Administration Guide

Nymi Connected Worker Platform 1.20.X
v3.0
2025-03-09

Contents

3 - Preface

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

Purpose

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

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	December 1, 2025	First release of this document for the CWP 1.20.0 release. Updates were made to reflect changes that were made in Nymi Enterprise Server (NES) to support Nymi Connect for Android and include: • New table entries for SQL database to reflect the tables related to client registration tokens and telemetry that is supported with Nymi Connect for Android. • New chapter *Using Nymi Connect for Android* that includes content that describes new windows in NES to support Nymi Connect for Android.
2.0	December 11, 2025	Second release of this document, which includes updates for CWP 1.20.1 to reflect changes to the NES SQL database table audit.InitialAccessToken.
3.0	March 9, 2026	Third release of this document. Updates to consider Nymi Bands with no vibration motor in the following sections: • Checklist for NB distribution • Customizing Haptic Feedback on Nymi Bands • Manage Individual User Policies • Creating an Individual User Policy

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 with Evidian Solution—Deployment Guide provides information about how to deploy the Nymi with Evidian solution components.
- **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

The user experience with the Nymi Solution starts with a one time Nymi Band enrollment in the Nymi Band Application.

The enrollment process takes less than 5 minutes to complete and associates user credentials to a Nymi Band.

Administrators manage the enrollment experience and how the user can use their Nymi Band by configuring individual or group policy settings on the Nymi Enterprise Server(NES).

Before the start of each shift the user wears their Nymi Band and then performs fingerprint or corporate credentials authentication to activate the Nymi Band. After successful authentication, the user can use the Nymi Band to perform contactless hand free logins, e-signatures and physical access on different endpoint devices and applications.

There are currently 2 main use cases for the Nymi Solution:

- Passwordless login and e-signature, which is where the user unlocks their desktop and completes the signatures by tapping their Nymi Band near the Bluetooth adapter or NFC reader that is attached to the user terminal.
- Physical access, which is where the user unlocks a door by tapping their Nymi Band on or near the door access panel.

To use the Nymi Band to complete authentication tasks, you require an a Nymi-Enabled Application(NEA) that integrates with the Nymi solution. There are three types of integration.

Direct Integration	Application that includes the Nymi SDK and interacts directly with the Nymi Solution to support the completion of authentication tasks with a Nymi Band. For example, POMSnet. This type of integration usually requires some configuration changes in the application to define key components in the customer environment, such as host names. For more information about how to use the Nymi Band with direct integration applications, refer to the Nymi Integration Guides section on the Nymi Support site. Nymi provides you with two direct integration applications, as described later in this document. • Nymi Application, which supports the use of the Nymi Solution with iOS NEAs.

	• Nymi Lock Control, which provides lock and unlock support to Nymi Band users on Windows user terminals.
Middleware(SSO Integration)	Application requires an additional piece of software to enable communication with the Nymi components. For example, Evidian Enterprise Access Management (EAM). An SSO integration usually requires you to perform some configuration changes to define key components in the environment, and in the case of Evidian, you manually copy the *nymi_api.dll* file to the Evidian installation directory. For more information about using the Nymi Band with EAM to complete authentication tasks in applications such as PAS-X, refer to the *Nymi with Evidian Solution—Deployment Guide* for more information.
Open Standards	Applications relies on open standards to communication with the Nymi components. For example, the Nymi Band can store FIDO2 credentials, which a FIDO2-enabled application can access while the Nymi Band remains authenticated. The Nymi Band is a certified FIDO2 authenticator and certified as Microsoft-compatible. This type of integration usually requires some changes to the open standards biometric authentication configuration. For more information about how to use the Nymi Band with FIDO-2 enabled applications, review the *Nymi Connected Worker Platform—FIDO2 Deployment Guide*.

4.1 - Bluetooth Adapter

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

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

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

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

4.2 - 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).

4.2.1 - 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"

