi Bands cannot use self-service re-enrollment to re-enroll a Nymi Band that was previously assigned to a another user.

About this task

Instruct the user to perform the following steps.

Procedure

1. Perform the delete user data operation on the Nymi Band identified for re-enrollment.
2. Log into the Nymi Band Application and complete the steps for enrollment.

   The steps to complete a re-enrollment and re-registration are identical to the steps that the user follows to complete a new enrollment and registration.
3. For FIDO2 only, when a user enrolls to another Nymi Band, the user must re-create the FIDO2 security key on the newly enrolled Nymi Band.

Results

If the user re-enrolls/re-registers their own Nymi Band, the same Nymi Band appears in the `User Properties` window in the NES Administrator Console.

If a user re-enrolls/re-registers a Nymi Band that was assigned to another user, the following changes appear in the `User Properties` window in the NES Administrator Console of the Enrollment NES and Registration NES:

- The original Nymi Band appears for the user is not active but remains as the primary Nymi Band.
- The newly enrolled Nymi Band appears for the user and is set to active.

The following figure provides an example where a user named tw-user2 enrolled to a Nymi Band with serial number AAAH-00125, and then performed a self-service enrollment to second Nymi Band with serial number ACAK-00056.

Figure 69: User with multiple Nymi Bands after self-service re-enrollment.

13.5.2 - Managing Nymi Band Re-Enrollments and Re-Registration Manually

When you do not enable self-service re-enrollments and self-service re-registrations, a CWP Administrator must perform steps in the NES Administrator Console before the user can re-enroll to their own Nymi Band or a Nymi Band that is assigned to another user.

13.5.2.1 - Replacing Nymi Bands Without Self-Service Re-Enrollment or Self-Service Re-Registration

In environments that do not allow users to perform self-service re-enrollments and self-service registrations, the process to issue a temporary Nymi Band, to replace a Nymi Band or to re-enroll/re-register to the same Nymi Band, requires the NES Administrator to disassociate the Nymi Band from the user in the NES Administrator Console before the user can enroll to another Nymi Band.

Issuing a temporary Nymi Band to a User

A user can only have one active Nymi Band. If a user requires a temporary Nymi Band, perform the following steps to disable the existing Nymi Band for the user, and then add a new Nymi Band for the user.

About this task

In the IT/OT configuration, perform these steps on the Enrollment NES and Registration NES.

Note: You must enroll the temporary Nymi Band. User data is not transferred between Nymi Bands.

This process involves two main steps:

*   Suspending the existing Nymi Band associated with the user
*   Enrolling a temporary Nymi Band to the user

Procedure

1. In the **Search** page, select the **Users** Option.
2. In the **Search** field, type the full or partial username, first name, or last name of the user.
3. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the **User Details** page.
5. Click the Serial Number of the original Nymi Band. The Nymi Band page appears.
6. Clear the **Is Active** box.
7. Select the **Is Primary** box.
8. Click **Save**.

    The original Nymi Band is disabled.

    Note: The Is Primary option provides an administrator with the ability to distinguish between the original (primary) Nymi Band and the temporary Nymi Band.

9. Contact the user to enroll the temporary Nymi Band.
10. The User page should appear with the following updated information:

    *   Is Active field for the original Nymi Band is empty.
    *   Is Primary field for the original Nymi Band displays Primary.
    *   Is Active field for the temporary Nymi Band displays Active.
    *   Is Primary for the temporary Nymi Band is empty.

Restore Use of the Original Nymi Band

When a user retrieves their original Nymi Band, they can continue to use the replacement Nymi Band or use their original Nymi Band.

To use the original Nymi Band, you can disassociate the temporary Nymi Band from the user or you can de-activate the Nymi Band.

Note: If you de-activate the Nymi Band, you can re-activate the Nymi Band and the user can use the Nymi Band again if they did not perform the delete user data operation.

Restoring the Nymi Band by Deactivating the Nymi Band
Perform the following steps in the NES Administrator Console to restore the original Nymi Band for a user who performed self-service re-enrolled/re-registration to temporarily use another Nymi Band.

About this task
In the IT/OT configuration, perform these steps on the Enrollment NES and Registration NES

Procedure

1. In the **Search** page, select the **Users** Option.
2. In the **Search** field, type the full or partial username, first name, or last name of the user.
3. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the **User Details** page.
5. On the **Users** page, perform the following actions:
   a) Click the **Disconnect** link beside the Nymi Band.
   b) On the Disassociate window, scroll down and click **Disassociate**.
6. Select the **Is Active** box and (if necessary) the **Is Primary** box.
7. Click **Save**. The original Nymi Band is enabled for the user. The Is Active field for the temporary Nymi Band is empty.

Replacing the Nymi Band for a User

A user can have one active Nymi Band only. If a user requires a new Nymi Band, for example, to replace a lost or broken one, perform the following steps to disable the existing Nymi Band for a user, and then add a new Nymi Band for the user.

About this task

In the IT/OT configuration, perform these steps on the Enrollment NES and Registration NES.

Note: You must enroll the new Nymi Band. User data does not transferred between Nymi Bands.

This process involves two main steps:

- Suspending or disassociating the user's existing Nymi Band.
- Enrolling the Nymi Band to the user.
- In IT/OT configurations, registering the Nymi Band to the user

Procedure

1. In the **Search** page, select the **Users** Option.
2. In the **Search** field, type the full or partial username, first name, or last name of the user.
3. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the **User Details** page.
5. Click the Serial Number of the original Nymi Band. The Nymi Band page appears.
6. Clear the **Is Active** box.
7. In the **Notes** field, add descriptive information, such as **Lost Band**.
8. Click **Save**.
   The original Nymi Band is disabled.

What to do next

Contact the user to enroll the new Nymi Band with the Enrollment Terminal. In IT/OT configurations, instruct the user to register with the Registration Terminal

When the enrollment and if required, registration succeeds, in the NES Administrator Console of the Enrollment NES and Registration NES click **Back to Owner**.

The User page should appear with the following updated information:

- **Is Active** field for original Nymi Band is empty.
- **Is Primary** field for the original Nymi Band is empty.
- **Is Active** field for the new Nymi Band displays **Active**.

Note: If the original Nymi Band is found, perform a Delete User Data process of the original Nymi Band.

Reassigning a Nymi Band

To assign a Nymi Band to a user when the Nymi Band is already registered to another user, you must perform a delete user data process on the Nymi Band, delete the Nymi Band from the NES database, and then instruct the new user to enroll and register the Nymi Band.

Before you begin

Perform a delete user data process of the Nymi Band. See section *Deleting User Data* for more information.

Note: Performing the delete user data process on a Nymi Band removes all user data for the original user. You can still query audit events for the original user of the Nymi Band. See *NES Audit Logging.*

About this task

Perform the following steps in the NES Administrator Console to assign a Nymi Band to a different user.

In the IT/OT configuration, perform these steps on the Enrollment NES and Registration NES

Procedure

1. In the **Search** page, select the **Users** Option.
2. In the **Search** field, type the full or partial username, first name, or last name of the user.
3. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the **User Details** page.
5. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **Disconnect**. On the Disconnect page, scroll down and then click **Disconnect**.

What to do next

Contact the user to enroll the new Nymi Band with the Enrollment Terminal. In IT/OT configurations, instruct the user to register with the Registration Terminal.

When the enrollment and if required, registration succeeds, in the NES Administrator Console of the Enrollment NES and Registration NES, search for the user in the NES Administrator Console, open the `User Details` page and confirm that in the **`Nymi Band`** table, the Nymi Band is Active.

13.5.2.2 - Re-enrolling/Re-registering a User to the Same Nymi Band without Self-Service

User might require re-enrollment and re-registration of their current Nymi Band in the event of multiple fingerprint authentication failures or when must use a different fingerprint for authentication, for example, due to a cut.

Before you begin

Perform a delete user data process of the Nymi Band. See section Deleting User Data for more information.

About this task

To re-enroll and re-register a user to their Nymi Band, the NES Administrator must delete the Nymi Band to user association in NES and the user or administrator must delete the user data on the Nymi Band.

Perform the following steps in the NES Administrator Console to assign a Nymi Band to a different user. In an IT/OT configuration perform these steps on the Enrollment NES and Registration NES.

Procedure

1. In the **`Search`** page, select the **`Users`** Option.
2. In the **`Search`** field, type the full or partial username, first name, or last name of the user.
3. Click **`Search`**. The `Search` page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the **`User Details`** page.
5. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **`Disconnect`**. On the Disconnect page, scroll down and then click **`Disconnect`**.

What to do next

Contact the user to enroll the Nymi Band with the Enrollment Terminal. In IT/OT configurations, instruct the user to register with the Registration Terminal.

When the enrollment and if required, registration succeeds, in the NES Administrator Console of the Enrollment NES and Registration NES, search for the user in the NES Administrator Console,

open the `User Details` page and confirm that in the **Nymi Band** table, the Nymi Band is Active.

13.6 - Suspending the Active Nymi Band for a User

Suspending the Nymi Band disables the ability of the assigned user to use the Nymi Band to complete authentication tasks. For example, the user cannot tap the Nymi Band to perform an e-signature or unlock a terminal session. Biometric authentication will continue to work for the user until you perform a Delete User Data process on the Nymi Band. See the section *Deleting User Data* for more information.

About this task

Perform the following steps to disable the primary Nymi Band for a user.

In the IT/OT configuration, perform these steps on the Enrollment NES and Registration NES

Procedure

1. In the **Search** page, select the **Users** Option.
2. In the **Search** field, type the full or partial username, first name, or last name of the user.
3. Click **Search**. The `Search` page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the **User Details** page.
5. Click the Serial Number of the original Nymi Band. The `Nymi Band` page appears.
6. Clear the **Is Active** box.
7. Select the **Is Primary** box.
8. Click **Save**.

13.7 - Disconnecting the Nymi Band from a user in NES

Disconnecting the Nymi Band that is associated with a user prevents the user from using the Nymi Band for authentication tasks, but the user can continue to authenticate to the Nymi Band until you perform a Delete User Data operation on the Nymi Band.

About this task

Note: In this release, if you disconnect a Nymi Band for a user, you lose the ability to gather historical information about Nymi Band usage from the NES database.

Perform the following steps in the NES Administrator Console to disconnect the Nymi Band that is associated with a user.