 }
}
```

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 Band and charging cradles from the box. • Nymi Band 3 contains enough battery charge to get you through the enrollment activities. The Nymi Band arrives in ship mode, to wake Nymi Band 3.0, press the top bottom. • Nymi Band 4 (ANSI) requires you to charge the Nymi Band for at least 30 minutes prior to enrollment. After enrollment, charge the Nymi Bands for at least 2 hours for a full charge. The battery life of a fully charged Nymi Band differs for ANSI and non-ANSI Nymi Bands. Based on a workday with 300 BLE or NFC taps over 10 hours, you can expect the following results: • non-ANSI Nymi Bands — 3days • Nymi Band 4 (ANSI) — 2 days

	Confirm the Nymi Band variant. Nymi ships variants of the Nymi Band based on use case.
	• If your environment requires Nymi Band 4 (ANSI), perform the following steps to confirm that the Nymi Band does not have a motor:
	  • Inspect each Nymi Band. Nymi Band 4 (ANSI) has a star engraved to the left of the fingerprint sensor and a serial number that begins with the letter “G”. For example, GEXX-1234.
	  • Put each Nymi Band on a charger. Confirm that charging icon appears on the Nymi Band screen but that the Nymi Band does not vibrate.
	• If your environment requires Nymi Band 4 (Seos/Legic) for the HID SEOS support, confirm that the serial number of the Nymi Band begins with the letter “D” or “F”.
	• If your environment requires Nymi Band 4 (Seos/Legic) for Legic Avant functionality, confirm that the serial number of the Nymi Band begins with the letter “F”.

	Use the NES Administrator Console to configure a group policy. For Nymi Band 4 (ANSI), disable Haptic Feedback in the active group policy.

Completed?	Task
	On the Nymi Band Application Terminal that you will use to enroll users: • Install the Nymi Band Application. • Plug the Nymi-provided Bluetooth Adapter into a USB port. • Import the root certificate into the Trusted Root Certificate Authorities store (if you use self-signed certificates).
	On the Nymi Band Application Terminal 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 into a USB port. • Import the root certificate into the Trusted Root Certificate Authorities store (if you use self-signed certificates). **Note:** *Configuring Corporate Credentials Authentication* provides more information about how to enable the Corporate Credentials option in the active group policy.
	On each user terminal: • Install the install Nymi Runtime and the Nymi-enabled Application. • Plug the Bluetooth adapter into a USB port. • Import the root certificate into the Trusted Root Certificate Authorities store (if you use self-signed certificates).
	• 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 Band 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 with Policies

NES provides NES Administrators with the ability to customize Connected Worker Platform by using group and individual policies.

Policies contain configuration settings that modify the behaviour of the Connected Worker Platform and define how users can use their Nymi Bands. NES Administrators can use the NES Administrator Console to:

- Create a new group policy, with configuration settings that apply to all users.
- Create individual user policies that apply to select users.
- 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 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.

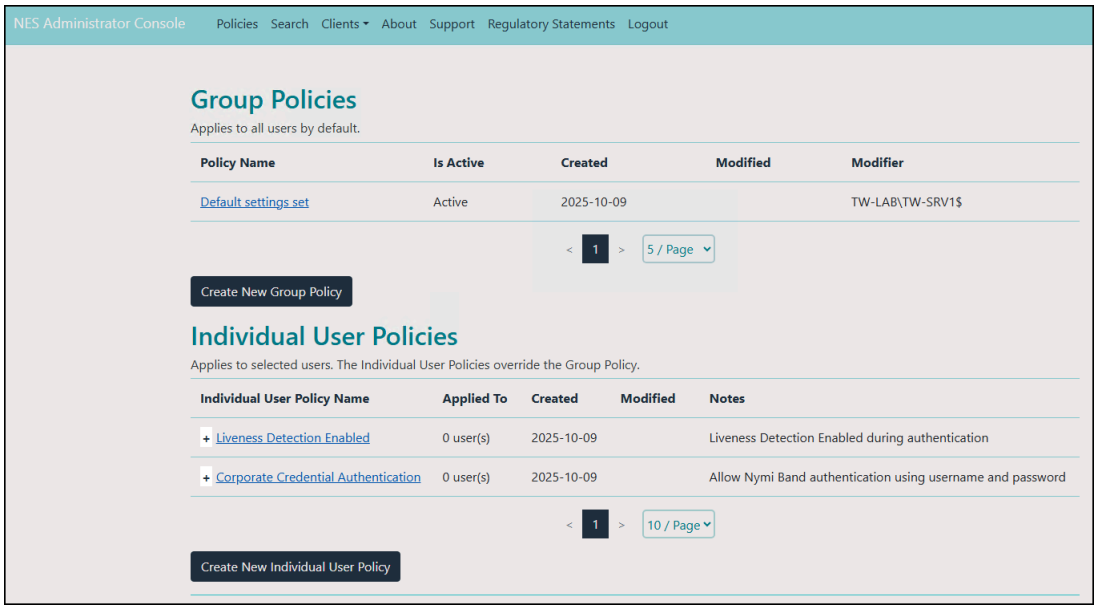


Figure 1: Policies page

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.

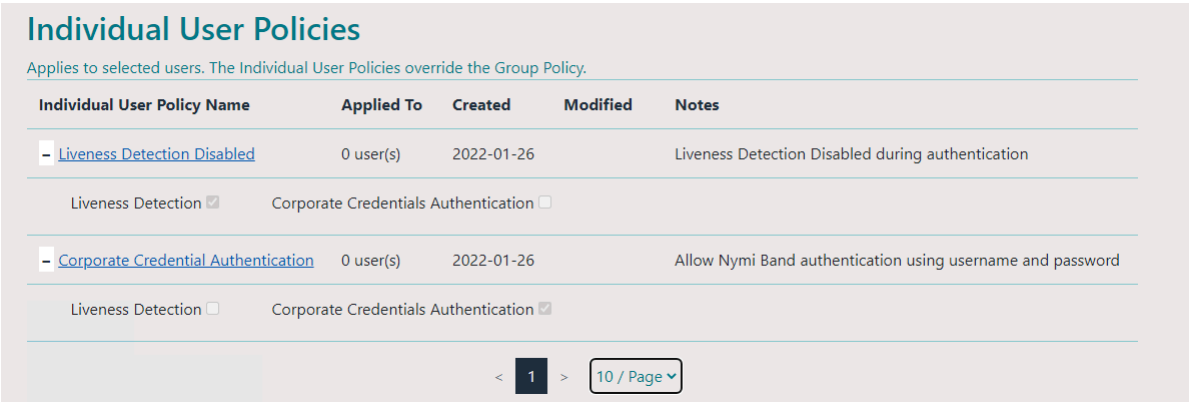


Figure 2: Individual User Policy settings view

   - 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 Nymi Enterprise Server(NES), a default group policy, `Default Settings Set` is configured with the following default 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.
- Do not check for liveness during authentication.
- Do not allow corporate credentials authentication.
- Allow haptic feedback on a Nymi Band that includes a vibration motor.
- 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 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.

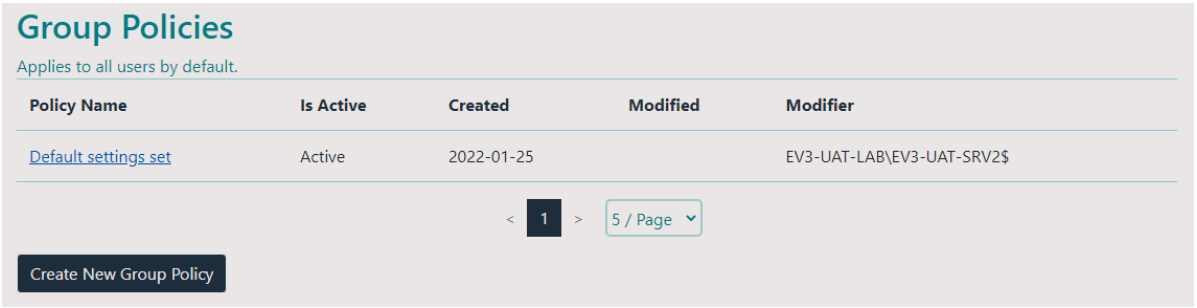


Figure 3: Group Policies Pane

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.

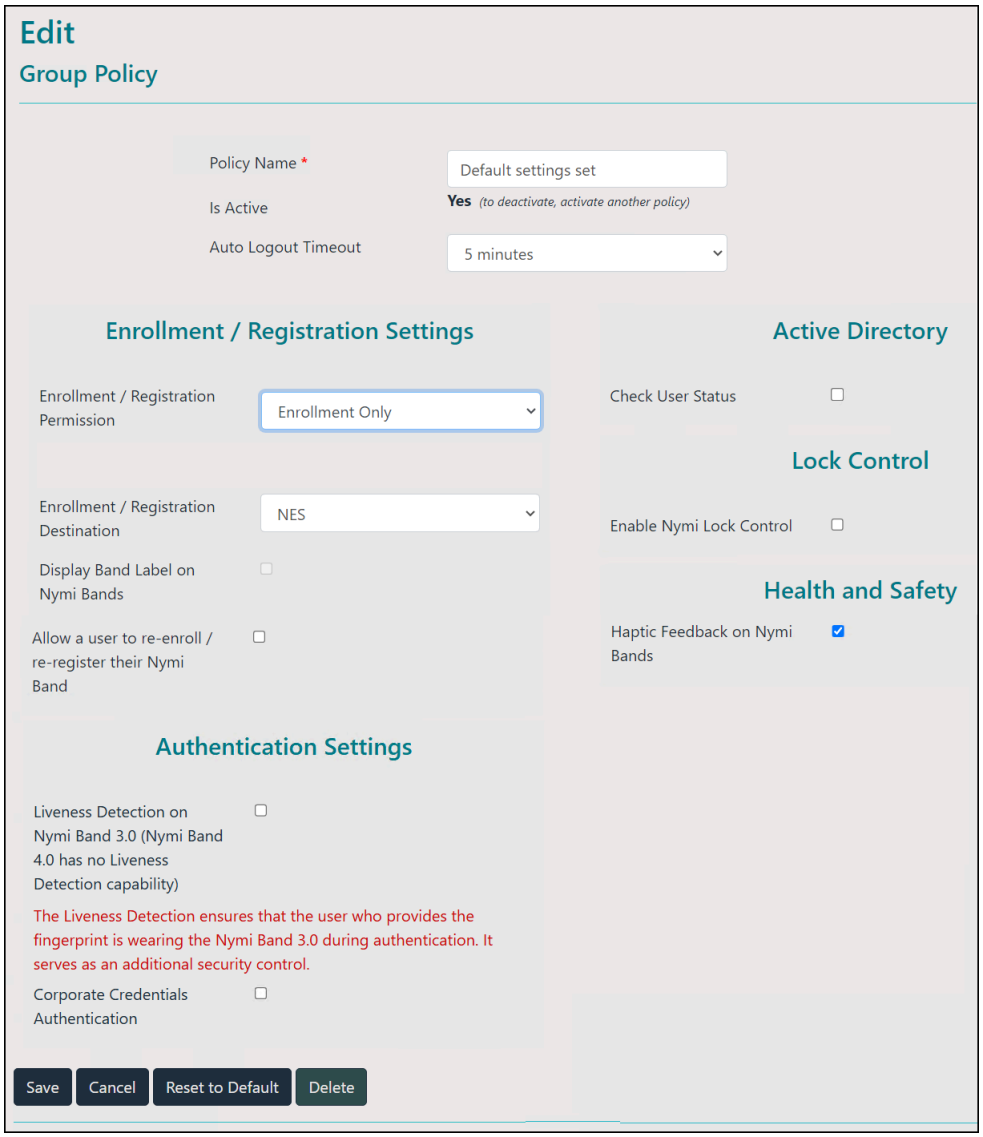


Figure 4: Edit Group Policy page

Note: Liveness Detection applies to Nymi Band 3.0 only. Nymi Band 4.0 does not support liveness detection.

6.2.2 - Creating a New Group Policy

Perform the following steps to create a new group 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 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.