In the IT/OT configuration, perform these steps on the Enrollment NES and Registration NES

Procedure

1. In the `Search` page, select the `Users` Option.
2. In the `Search` field, type the full or partial username, first name, or last name of the user.
3. Click `Search`. The `Search` page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the `User Details` page.
5. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click `Disconnect`. On the Disconnect page, scroll down and then click `Disconnect`.
6. On the `Disconnect` screen, scroll to the bottom and select `Disconnect`.

14 - Data Storage

Nymi stores information related to NES in a SQL database.

Users can install a SQL querying tool such as SSMS or a custom built application that is capable of running T-SQL queries and run SQL queries to view the database tables.

14.1 - Storage of NES Data

Nymi stores information related to the NES configuration, the Nymi Band, and the Active Directory username for users in several tables in a SQL database. You can perform queries to gather transactional information, such as changes to the NES policy configuration, enrollments, and Nymi Band deactivations.

By default, the account that installs the SQL server software has read access to the NES database. During NES configuration you can add additional Auditor accounts that have read-only access to Audit tables. The Auditor account is not limited to specific Active Directory (AD) users, but can be an AD group, so that AD users can be added to that group later by AD administrator.

14.1.1 - Adding Additional Users or Groups to View and Query the Audit Database

When you configure NES during deployment, you define the users or groups that have access to the NES audit log database.

About this task
Perform the following actions to provide additional users or groups access to the NES SQL database.

Note: These steps apply to an NES database that was configured to use Windows authentication.

Procedure

1. Log in to the NES server with the account that performed the NES installation and configuration.
2. Navigate to the directory that contains the NES installation software.
3. From the directory that contains the extracted NES installation package, run *..\NesInstaller \install.exe.*
4. On the `User Access Control` window, click **Yes**.

5. On the `Open File - Security warning` window, click **Run**.

6. If applicable, on the `User Access Control` page, review the Microsoft .NET EULA, and then click **Accept**. Complete the .NET installation and continue with the NES installation.

7. On the `Application Install Security Warning` window, click **Install**.

8. On the `Open File - Security warning` window, click **Run**.

9. On the left navigation pane, click **Location**, and then perform the following steps.

  a) In the **Install Root** field, confirm that the path to the NES services is correct, as it was specified during the initial deployment.

  The default location is *C:\inetpub\wwwroot*.

  b) In the **Instance Name** field, type the descriptive name that was specified during the initial deployment for the NES web application instance name. For example, NES. See Configuration Attribute Values in the Nymi Connected Worker Platform—Deployment Guide.

  Note: Ensure that the values that you specify in the **Install Root** and **Instance Name** match the values that you specified when you deployed the previous version of NES. When the values that you specified in the **Install Root** and **Instance Name** are correct, the **Location** test results will show Install Type: Update/ Re-Install. If there is no match for the values entered, the **Location** test results will show New Installation for the Install Type. The following figure provides an example of the **Location** window for an NES upgrade.
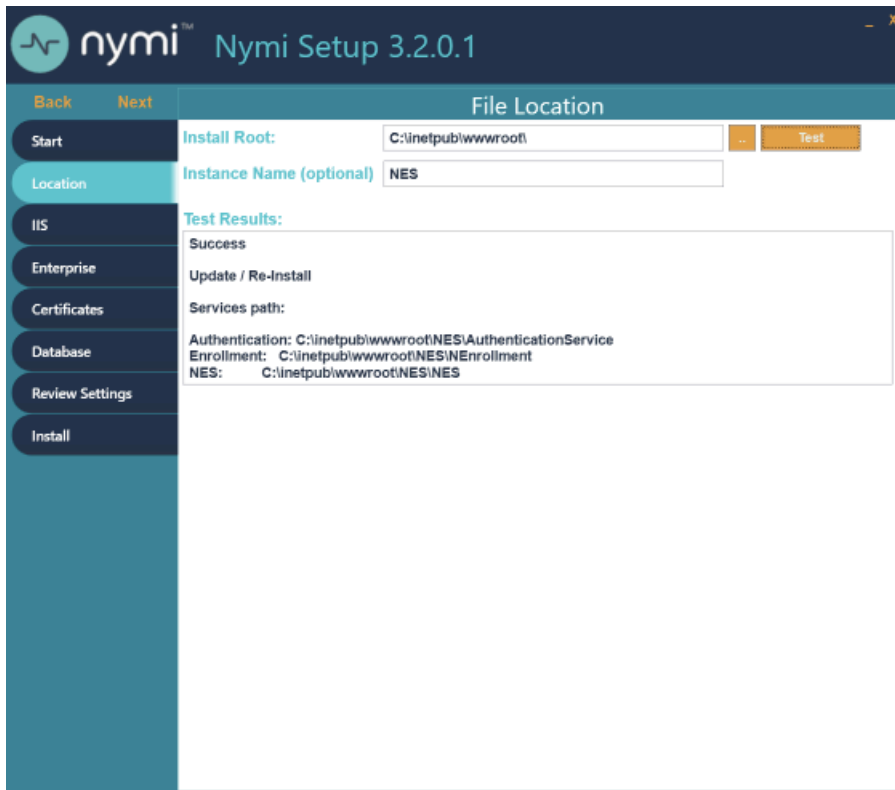
Figure 70: Update / Reinstall installation type

10. On the **Database** page, click right-click in the Users table and select **Add**.

The `Database Credentials Editor` window appears.

11. From the **Login Type** list, select **Auditor**.

12. In the **Domain Account** field, type the domain and username (or group name) of the user in the format *domain_name\user_name.*

13. In the **Database User** field, type the name of the SQL user to associate with the user or group.

14. Click **OK**.

15. Click **Verify Users**.
If the NES installer finds the user or group in active directory, the message No errors found appears in the status window. If an error appears, right-click on the user or group in the **Database** table, and select **Edit** to correct the credential information.

16. On the **Install** tab, click **Apply Settings**.
The output displays Creating Database Auditor Login is done.

14.1.2 - NES SQL Database Overview

Connected Worker Platform records configuration information about the Connected Worker Platform components in the NES database. When configuration changes are made, the system records information in the appropriate SQL tables.

The NES database name is Nymi.*instance_name*, where *instance_name* is the instance name that was specified in the NES Setup wizard. For example, Nymi.NES. If an instance name was not specified, the default database name is Nymi.NESg2.admin.

The NES SQL database contains several schemas that are named and grouped according to the type of stored data.

Date and time values appear in UTC (Coordinated Universal Time) timezone.

The following figure shows the structure of the NES database, including the relationship between each schema, the primary keys, and foreign keys.
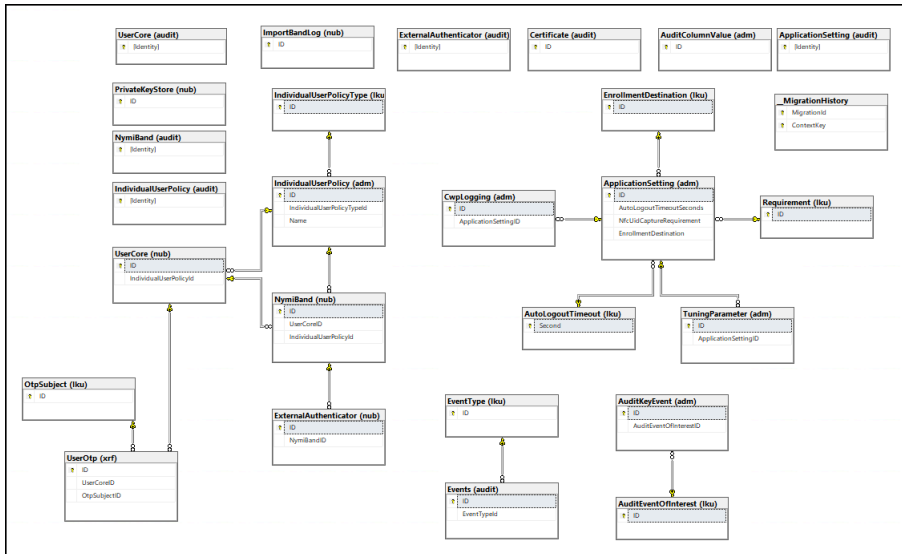
Figure 71: NES Database Structure

adm and nub Schemas

Transactional tables that contain the current record of the information for each Connected Worker Platform component.

Table 8: adm and nub Schemas

Table Name	Purpose
adm.ApplicationSettings	Contains a entry for each NES policy and the values that are currently assigned to each settings in the policy.
adm.AuditColumnValue	Legacy table.
adm.AuditKeyEvent	Legacy table.
nub.ExternalAuthenticator	Contains an entry for Nymi Band that contains an external authenticator.
nub.NymiBand	Contains current information about each Nymi Band that has been enrolled on the NES server.
nub.PrivateKeyStore	Contains a entry for each private key that is stored in the Microsoft keystore.
nub.UserCore	Contains an entry for each user and the current value of each user property.
nub.UserOtp	Contains a entry for each private key that is stored in the Microsoft keystore.

dbo.__MigrationHistory

Transactional table that stores information about SQL database migrations that occur during an NES upgrade.

Iku Schema

Lookup tables that contain a list of acceptable values settings that appear in the adm.ApplicationSettings table, and are selected by an NES Administrator in the properties page of the policy in the NES Administrator Console.

Table 9: Iku schema

Table Name	Purpose
Iku.AuditEventsOfInterest	Legacy option.
Iku.EnrollmentDestination	Contains a list of acceptable values for the **Enrollment Destintation** setting.
Iku.OtpSubject	Legacy option.
Iku.Requirement	Contains a list of acceptable values for the **NfcUIDCapture** setting.
Iku.AuditLogoutTimeout	Contains a list of acceptable values for the **Auto Logout Timeout** setting.
Iku.EventType	Contains a list of acceptable values for events.

xrf.UserOtp Schema

Legacy transactional table that contains information about each OTP that is created for a user.

audit Schemas

Log tables that record each event that occurs as a result of a change in a transaction table. The audit schemas contain the same columns as each corresponding transactional table as well as 4 additional columns that identify the time of the event, the type of event, the system user, and the schema entry identifier. Stores information about changes (creation, updates and deletions) that result in changes to the nub and adm table objects. These changes are tracked as events. There is one row for each event type and a single change can results in several recorded events types. Accessing the data in the audit tables enables users to gather useful information for audit and compliance purposes. The following sections provide detailed information about the contents of each audit table.

audit.Events SQL Schema

This table contains enrollment information that pertains to NES users. Each attribute name that is listed in the Column Name is prefaced with Identity. For example, identity.EventTime.