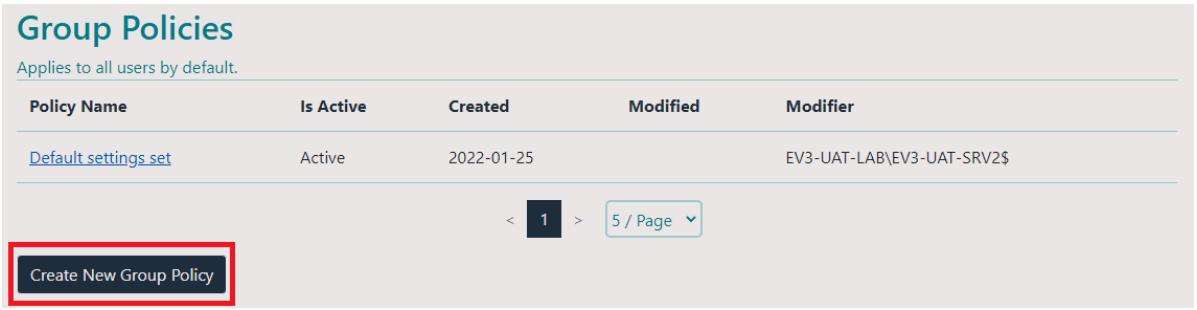


Figure 5: Group Policy page

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 applications and Nymi-enabled Applications(NEAs)
- User-driven self re-enrollment of their Nymi Band or any active Nymi Band.

6.2.5.1 - (Nymi IT/OT Solution only) Configuring NES Permissions

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`**.

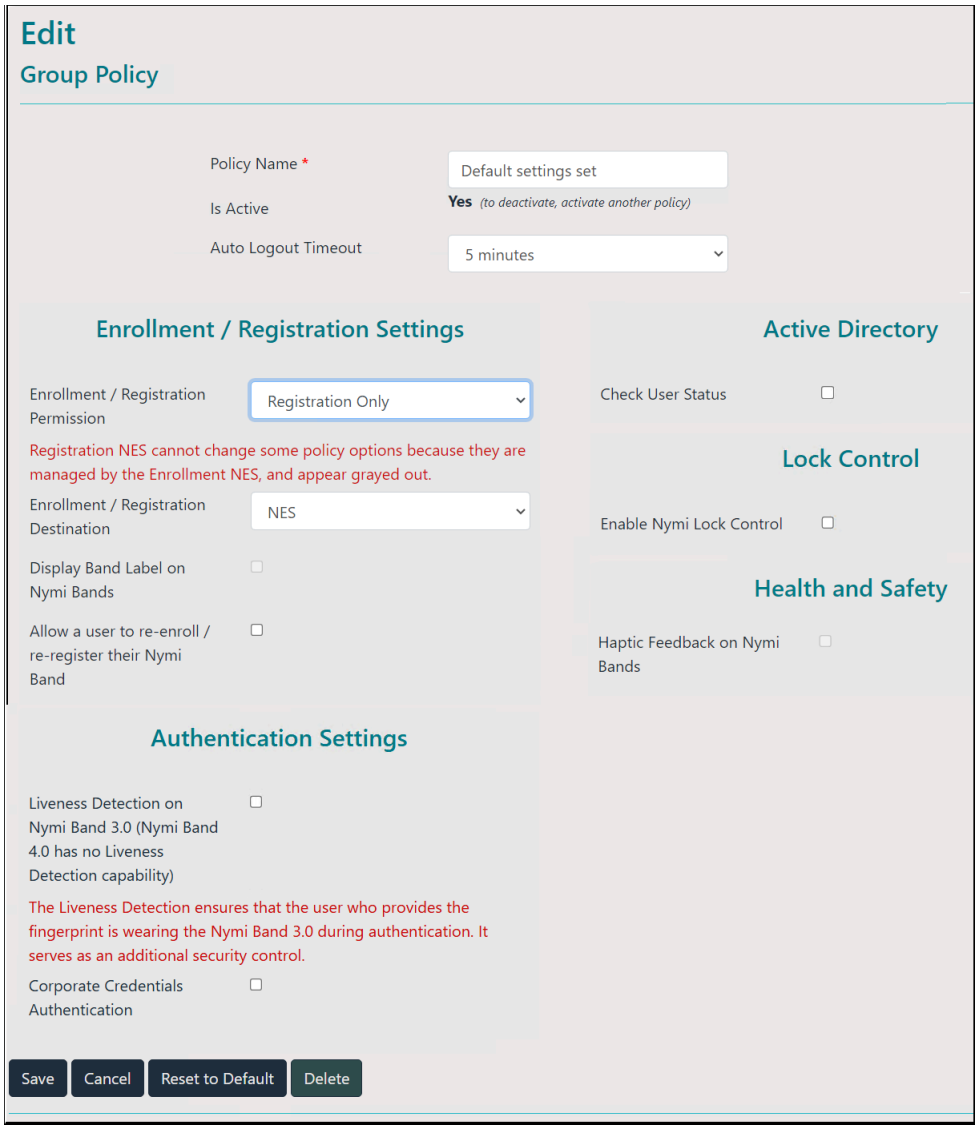


Figure 6: Registration Only Group Policy Example

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 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 with Evidian Solution—Deployment 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.
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 Band 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 Band 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

Note: Liveness detection applies to Nymi Band 3.0 only. Liveness detection is not available in Nymi Band 4.0.

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 Band 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 Nymi Enterprise Server(NES) policy.

About this task

By default, Liveness Detection is disabled.

Note: Liveness detection applies to Nymi Band 3.0 only. Liveness detection is not available in Nymi Band 4.0.

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 Band 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.

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 an NEAbioLock SAP.

Procedure