Table 10: audit.Events SQL Schema

Column Name	Description
EventTypeID	ID that denotes the type of event. There are several types of events: • 1—The Nymi Band used to perform the first tap during the enrollment process is not the same Nymi Band that was used to perform the second tap during the enrollment process. • 2—The username or password that was provided to log into the Nymi Band Application was not correct. • 3—Enrollment completed. • 4—The Nymi Band that the user used to perform the tap operation is assigned to a different user. • 5—The False Acceptance Rate value of 1:50000K was applied to the Nymi Band of the user. • 6—Presence Authentication Code (PAC) Verification Failed for the Nymi Band of the user. • 7—PAC verification succeeded but the Nymi Band has lost track of time. • 8—The system encountered an error during PAC verification. • 9—PAC verification initialization failed as a result of a bad request. • 10—PAC verification initialization failed because the advertising key was not found. • 11—Could not generate the advertising key because of an internal server error. • 12—Could not generate the advertising key because the CMAC that was supplied does not match the CMAC that was created. • 13—PAC verification succeeded • 14—Time on the Nymi Band is out of bounds with the time on the NES server. • 15—Time on the Nymi Band Application is out of bounds with the time on the NES server. • 16—Re-enrollment attempt failed because the SEOS-enabled Nymi Band is assigned to a different user. • 17—Re-enrollment attempt failed because the Nymi Band is assigned to a different user and the policy settings only allow re-enrollment to the same Nymi Band. • 18—Re-enrollment attempt to the Nymi Band of a different user succeeded. • 19—Re-enrollment attempt by a user for their own Nymi Bandsucceeded. • 21—Re-enrollment attempt failed because the Nymi Band is assigned to a different user and the NES policy settings only allow re-enrollment to the same Nymi Band. • 22—Re-enrollment attempt failed for the because NES policy does not allow re-enrollment.

Column Name	Description
EventTypeID (continued)	• 23—Nymi Band registration attempt succeeded. • 24—Nymi Band registration attempt failed.
UserCoreID	ID of the user that is associated with the Nymi Band, as it appears in the audit.UserCore table. When an NES Administrator disassociates a Nymi Band from a user in the NES Administrator Console, the UserCoreId value is as NULL for the associated Update and Delete Event Type entries in the table.
Username	Active Directory account that logged in to the Nymi Band Application to perform the enrollment.
InitialTapNymiBandId	The NFC UID for the first Nymi Band tap in the Nymi Band Application.
ConfirmTapNymiBandId	The NFC UID for the second Nymi Band tap in the Nymi Band Application.
CreatedAt	Date and time that the object entry was created in the table.
ModifiedAt	Date and time that the object entry was modified in the table.
ModifiedBy	User account that modified the object entry in the table. For example, when the user performs an enrollment, the AD user account for the user appears.
DisconnectUserCoreId	The ID of the previously assigned Nymi Band user.
HardwareID	The serial number of the Nymi Band.

audit.UserCore SQL Schema

This table contains information that pertains to NES users. Each attribute name that is listed in the Column Name is prefaced with Identity. For example, identity.EventTime.

Table 11: audit.UserCore SQL Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.
EventType	Type of event, denoted by a single character. There are three event types: • C—when the user is enrolled or for an unenrolled user, the first time that an NES Administrator performs a search for the user in the NES Administrator Console. • U—when the properties of the user is updated.

Column Name	Description
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	ID of the user in the audit.UserCore table.
Domain	Domain of the user.
Username	Login name of the user.
MiscNote	Displays the value that appears in the **Notes** field in the properties of the user account. Values that can appear: • NULL when the **Notes** field is empty. For example, when the user entry was initially created in the database as a result of an enrollment, or when an NES ADminsitrator removes the text that appears in the **Notes** field. • Text specified by the NES Administrator in the **Notes** field for the properties of the Nymi Band in the NES Administrator Console. • The value **Created from an AD search result**, which is the text that appears in the **Notes** field when the user entry is created in the database as a results of an NES Administrator searching for a user in the NES Administrator Console for which a Nymi Band enrollment has never occurred.
CreatedAt	Date and time that the object entry was created in the table.
ModifiedAt	Date and time that the object entry was modified in the table.
ModifiedBy	User account that modified the object entry in the table. For example, when the user performs an enrollment, the AD user account for the user appears. When an NES Administrator modifies the **Notes** field for the properties of the user in the NES Administrator Console, then the AD user account for the NES Administrator appears.

`audit.NymiBand SQL Schema`

This table contains audit log data pertaining to Nymi Band events. Each attribute name that is listed in the Column Name is prefaced with Identity.

Table 12: audit.NymiBand SQL Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.

Column Name	Description
EventType	Type of event, denoted by a single character. There are three event types: • C—when the Nymi Band is enrolled. • U—when the properties of the Nymi Band is updated. • D—when the Nymi Band to user association is deleted.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	ID of the Nymi Band in the audit.NymiBand table.
UserCoreId	ID of the user that is associated with the Nymi Band, as it appears in the audit.UserCore table. When an NES Administrator disassociates a Nymi Band from a user in the NES Administrator Console, the UserCoreId value is as NULL for the associated Update and Delete Event Type entries in the table.
NymiBandID	MAC address of the Nymi Band. The NymiBandID is randomly generated at the time of enrollment, and changes on re-enrollment.
NfcUID	NFC address of the Nymi Band.
AuthorisationID	N/A. The value appears as NULL.
HardwareID	Nymi Band serial number.
SymmetricKeyID	SymmetricKey ID that was created on the Nymi Band. Values that can appear: • An encrypted key sequence when **Corporate Credentials Authenticator** is enabled in the policy or the **Enrollment Destination** is set to **NES and Evidian**. • NULL when in the policy the **Corporate Credentials Authenticator** is not enabled and the **Enrollment Destination** value is **NES only** at the time of enrollment.
EncryptionIV	Encryption Initialization Vector that is used to support encrypting the password for a user. A value appears in this field when the Nymi Lock Control option is enabled in the default policy at the time that user enrolled the Nymi Band.
EncryptedPassword	Encrypted password for a user. A value appears in this field when the Nymi Lock Control option is enabled in the default policy at the time that the user enrolled the Nymi Band.

Column Name	Description
IsActive	Status of the Nymi Band as set in the NES Administrator Console. Values that can appear: • 0 when the Nymi Band inactive. • 1 when the Nymi Band is active.
IsPrimary	Status of the Nymi Band as set in the NES Administrator Console. Values that can appear: • 0 when the Nymi Band not the primary Nymi Band. • 1 when the Nymi Band is primary.
HasFingerprint	Status of the fingerprint enrollment for the Nymi Band. Values that can appear: • 0 when a fingerprint enrollment has completed. • 1 when a fingerprint enrollment has not been completed.
EnrollmentStatus	N/A. The value appears as NULL.
MiscNote	Displays the value that appears in the **Notes** field in the properties of the Nymi Band.
BandSubordinateCaCert	N/A. The value appears as NULL.
BandCert	N/A. The value appears as NULL.
UserCert	N/A. The value appears as NULL.
BandLabel	The Band Label name given to the Nymi Band during enrollment, when the **Display Band Label on Nymi Bands** option is enabled. The value is NULL when the **Display Band Label on Nymi Bands** option was disabled at the time of enrollment.
FirmwareVersion	Firmware version on the Nymi Band at time of enrollment.
CreatedAt	Date and time that the object entry was created in the table.
ModifiedAt	Date and time when the object entry was modified in the table.
ModifiedBy	The user who modified the object.
EvidianEnrollmentCompleted	Status of the enrollment of Nymi Band on an Evidian EAM Controller. Values that can appear: • 0 when enrollment completed. • 1 when enrollment did not complete or occur.

Column Name	Description
IsSynced	Status of application of the latest individual user policy settings to the associate user. Values that can appear: • 0 when the properties of a user do not include changes in the settings of an applicable individual user policy. The user must log into the Nymi Band Application while wearing their authenticated Nymi Band to receive updated individual policy settings. • 1 when the properties of a user includes the current settings of an applicable individual user policy.
IndividualUserPolicyId	ID of the individual user policy that is assigned to the user or NULL if the user does not have an assigned individual user policy.
SeosId	SEOS ID of the Nymi Band, which Nymi assigns to the Nymi Band during the manufacturing process or NULL if the Nymi Band is not SEOS-enabled.
StaticMacAddress	Default Nymi Band ID, which Nymi assigns to the Nymi Band during manufacturing.
TSetTime	Time when the Nymi Band Application performed the set_time operation on the Nymi Band, during the enrollment process or when the user logged into the Nymi Band Application. Authenticated Bluetooth taps use this time during the process of validating the user that is associated with the Nymi Band.
IsBandEnrolledHere	Status of the Nymi Band enrollment on this NES. Values that can appear: • 0—The user completed the Nymi Band enrollment on another NES and registered the Nymi Band on this NES. • 1—The user completed the Nymi Band enrollment on this NES.

audit.ApplicationsSetting SQL Schema

This table contains audit log data pertaining to NES application settings that are defined in the each NES policy. Each attribute name that is listed in the Column Name is prefaced with Identity.

Table 13: audit.ApplicationsSetting SQL Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.

Column Name	Description
EventType	Type of event, denoted by a single character. There are three event types: • C—when a new policy is created or change to an existing policy is created. • U—when a setting in a policy is modified. • D—when a policy is deleted.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	The database ID of application settings on audit.ApplicationSettings table.
IsActive	Status of the policy as set in the NES Administrator Console. Values that can appear: • 0 when the policy is not the active policy. • 1 when the policy is the active policy.
Description	Name of the policy that contains the setting.
AutoLogoutTimeoutSeconds	Length of time after which the Nymi Band Application automatically disconnects an idle user.
NfcUIDCaptureRequirement	Status of the requirement to capture the NFC UID of the Nymi Band during enrollment. The value is always M (Mandatory).
FingerprintRequirement	Legacy option that defines the status of the requirement to capture the fingerprint of the user during enrollment. The value is always M (Mandatory).
PassworthAuthOption	Status of the option to allow authentication by corporate credentials. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
FingerprintOption	Legacy option that defines the status of the fingerprint capture option. The value is always 1 (enabled).
LockControlSupportOption	Status of the option to allow Nymi Lock Control. Values that can appear: • 0—when the setting is disabled. • 1—when the setting is enabled.
DoorSecurityOption	N/A
AdCheckUserStatus	Status of the Check User Status setting. Values that can appear: • 0—when the setting is disabled. • 1—when the setting is enabled.

Column Name	Description
AdCacheUserStatus	Status of the **Cache User Status** setting. Values that can appear: • 0—when the setting is disabled. • 1—when the setting is enabled.
AdCacheExpiryTimeSeconds	Expiry time of user status cache in seconds. When the **Cache User Status** setting is disabled, NULL appears.
ManualOtpOption	Legacy option.
ManualNeaOtpOption	Legacy option.
LockWhenAway	Status of the **Lock When Away** setting for Nymi Lock Control. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
MonitorProximity	Legacy option.
KeepUnlockedWhenPresent	Status of the **Keep Unlocked When Present** setting for Nymi Lock Control. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
CheckProximityForUnlock	Legacy option.
LockProximitySphera	Proximity distance for Nymi Lock Control that is defined in the adm.ApplicationSettings table. Nymi recommends that you leave the default value of 3.
UnlockProximitySphera	Proximity distance for Nymi Lock Control that is defined in the adm.ApplicationSettings table. Nymi recommends that you leave the default value of 2.
ProximityLockCountdown	Starting time for the countdown timer in seconds, that Nymi Lock Control displays to the user when the Nymi Band moves out of close proximity to the Bluetooth adapter.
BandLabelOnBandEnabled	Status of the **Display Band Label on Nymi Bands** setting. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
BandLabelOnBandCustomizationEnabled	Status of the **Allow Band Label Customization** setting. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
CreatedAt	Date and time that the object entry was created in the table.

Column Name	Description
ModifiedAt	Date and time when the object entry was modified in the table.
ModifiedBy	User who modified the object entry in the table.
EnrollmentDestination	Status of the **Enrollment Destination** setting. Values that can appear: • 1 when enrollment data is sent to NES only. • 2 when enrollment data is sent to NES and Evidian.
SDCTEnabled	Legacy option.
SDRemindersEnabled	Legacy option.
UnlockWhenPresent	Status of the **Unlock When Present** setting for Nymi Lock Control. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
LivenessDetectionEnabled	Status of the **LivenessDetectionEnabled** setting. Values that can appear: • NULL when the setting was not available at the time that the entry was created. • 0 when the setting is disabled. • 1 when the setting is enabled.
HealthAttestation	Legacy option.
TemperatureReporting	Legacy option.
SeosTimeout	Legacy option.
HapticFeedbackOnBandEnabled	Status of the **HapticFeedbackonBandEnabled** setting. Values that can appear: • NULL when the setting was not available at the time that the entry was created. • 0 when the setting is disabled. • 1 when the setting is enabled.
FAR	Status of the **FAR** setting. Values that can appear: • 0 when the setting is 1:20,000 (default). • 1 when the setting is 1:50,000.
TInterval	Used for authenticated Bluetooth tap operations. The time interval for PAC message rotation. Default: 1 second

Column Name	Description
DmNBANESTime	Used for authenticated Bluetooth tap operations. Midpoint time difference between the Nymi Band Application and NES. For a domain-joined enrollment terminal this time is the estimated time accuracy inherent in the Network Time Protocol (NTP, IETF RFC 1305) used by Windows to synchronize time between computers.
DvNBANESTime	Used for authenticated Bluetooth tap operations. Variation time difference between the Nymi Band Application and NES. For a domain-joined enrollment terminal this time is the estimated time accuracy inherent in the Network Time Protocol (NTP, IETF RFC 1305) used by Windows to synchronize time between computers.
DmNBANBTime	Used during PAC verification for authenticated Bluetooth tap operations. Midpoint time difference between the Nymi Band and the Nymi Band Application, which results from the inherent delay in sending the set_time message to the Nymi Band.
DvNBANBTime	Used during PAC verification for authenticated Bluetooth tap operations. Variation time difference between the Nymi Band and the Nymi Band Application, which results from the inherent delay in sending the set_time message to the Nymi Band.
DmClockDrift	Used during PAC verification for authenticated Bluetooth tap operations. Clock drift value for the Nymi Band.
DvClockDrift	Used during PAC verification for authenticated Bluetooth tap operations. Clock drift value for the Nymi Band.
DmIntent	Intent delay time that is applied to PAC verification activities for authenticated Bluetooth tap operations.
DvIntent	Intent delay time that is applied to PAC verification activities for authenticated Bluetooth tap operations.
AllowReEnrollment	Status of the **AllowReEnrollment** setting. Values that can appear: • 0 when the user cannot perform re-enrollment of their Nymi Band until an CWP Administrator disassociates the Nymi Band for the user. • 1 when the user can perform re-enrollment of their Nymi Band without the need for the CWP Administrator to first disassociate the Nymi Band for the user.

Column Name	Description
AllowReenrollementOfActiveNymiBand	Status of the `AllowReenrollementOfActiveNymiBand` setting. Values that can appear: • 0 when the user cannot perform an enrollment of a Nymi Band that is associated with another user until an CWP Administrator disassociates the Nymi Band for the user. • 1 when the user can perform an enrollment of a Nymi Band that is associated with another user without the need for the CWP Administrator to first disassociate the Nymi Band for the user.

`audit.ExternalAuthenticator SQL Schema`

This table contains audit log data pertaining to external user authentication events. Each attribute name that is listed in the Column Name is prefaced with Identity.

Table 14: audit.ExternalAuthenticator SQL Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.
EventType	Type of event, denoted by a single character. There are three event types: • C—when the external authenticator is created on the Nymi Band. • U—when the properties of external authenticator on the Nymi Band is updated. • D—when external authenticator is deleted on the Nymi Band.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	ID of the object entry in the audit.ExternalAuthenticator table.
PublicKey	Base-64 pem encoded public key on the Nymi Band.
BandExternalAuthenticatorid	ID of the external authenticator.
NymiBandId	ID of the associated Nymi Band in the audit.NymiBand table.

Column Name	Description
Name	Name of the application that created the External Authenticator. Values that can appear: • NEM—Nymi Band Application, when the **Corporate Credentials Authenticator** setting is enabled in the policy and the **Enrollment Destination** setting is set to **NES only**. • Evidian—EAM controller when the **Enrollment Destination** setting is set to **NES and Evidian**.
MiscNote	Additional information.
CreatedAt	Date and time that the object entry was created in the table.
PrivateKeyWO	N/A.
PrivateKeyStoreID	UUID and the key ID of the private key in the Microsoft keystore.
HapticFeedbackonBandEnabled	Status of the **HapticFeedbackonBandEnabled** setting. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
ModifiedAt	Date and time when the object was modified.
ModifiedBy	The user who modified the object, which is the account that was logged into the Nymi Band Application at the time the external authenticator was created or removed on the Nymi Band.

audit.Certificate SQL Schema

Stores information about all the NEA certificate creation events, when a certificate is issued to the Nymi Band Application and all other NEAs. Each attribute name that is listed in the Column Name is prefaced with Identity.

Table 15: audit.Certificate SQL Schema

Column Name	Description
ID	Unique identifier for the schema entry.
NotBefore	Date before which the certificate is not valid.
NotAfter	Date after which the certificate is not valid.
SerialNumber	Serial number of the certificate.
RequesterTime	Date and time that the application requested the certificate.
RequesterDomain	Domain of the user that was logged into the application at the time of the certificate request.

Column Name	Description
RequesterUserName	User name of the user that was logged into the application at the time of the certificate request.
RequesterIp	IP address of the machine from which the request originated.

`audit.IndividualUserPolicy Schema`

Stores information about all the configured individual user policies. Each attribute name that is listed in the Column Name is prefaced with Identity.

Table 16: audit.IndividualUserPolicy Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.
EventType	Type of event, denoted by a single character. There are three event types: • C—when the external authenticator is created on the Nymi Band. • U—when the properties of external authenticator on the Nymi Band is updated. • D—when external authenticator is deleted on the Nymi Band.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	ID of the object entry in the audit.ExternalAuthenticator table.
IndividualUserPolicyTypeID	ID that denotes the type of the Individual User Policy. There are two types: • 1—Predefined user policy • 2-User—created user policy.
Name	Name that the policy creator assigned to the individual policy.
Note	Text that appears in the **`Note`** field for the individual policy.
LivenessDetectionEnabled	Status of the **`LivenessDetectionEnabled`** setting. Values that can appear: • NULL when the setting was not available at the time that the entry was created. • 0 when the setting is disabled. • 1 when the setting is enabled.

Column Name	Description
PassworthAuthOption	Status of the option to allow authentication by corporate credentials. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
CreatedAt	Date and time that the object entry was created in the table.
ModifiedAt	Date and time when the object was modified.
ModifiedBy	The user who modified the object, which is the account that was logged into the Nymi Band Application at the time the external authenticator was created or removed on the Nymi Band.
HapticFeedbackonBandEnabled	Status of the **HapticFeedbackonBandEnabled** setting. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
FAR	Status of the **FAR** setting. Values that can appear: • 0 when the setting is 1:20,000 (default). • 1 when the setting is 1:50,000.
AllowReEnrollment	Status of the **AllowReEnrollment** setting. Values that can appear: • 0 when the user cannot perform re-enrollment of their Nymi Band until an CWP Administrator disassociates the Nymi Band for the user. • 1 when the user can perform re-enrollment of their Nymi Band without the need for the CWP Administrator to first disassociate the Nymi Band for the user.
AllowReenrollementOfActiveNymiBand	Status of the **AllowReenrollementOfActiveNymiBand** setting. Values that can appear: • 0 when the user cannot perform an enrollment of a Nymi Band that is associated with another user until an CWP Administrator disassociates the Nymi Band for the user. • 1 when the user can perform an enrollment of a Nymi Band that is associated with another user without the need for the CWP Administrator to first disassociate the Nymi Band for the user.

14.1.3 - Viewing and Querying Audit Schema

Users with read access to the NES SQL database can view and query audit information by using a SQL querying tool such as SSMS or a custom-built application that is capable of running T-SQL queries.