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

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

Option	Description
	user status and stores the results in cache again. Nymi suggests that you change this value to 30 seconds.

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* in the *Nymi Connected Worker Platform—Deployment Guide*.
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. The *Editing the nbe.toml File* section in the *Nymi Connected Worker Platform—Deployment Guide* provides more information. • 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 Band 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 Band 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 a Nymi Band for all users or for individual users.

Review the following sections for information about customizing haptic feedback on the Nymi Band 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

Nymi Enterprise Server (NES) provides you with the ability to manage liveness detection, corporate credentials, haptic feedback, and self service re-enrollment settings at an individual user level.

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.

NES provides two pre-configured Individual User Policies, which implement the following default behaviour:

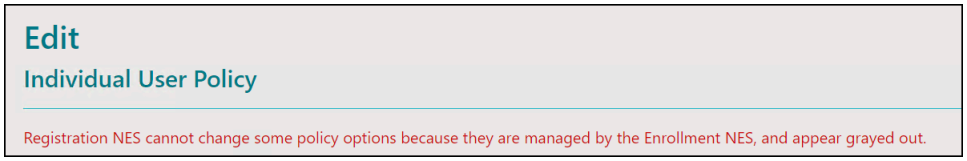
- Liveness Detection Disabled—Biometric authentication of the Nymi Band only validates that there is a fingerprint match and does not perform a liveness check. By default, haptic feedback is enabled on the Nymi Band and the user cannot perform a