About this task

Perform the following steps to use SSMS to view the entries in an audit schema.

Procedure

1. Open SSMS and connect to the SQL server.
2. In the `Object Explorer`, navigate to your server, and open **Databases**.
3. Locate the database instance Nymi.*instance_name*.
4. Right-click the audit schema that you want to view, and then select **Select Top 1000 Rows**.
   A results window appears that displays the values for the most recent 1000 schema entries in a table.

Tracing changes in the audit tables

You can verify that the audit log table is populating with the latest values by following these steps:

1. Enroll a Nymi Band. In the audit.NymiBand table, a series of update and create records are logged.
2. In the NES Administrator Console, edit the properties of the Nymi Band, add a note, and then click **Save**.
3. In SSMS view the Nymi.*instance_name*.audit.NymiBand table, confirm that an update entry appears, and that the **MiscNote** column displays the new note.
4. In the NES Administrator Console, edit the properties of the Nymi Band. Do not make any changes and then click **Save**.
5. In SSMS view the Nymi.*instance_name*.audit.NymiBand table and confirm that an update entry does not appear.
6. In the NES Administrator Console, edit the properties of the Nymi Band, remove the note, and then click **Save**.
7. In SSMS view the Nymi.*instance_name*.audit.NymiBand table, confirm that an update entry appears, and that the **MiscNote** column displays NULL.

14.1.4 - Performing More Complex Queries of the Audit Tables

The Audit Logs contain data for all create, update, delete events that are related to users, Nymi Bands, certificates, application settings, and the external authenticator.

Overview of SQL queries

The following provides you with a high level overview of the steps to follow to build more complex queries that gather information that is contained in multiple schemas in the Nymi.*instance_name* database when a table contains a foreign key that is linked to the primary key of another table.

1. Define a SELECT statement then list the subsequent table columns data values that the query retrieves.
2. Add a FROM clause to define the primary table from which to retrieve the column data values, and use an AS statement renames the table.
3. Add a JOIN clause to define the table that contains column value data that is related to the primary table, and the AS statement renames the table.
4. Specify an ON clause to define the conditions of JOIN clause.
5. Add an WHERE clause that defines a filter for the results.

Querying for the database to gather information about enrollments and the Nymi Band to user relationship

The Nymi.**instance_name**.audit.UserCore schema contains information that is specific the users in the CWP environment. The Nymi.**instance_name**.audit.NymiBand schema contains information that is specific to the Nymi Bands in the CWP environment

These two schemas share the a common UserID value, which allows you to generate results that provide details about a user and their associated Nymi Band.

To retrieve information from the Nymi.**instance_name**.audit.UserCore and Nymi.**instance**.audit.NymiBand tables and display information about the last 1000 enrollments, perform the following steps.

Note: In the following example, the NES instance name is NES.

1. Open `SSMS` and connect to the SQL server.
2. On the Toolbar, click `New Query`.
3. In the `SQL Query` window, type the following SQL query command.

```
SELECT TOP (1000)
nb.[Identity]
,nb.[EventTime]
,nb.[EventType]
,nb.[SystemUser]
,nb.[ID]
,nb.[UserCoreID]
,nb.[NymiBandID]
,nb.[NfcUID]
,nb.[IsActive]
,nb.[IsPrimary]
,nb.[HasFingerprint]
,nb.[EnrollmentStatus]
,nb.[MiscNote]
,nb.[CreatedAt]
,uc.Domain
```

```
,uc.Username
FROM [Nymi.NES].[audit].[NymiBand] AS nb
JOIN [Nymi.NES].[audit].[UserCore] AS uc
ON nb.UserCoreID = uc.ID
WHERE nb.EventType = 'C'
```

In this query:

a. **SELECT** statement returns the first 1000 rows and the subsequent table columns define the table columns data values that the query retrieves.

b. **FROM** clause defines [Nymi.NES].[audit].[NymiBand] as the primary table from which to retrieve the column data values, and shortens the table name to nb.

c. **JOIN** clause defines [Nymi.NES].[audit].[UserCore] as the table that contains column value data that is related to the primary table, and shortens the table name to uc.

d. **ON** clause defines the primary key of the Nymi.NES.audit.NymiBand table. and the foreign key of Nymi.NES.audit.UserCore table.

e. **WHERE** clause specifies that only Create (C) rows and the associated data values appear in the query results.

4. On the Toolbar, click **Execute**.

The Nymi Support Knowledge Base provides more information about creating and running complex SQL database queries.

15 - Log Files

NES, the Nymi Band, and the Nymi Band Application write information to log files, which enables you to monitor and troubleshoot issues that you might encounter with the Connected Worker Platform components. Log files from the Nymi Band may also be required for troubleshooting issues with your Nymi Solution Consultant.

15.1 - Enrollment Terminal Log Files

Use the Menu option in the Nymi Band Application to save or view the log files.

15.1.1 - Saving Nymi Band Application log files

Perform the following actions to save a zip file of the log files.

About this task

Procedure

1. In the Nymi Band Application, from the navigation bar, select `Logs > Save Log Files`.
   The `Save Log Files Save As` window appears.
2. From the `Folder` list, select a folder to save the files.
3. In the `File name` field, type a name for the zip file.
4. Click `Save`.

15.1.2 - Viewing Nymi Band Application log files

Perform the following actions to view the log files.

About this task

Procedure

1. In the Nymi Band Application, from the navigation bar, select `Logs > Explore Logs`.
   Windows Explorer opens and displays the content of the log files folder. The default path to the log files is *C:\users\username\AppData\Roaming\Nymi\NEM\Logs*.
2. Double-click the log file to open the contents in the default text editor. The Nymi Band Application logs information in two files:
   - *nem.log*—Contains information about the Nymi Band Application.
   - *nymi_api.log*—Contains information about the Nymi SDK.

15.2 - Windows User Terminal Log Files

Nymi Runtime is installed on the user terminals in the environment. The Nymi Runtime includes the Nymi Bluetooth Endpoint and Nymi Agent services.

- The Nymi Bluetooth Endpoint log file (*nymi_bluetooth_endpoint.log*) is located in *C:\Nymi \Bluetooth_Endpoint\logs* folder.
- The Nymi Agent log file (*nymi_agent.log*) is located in the *C:\Nymi\NymiAgent* folder.

In some configurations, for example, in RDP and Citrix Environments, the configuration uses a centralized Nymi Agent. In this configuration, the *nymi_bluetooth_endpoint.log* is on the user terminal and the *nymi_agent.log* file is located on remote machine, on which the Nymi Agent is installed.

To enable debug mode for the Nymi Runtime services, create a system environment variable named `NYMI_DEBUG` with a non-zero value, and then restart the Nymi services.

15.3 - Nymi Application Log files

iOS devices that access web-based Nymi-enabled ApplicationNEAs require the Nymi Application, which includes the Nymi Bluetooth Endpoint component of Nymi Runtime. The option to log Nymi Bluetooth Endpoint messages is enabled by default.

To access the log file, open the Nymi Application and touch the `Logs` icon in the upper right corner, as shown in the following figure.
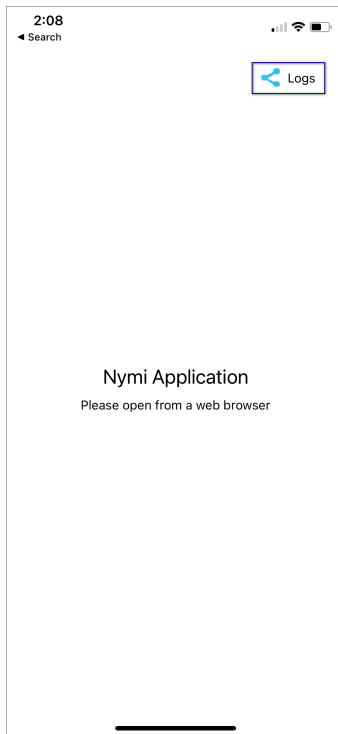
Figure 72: Nymi Application Logs

Note: If logging is disabled at the system level, the `Logs` icon does not appear.

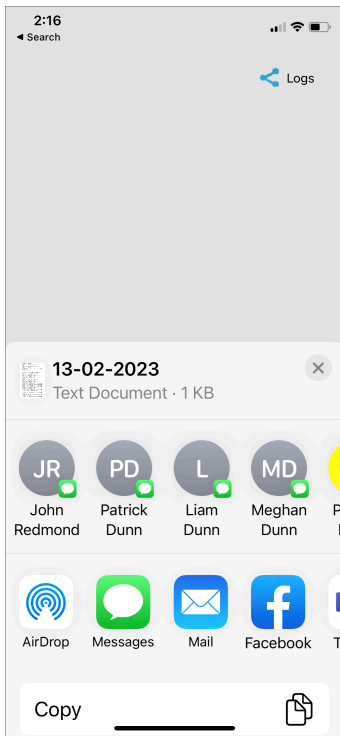On the file sharing options screen, select the method to share the file, for example, Air Drop or email.

Figure 73: Nymi Application Send Options

To disable logging, navigate to `Settings > Nymi`, and then toggle `Logs` to the off position, as shown in the following figure.
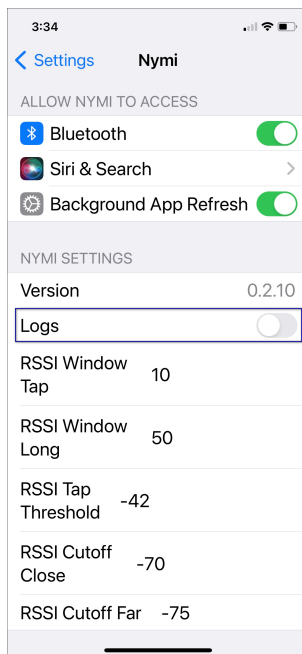
Figure 74: Disabling Nymi Application Logging

15.4 - Nymi Lock Control Log Files

Nymi Lock Control creates log files for security and troubleshooting purposes.

To enable debug mode for Nymi Lock Control , create a system environment variable named *NYMI_DEBUG* with a non-zero value, and then restart the Nymi services.

Security log

The *C:\Users\Public\AppData\Nymi\unlock\Log\credential-provider.log* file contains a record of the time and result of each authentication attempt on the user terminal.

Collecting log files and contacting support

To quickly create a zip file of the Nymi Lock Control log files that you can send to Nymi Support, perform the following steps:

1. Right-click the Nymi Lock Control icon on the system tray and select **Contact Nymi Support**.
2. On the `Include Logs?` window, click **Yes**.
3. On the `Nymi Support` page, log in with your Nymi Support account.
4. On the `Nymi Support` page, click `Submit a Request,` and then in the drop-down, select **Technical Issue**.
5. Fill in the appropriate details, and in the **Attachments** section, click **Add file**.

6. Navigate to the *C:\Users\[username]\AppData\Roaming\Nymi\unlock\ZipLog* folder, and then select the zip file.

15.5 - (CWP 1.18.0 and later) NES Log Files

NES has separate log files for each web service. When you encounter an issue, review the messages that appear in each log file.

15.5.1 - (CWP 1.18.0 and later) Changing NES Log Levels

By default, Nymi Enterprise Server (NES) logs all messages to the log files.

About this task

NES supports the following log levels:

Level	Description	Message levels included in the log file
OFF	Turns off logging completely. NES does not log messages, regardless of their severity level.	n/a
ALL	NES logs all messages including low level debug messages, regardless of their severity level.	• DEBUG • INFO • WARN • ERROR • FATAL
DEBUG	NES logs messages at the DEBUG level and higher. DEBUG messages provide detailed information for debugging and troubleshooting purposes.	• DEBUG • INFO • WARN • ERROR • FATAL
INFO	NES logs messages at the INFO level and higher. INFO messages provide general information about the operation and progress of the application.	• INFO • WARN • ERROR • FATAL

Level	Description	Message levels included in the log file
WARN	NES logs messages at the WARN level and higher. WARN messages indicate potential issues or unusual conditions that might require attention.	• WARN • ERROR • FATAL
ERROR	NES logs messages at the ERROR level and higher. ERROR messages indicate errors or exceptions that occur during the execution of the application.	• ERROR • FATAL
FATAL	NES logs messages at the FATAL level only. FATAL messages represent critical errors that cause the application to terminate or become unusable.	• FATAL

Note: Nymi recommends that you leave the level at the default level *ALL*

To change the logging level, perform the following steps:

Procedure

1. Edit the *C:\inetpub\wwwroot\nes_service_name\NESg2.Admin\web.config* file and in the <log4net> section, change the value for each *level value* parameter from to the required level.

   For example, to change from the default value *ALL* to *DEBUG*:

   ```
   <root>
      <level value="DEBUG" />
      <appender-ref ref="RollingLogFileAppender" />
   </root>
   <logger additivity="false" name="RollingLogFileAppender">
   <level value="DEBUG" />
    <appender-ref ref="RollingLogFileAppender" />
   </logger>
   ```

2. Edit the *C:\inetpub\wwwroot\nes_service_name\NEnrollment\web.config* file and in the <log4net> section, change the value for each *level value* parameter from **ALL** to **INFO**.

   For example, to change from the default value *ALL* to *INFO*:

   ```
   <root>
   <level value="INFO" />
      <appender-ref ref="RollingLogFileAppender" />
   </root>
   ```

```
<logger additivity="false" name="RollingLogFileAppender">
    <level value="INFO" />
    <appender-ref ref="RollingLogFileAppender" />
</logger>
```

3. Edit the *C:\inetpub\wwwroot\nes_service_name\AuthenticationService\web.config* file and in the <log4net> section, change the value for each *level value* parameter from **Information** to **Verbose**.

For example, to change from the default value *ALL* to *FATAL*:

```
<root>
    <level value="FATAL" />
    <appender-ref ref="RollingLogFileAppender" />
</root>
<logger additivity="false" name="RollingLogFileAppender">
    <level value="FATAL" />
    <appender-ref ref="RollingLogFileAppender" />
</logger>
```

4. Restart the IIS.

15.5.2 - NES Web Service Log File Locations

The NES log files are in the following locations, where `nes_service_name` is the Instance name selected during the NES installation:

- *C:\ProgramData\Nymi\NESg2.Admin\Default_Web_Site\nes_service_name\log*
- *C:\ProgramData\Nymi\NEnrollment\Default_Web_Site\nes_service_name_ES\log*
- *C:\ProgramData\Nymi\AuthenticationService\Default_Web_Site\nes_service_name_AS\log*

15.5.3 - Nymi Support Tool

The Nymi Support Tool enables you to collect log information and generate a zip file that Nymi can review for troubleshooting purposes. The following logs and information is collected: NES Installation log files, Windows event logs, NES log files and NES instance configuration files.

About this task

Follow these steps to generate a log zip file.

Procedure

1. On NES server, double-click *..*`nes_installation_folder`*\NesSystemInfo \NymiSupportTool.exe*.
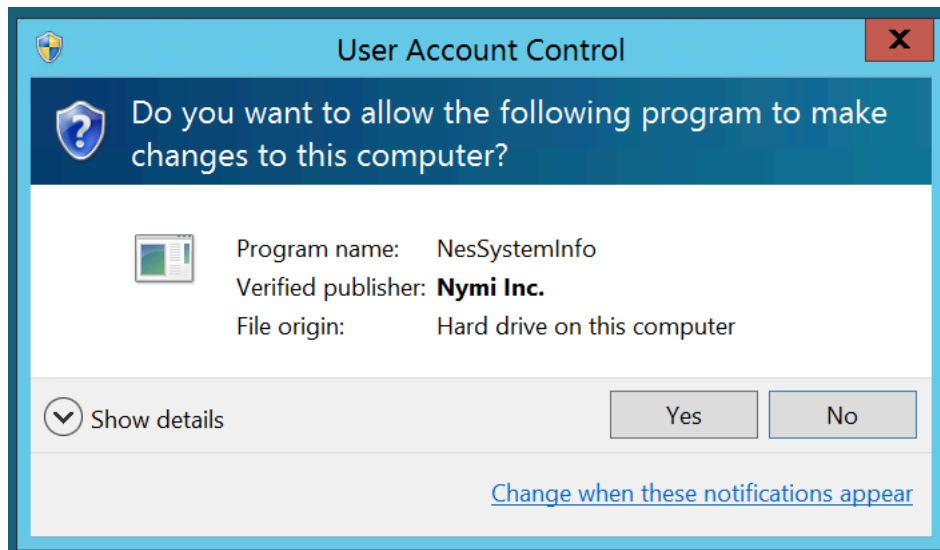The `User Account Control` dialog box appears.

Figure 75: The User Account Control

2. On the `User access control` window, click **`Yes`** to start the script.

3. On the **`Save As`** window, click **`Save`** to accept the default zip file name and location. By default the name of the zip file is the server hostname and the default directory is the *Documents* folder for the user running the command.
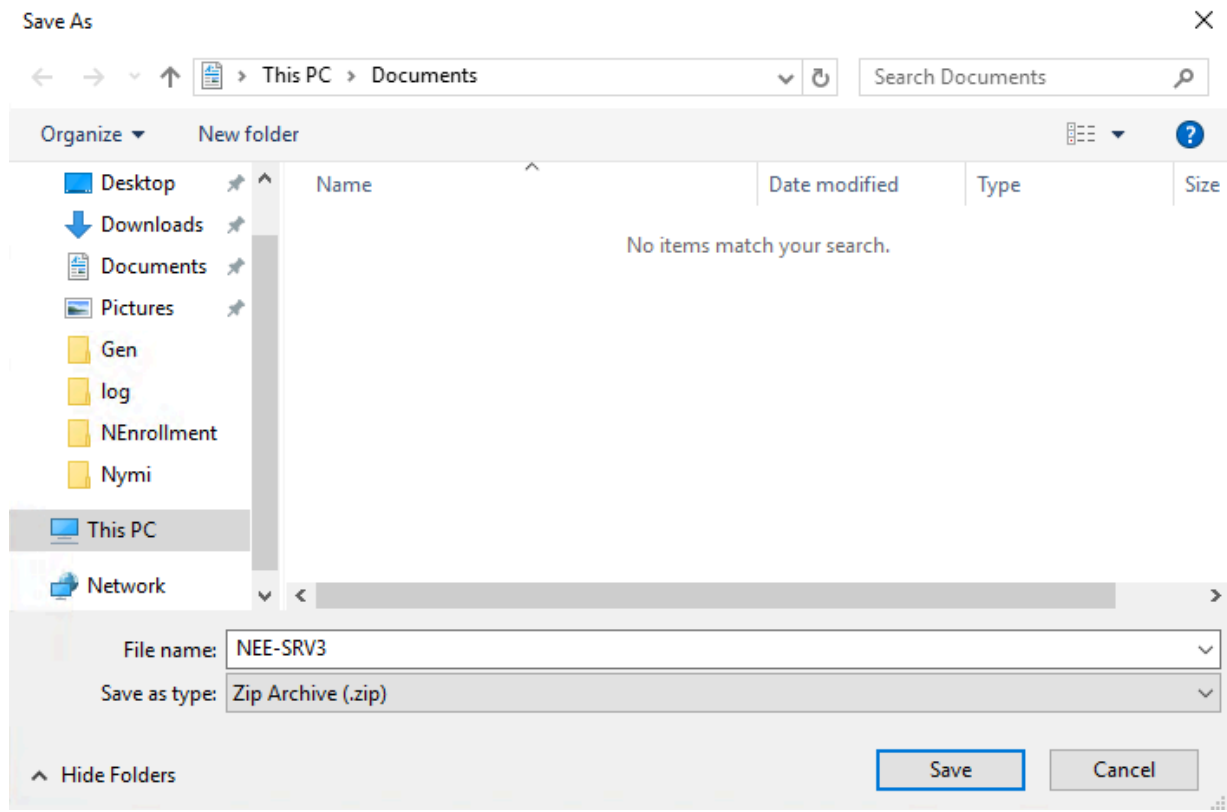
Figure 76: Saving Nymi Support Tool zip

Results

The zip file contains the following files and directory structure:

- *InstallLogs\NESg2.Installer* - Folder that contains the logs files that were created during the NES installation.
- *inetsrv\Config* - Folder that contains the *applicationHost.config*, which contains IIS configuration information.
- *NesInstances\nes_instance_name* - Folder that contains the IIS *web.config* files for the NES Authentication Service, Enrollment Service and Directory Service, and *info.txt* file that contains path and version information for each service..
- *EventLogs* - Folder that contains the Windows Event log files on the NES server.
- *SysInfo.txt* - File that contains information about the configuration of the NES server.
- *SupportTool.log* - Log file that contains the output of the *NymiSupportTool.exe* command.