self-re-enrollment on their Nymi Band or another active 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 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. The **`Liveness Detection`**, **`Haptic Feedback on Nymi Bands`**, and the **`Allow a user to re-enroll to any active Nymi Band`** options are disabled.

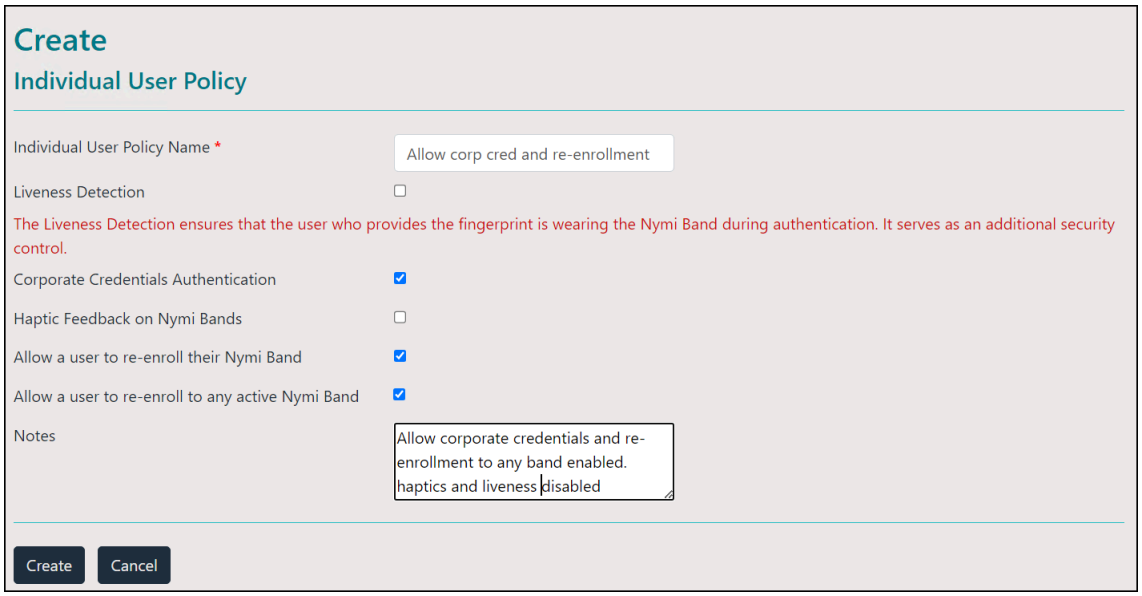


Figure 7: Create Individual Policy page

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 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.

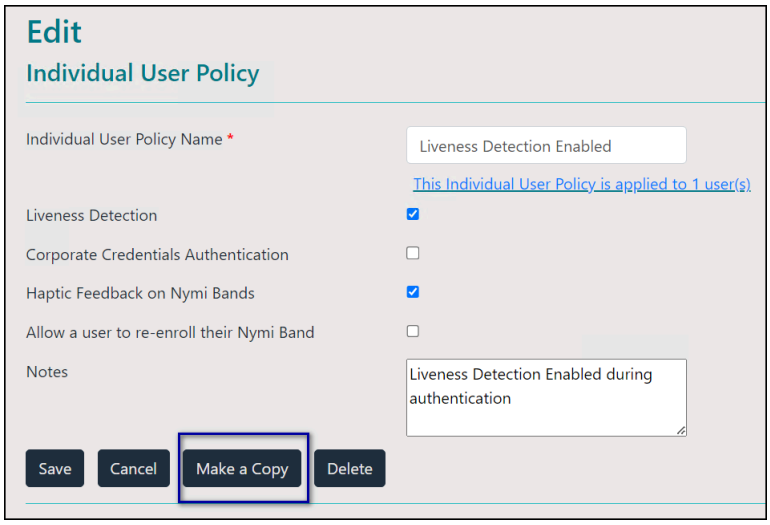


Figure 8: Make a Copy button

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. The **`Liveness Detection`**, **`Haptic Feedback on Nymi Bands`**, and the **`Allow a user to re-enroll to any active Nymi Band`** options are disabled.

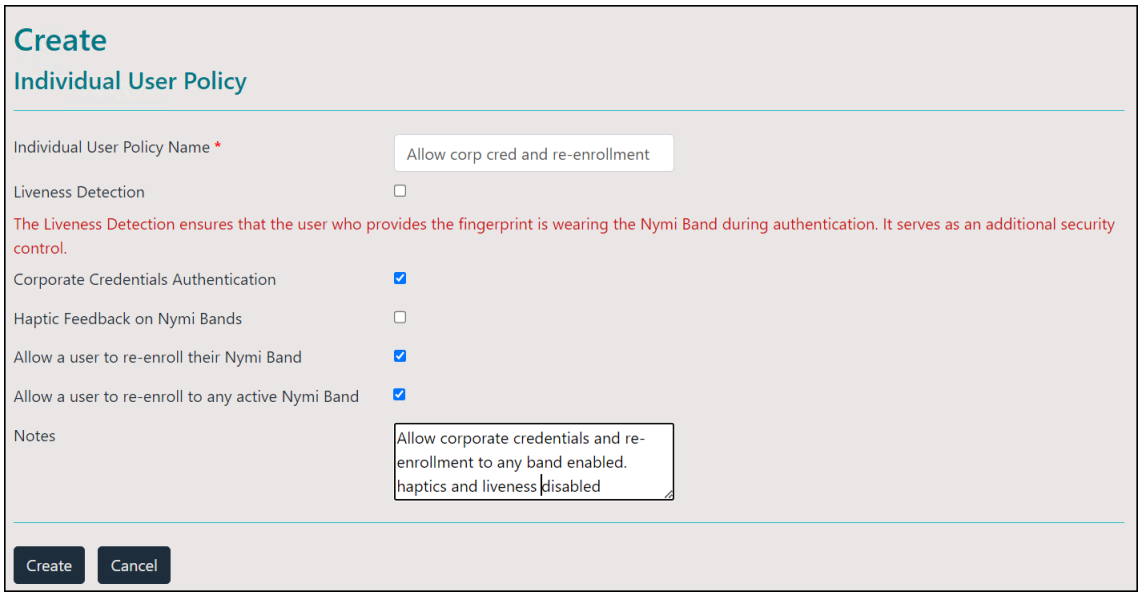


Figure 9: Create Individual Policy page

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 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 Band 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 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.

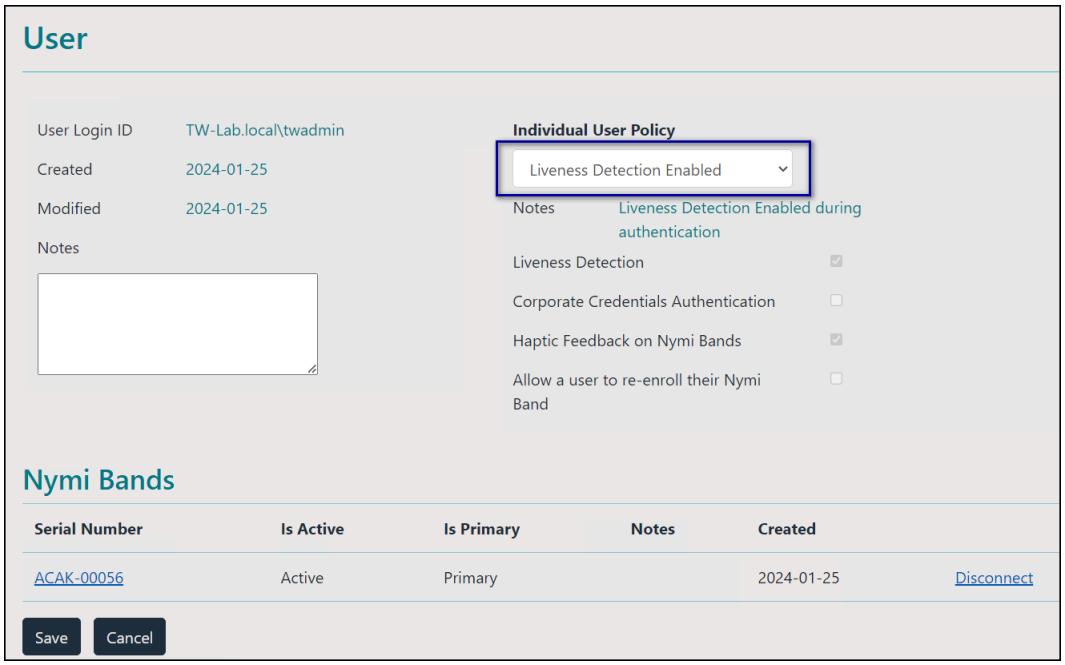


Figure 10: User Properties page

7. Click **Save**.

Results

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Band 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.

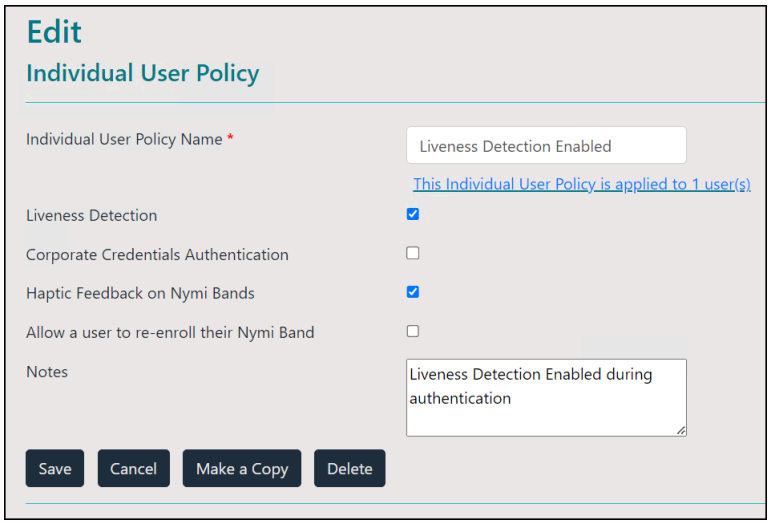


Figure 11: Edit Individual User Policy page

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.

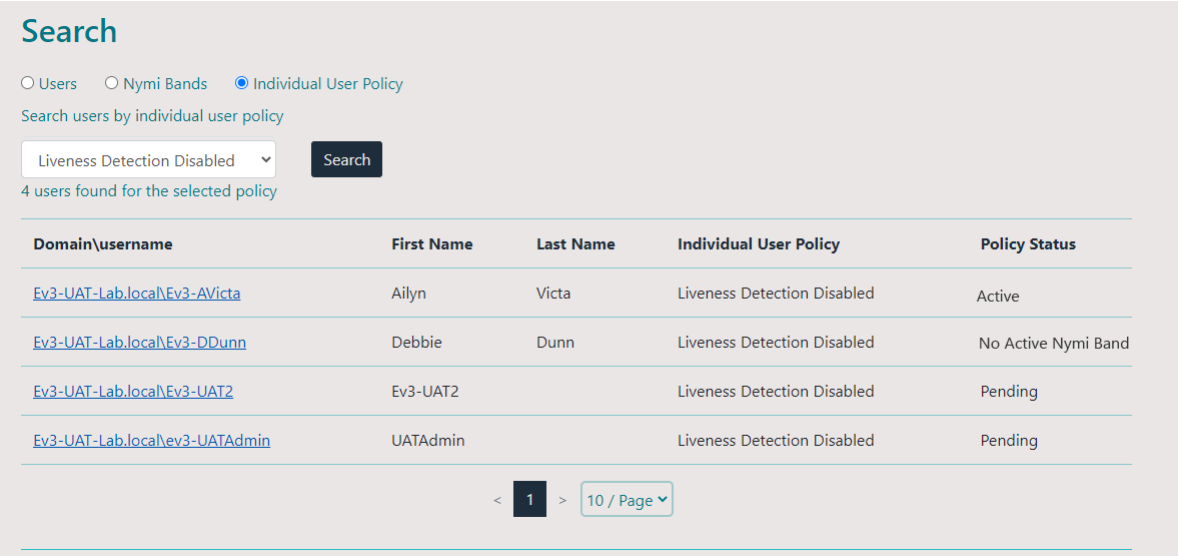


Figure 12: Individual User Policy Search Results