15.6 - Firmware Log Files

The Nymi Solution Consultant may request logs from the Nymi Band to troubleshoot issues.

To retrieve log files from the Nymi Band, first plug the Bluetooth Adapter supplied by Nymi into the workstation and put the Nymi Band must be on the charger.

15.6.1 - Firmware Log Retrieval

About this task

To retrieve logs from the Nymi Band, perform the following steps:

Procedure

1. Place the Nymi Band on the charger and move the Nymi Band and charger close to the BLE radio antenna on the terminal (BLED112 adapter). This will ensure the logs are retrieved from the correct Nymi Band.
2. Download and extract the firmware package into a directory of your choice on a Windows computer. For example, *C:\Nymi_firmware*.
3. If the Windows machine has the Nymi Band Application installed on it, stop the Nymi Bluetooth Endpoint service.
4. Navigate to the *C:\nymi_firmware\build\exe.win32-2.7* directory.
5. Run the nsp_logs_download.exe. A command prompt window opens with the status of the log file download. When the download completes, the command window closes and the firmware log file is saved to the folder that contains the nsp_logs_download.exe file.

   Note: The log files from the Nymi Band are encrypted. Provide the log file to your Nymi Solution Consultant.

15.7 - Submitting a Support Request

You can submit a support request to Nymi from the NES Administrator Console.

About this task

Procedure

1. In the NES Administrator Console, click **Support**.
2. Click **Submit a ticket**.
3. In the **Subject** field, provide a short description of the issue and the name of your company.
4. From the **Submit a request list**, select the appropriate option for your issue, for example, Nymi Customers - Technical Support.
5. In the **Description** field, provide the details about the issue that you are seeing.
6. Optionally, attach the Nymi Band Application log files and NES support tool output.
7. Click **Submit**.

Note: For information on the NES support tool, refer to the Nymi Connected Worker Platform—Administration Guide for more information.

16 - Manage the Connected Worker Platform Environment

This section provides you with information about how to maintain and mange the Connected Worker Platform components.

16.1 - Manage NES

This section provides information about how to manage NES and Windows components that NES relies upon.

16.1.1 - Uninstalling the NES Installer Application

You can perform the following steps to remove the NES Installer software. This process is optional, but available to help with your cleanup activities.

About this task

Procedure

1. From `Control Panel > Programs > Programs and Features`, select `NES Installer`.
2. Click `Uninstall/Change`
3. On the `NES Maintenance` window, leave the default selection `Remove the application from this computer`, and then click `OK`.

16.1.2 - NES Backup and Recovery

Review this section for information about how to perform backups and recoveries of the NES host and NES database.

This section assumes that you:

- Deployed NES on a virtual machine
- The SQL instance resides on a server that differs from the NES server.
- Maintain the same FQDN and IP address for the NES virtual machine at the time of backup and the time of restore.
- Maintain the same FQDN and IP address for the SQL server virtual machine at the time of backup and the time of restore.

16.1.2.1 - NES Backups

To protect the Connected Worker Platform and certificate data on the NES machine, perform a backup of the NES virtual machine after you complete the initial installation and each time you change the NES or IIS configuration.

Use VMware vMotion or perform snapshots to backup the virtual machine.

16.1.2.2 - NES Database Backups

NES stores Nymi Band information, Nymi Band user information, and audit events securely in a SQL database named Nymi.*NES_service_name*, where *NES_service_name* is the NES service mapping name that you configured in the `NES Setup` wizard. For example, ***Nymi.nes***

Use your corporate backup and recovery software to back up the SQL database. The recovery point objective (RPO) determines the frequency of the NES database backup.

See Microsoft for more information about how to protect the SQL server.

16.1.2.3 - NES Server and Database Recoveries

Use your corporate backup and recovery software to restore the NES database on the SQL server and use VMware vMotion or snapshots to restore the virtual machine.

Note: You cannot recover the following data from a database restore:

- Any NES database changes, such as Nymi Band enrollments, Nymi Band re-enrollments, Nymi Band disassociations, and application policy changes that you perform after the last backup and prior to the failure.
- NES audit events that were recorded after the last backup and prior to the failure.

16.1.3 - Managing Database Logins

Manage the database logins using the Add, Edit and Delete buttons.

The **Database** page in the installation wizard enables you to configure settings that apply applied to the database. You can manage the Database Logins settings by adding, editing and deleting information.

16.1.3.1 - Adding Database Logins

The Database window enables you to configure settings that apply to the database. In the Connection String area, if the connection uses Integrated Security and the Security property is set to **True**, you can add Database Logins.

About this task

To add a new user perform the following steps:

Procedure

1. In an empty row of the `Manage Database Logins` table, right-click and select **Add**. The `Select User Credentials` window appears.

2. From the `Login Type` drop-down list, select Auditor or User.

   - Auditor – Provides the database user with read-only access to the database
   - User – Provide the database user with full control access to the database

3. In the `Domain Account` field, type the domain name followed by the user account or group account.

   Note: Ensure that a backslash separates the domain and account user or group.

4. In the `Database User` field, type the name of the database user.

5. Click **OK**.

6. On the Database page, click the `Verify Users` button to ensure that the new user is valid. The Database Login is added to the `Manage Database Logins` area. This Database Login is added to the SQL database when you are finished configuring the NES Setup Wizard. Proceed to the `Install` tab, and and press **Install** or **Upgrade**.

16.1.3.2 - Editing Database Logins

About this task

To edit a database login, perform the following steps:

Procedure

1. In the `Manage Database Logins` table, right-click and select **Edit**.
2. Modify the fields as required.

   Note: You cannot change the Login type for a service login account.

3. Click **OK**.

16.1.3.3 - Deleting Database Login

About this task

You can delete any Auditor login that you have added.

Procedure

1. In the `Manage Database Logins` area, click the row that you want to delete and right-click.
2. From the drop-down box, select **Delete**.
3. Enter **Delete**.
4. Click **OK** to confirm the deletion.
   The selected login is deleted.

16.1.4 - Adding and Removing NES Administrator Access

Access to the NES Administrator Console as an NES Administrator is defined through the addition and removal of user accounts in the Windows group that you specified during the configuration of the NES server.

Before you begin

To determine the Windows group that was defined during the NES deployment, edit the *C:\inetpub\wwwroot\nes_\WES\web.config* file and search for the `string name="AdminGroup"`. The value that appears between the value tags immediately after the string name is the Windows group name. Alternatively, log into the NES Administrator Console as an NES Administrator, click **About**, and then click **View Full System Diagnostics**, a list of the NES Administrator groups appear in the **Local Domain** section.

About this task

Perform the following steps to add or remove NES Administrator for a user.

Procedure

1. Log in to a domain controller as an administrator.
2. Edit the group.
3. Add or remove the users and groups, as required.
4. Save the group.

16.1.5 - Updating the Application Pool Identity Password

If you configured the Application Pool Identity to start with a specific user account, Nymi recommends that you use an account with a password that does not expire or change.

About this task

If policies in your organization require that the password for the user account expires, perform the following steps to update the password in IIS.

Procedure

1. Log in to NES server as an administrator and start `IIS Manager`.
2. In the left navigation pane, expand the server, and then select **Application Pools**, as shown in the following figure.
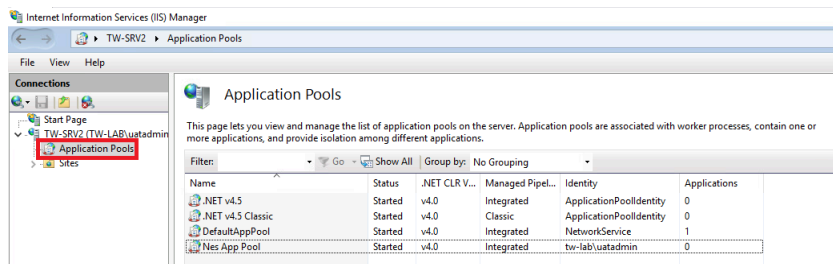
Figure 77: IIS Application Identity Pools

3. Select the NES application pool, the default name is NES App Pool.

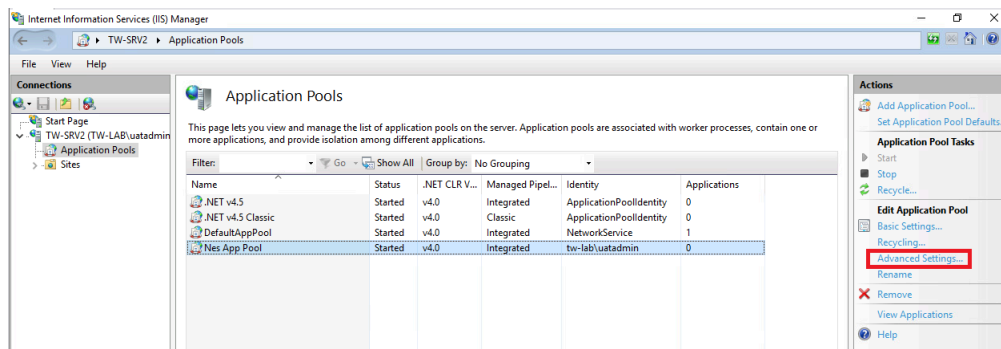**4.** From the `Actions` pane on the right of the window, click **`Advanced Settings`**

Figure 78: IIS Application Identity Advanced Settings

5. On the `Advanced Settings` window, select **`Identity`**, and then click the ellipses.
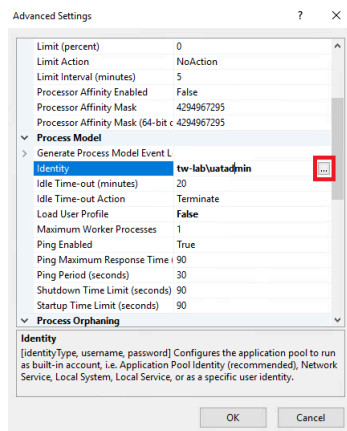

Figure 79: IIS Application Identity Advanced Settings

6. On the `Application Pool Identity` pop-up, click **`Set`**.

7. On the `Set Credentials` window, perform the following actions:

  a) In the **`Username`** field, type the username in the format `domain\username`

  b) In the **`Password`** and **`Confirm Password`**fields, type the new password.

  c) Click **`OK`**.

The following figure provides an example of the `Set Credentials` window.

Figure 80: Set Credentials window

16.2 - System Diagnostics

The NES Administrator Console contains a system diagnostics page that provides NES users and administrators with system information that can help resolve system configuration issues.

16.2.1 - Access the NES Administrator Console

Perform the following steps to connect to the NES Administrator Console and confirm the status of the system.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing ***https://nes_server/NES_service_name*** or ***http://nes_server/NES_service_name*** depending on the NES configuration, where:

- `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
- `NES_service_name` is the service mapping name for the NES web application. The default service mapping name is *nes*.

  For example, ***https://nes.cwp.company.com/nes***.

  Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console and require it during the CWP Backend deployment.

2. On the `Sign in` window, type the credentials of a user that is a member of the NES Administrators group, and then click **Sign In**.

3. On the main menu, click **About**.
   The `System Diagnostics` page appears.

4. Click **View Full System Diagnostics**.
   The NES server analyzes the status of dependencies and displays the results on the page. The following figure shows the various tests that are performed and the status. In this example, all tests passed and there was one warning the that L2 certificate will expire soon.
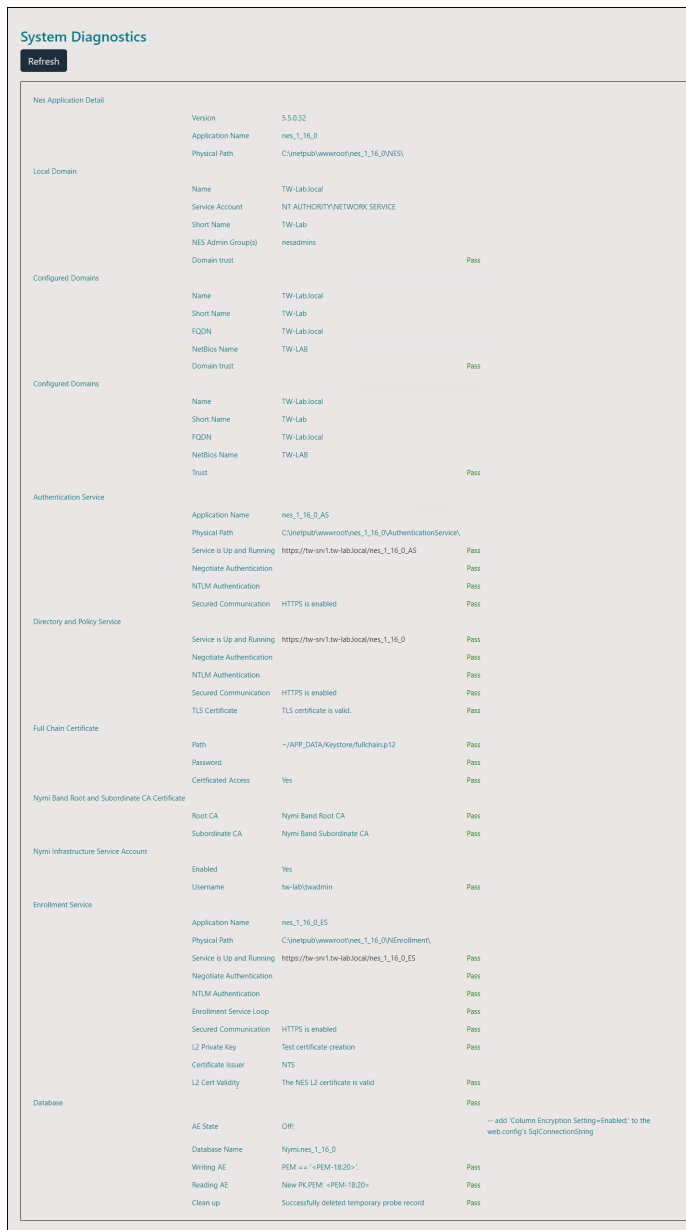
Figure 81: System Diagnostic Tests

5. Verify the username has administrative access by observing `Policies`, and `Search` in the main menu.

What to do next

The *Nymi Connected Worker Platform—Troubleshooting Guide* provides information about how to resolve issues that you might encounter when you run system diagnostics and attempt to access the NES Administrator Console.

16.2.2 - System Diagnostics Information

The system diagnostics runs a NES system diagnostic test and provides a snapshot of NES application information such as service availability, service failures and communication between NES services and hardware and software components.

Benefits

The system diagnostics page provides the following benefits:

- Summary information about the NES Application
- Failed services can be easily identified.
- Error codes help troubleshoot issues.
- Diagnostics helps on site troubleshooting.

NES System Diagnostics Information

To access the System Diagnostics information, log into the NES Administrator Console and click **About** in the main menu. Navigate to the **NES Administrator Console Diagnostic** page then click **View Full Diagnostics**.

The following information is displayed on the System Diagnostics page:

Table 17: NES Application Details

Service	Description
Version	Version of the NES Application.
Branch	The branch from which the build was created.
Application Name	The service names of the NES web application.
Physical Path	The physical path of the NES application

Table 18: Local Domain

This section of the system diagnostics page describes the domain where NES is running.

Service	Description
Name	The name of the local domain of the NES application.
Service Account	The name of the domain service account.
Short Name	The short name of the local domain.
Domain trust	Tests if the machine has a trusted relationship with the domain controller. Provides a Pass or Fail status indicator. A failed status requires domain trust to be reestablished between the machine and domain controller.

Table 19: Configured Domains

This section of the system diagnostics page describes domains that are configured in the NEnrollment web configuration file.

Service	Description
Name	The name of the domain account in the configuration file.
Short Name	The short name of the domain account in the configuration file.
FQDN	The fully qualified domain name under which the service is running configured in the configuration file.
NetBios Name	The NetBios name of the domain in the configuration file.
Trust	Tests if the NES machine has a trusted relationship with the domain controller. Provides a Pass or Fail status indicator. A failed status requires domain trust to be reestablished between the NES machine and domain controller.

Table 20: Authentication Service

This section of the system diagnostics page describes the status of the NES Authentication Service.

Service	Description
Service is Up and Running	Provides a link to system Authentication Service information page. Provides a Pass or Fail indicator.
Negotiate Authentication	Provides a Pass or Fail indicator.
NTLM Authentication	Provides a Pass or Fail indicator.
Secured Communication	Provides a Pass or Fail indicator.

Table 21: Directory and Policy Service

This section of the system diagnostics page describes the status of directory and policy services.

Service	Description
Service is Up and Running	Provides a link to NES Administrator Console page. Provides a Pass or Fail indicator.
Negotiate Authentication	Provides a Pass or Fail indicator.
NTLM Authentication	Provides a Pass or Fail indicator.
Secured Communication	Provides a Pass or Fail indicator.

Service	Description
TLS Certificate	Provides a Pass or Fail for the validity of the TLS certificate. Provides the expiry date (m,d,y) of the TLS certificate within three months of the expiration date.

Table 22: Enrollment Service

This section of the system diagnostics page describes the status of the Enrollment Service.

Service	Description
Service is Up and Running	Provides a link to NES Enrollment Service page. Provides a Pass or Fail indicator. Configure the Enrollment Service using the Policy option from the main menu.
Negotiate Authentication	Provides a Pass or Fail.
NTLM Authentication	Provides a Pass or Fail.
Enrollment Service Loop	Provides a Pass or Fail.
Secured Communication	Provides a Pass or Fail.
L2 Private Key	Tests the certificate creation. Indicates a Pass or Fail.
Certificate Issuer	Indicates if the certificate was issues by the Nymi Token Server.
L2 Cert Validity	Indicates if the certificate is valid. Provides the expiry date (m,d,y) of the NES L2 certificate.

Table 23: Database

Service	Description
AE State	Provides information about the always encrypted state of the SQL database.
Database Name	Provides the name of the NES database.
Writing AE	Provides a Pass or Fail indicator about the availability of the information writing always encrypted functionality. Indicates a Pass or Fail.
Reading AE	Provides a Pass or Fail indicator about the availability of the reading always encrypted functionality. Indicates a Pass or Fail.
Clean up	Provides a Pass or Fail indicator for the status of the database clean up service. Indicates a Pass or Fail.

17 - Uninstalling Nymi Components on Endpoints

This section provide information about how to uninstall the Nymi application from endpoints, such as the user terminals and enrollment terminals.

17.1 - Uninstalling the Nymi Band Application

To remove the Nymi Band Application, uninstall the following applications:

- Nymi Runtime
- **Nymi Band application**

The uninstallation process removes the `Nymi Agent` and `Nymi Bluetooth Endpoint` services.

17.2 - Uninstalling Nymi Lock Control

About this task

Perform the following steps to uninstall Nymi Lock Control.

Procedure

1. On the System Tray, right-click the Nymi Lock Control icon, and select `Quit`.
2. Open `Add or Remove Programs`.
3. In `Apps and Features`, search for Nymi Lock Control.
4. Select Nymi Lock Control, and then click `Uninstall`.
5. On the `User Account Control` window, click `Yes`.

17.3 - Uninstalling the Nymi Runtime

Perform the following steps to remove Nymi Runtime.

Procedure

1. Backup configuration files.

   - For user terminals that use Nymi Lock Control, navigate to *C:\Nymi\Bluetooth_Endpoint* and make a copy of the *nbe.toml* file.
   - For centralized Nymi Agent, navigate to *C:\Nymi\NymiAgent* and make a copy of the *nymi_agent.toml* file.

2. Stop the Nymi services, including the Nymi Bluetooth Endpoint and Nymi Agent .

   Note: For a Centralized Nymi Agent deployment, the Centralized Nymi Agent server does not have the Nymi Bluetooth Endpoint service and the user terminals do not have the Nymi Agent service.

3. In `Add or Remove programs`, select `Nymi Runtime`, and then click `Uninstall`.

17.4 - Uninstalling on Nymi Bluetooth Endpoint on HP Thin Pro

Perform the following steps to remove the Nymi Bluetooth Endpoint application from an HP Thin Pro client.

Procedure

1. Connect to the HP Thin Pro client and open an X Terminal session.
2. Type *dpkg --purge nbed_`x.y.z`_amd64.deb*

   Where you replace `x.y.z` with the actual version number of the file.