7 - Nymi Band Enrollment Process Overview

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 Connected Worker Platform provides an additional method of authentication called a corporate credential authenticator. When you enabled Corporate Credentials authentication in the NES policy, then during enrollment, 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.

The *Nymi Band User Guide* provides detailed information about how a user performs a Nymi Band enrollment.

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 Nymi Enterprise Server(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 Nymi Enterprise Server(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.

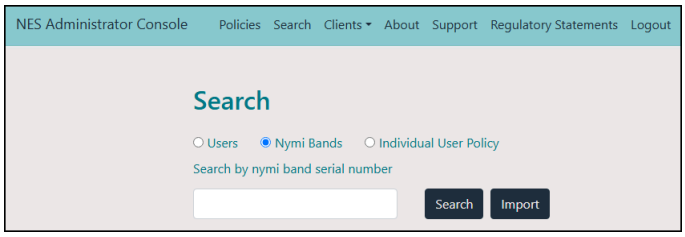


Figure 13: Import option in Search window

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

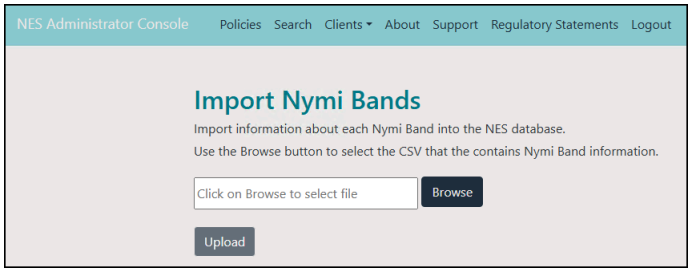


Figure 14: Browse in Import Nymi Bands window

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.

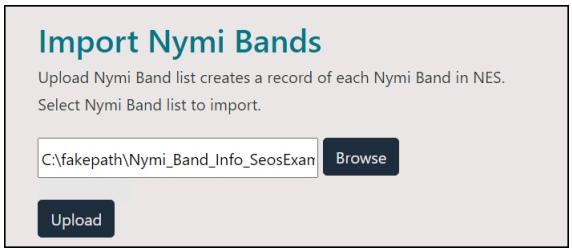


Figure 15: Import file window with filename

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.

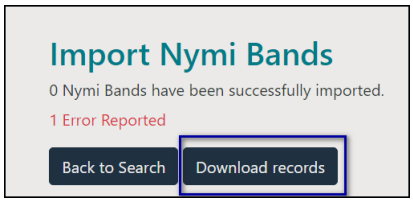


Figure 16: Nymi Band Import error

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 Nymi Band that encountered an issue.

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 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.

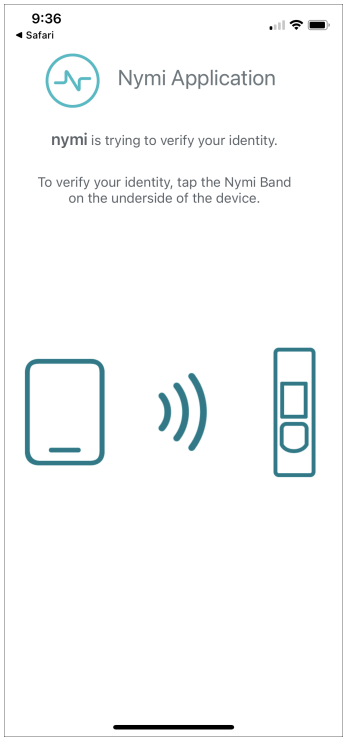


Figure 17: Nymi Application

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

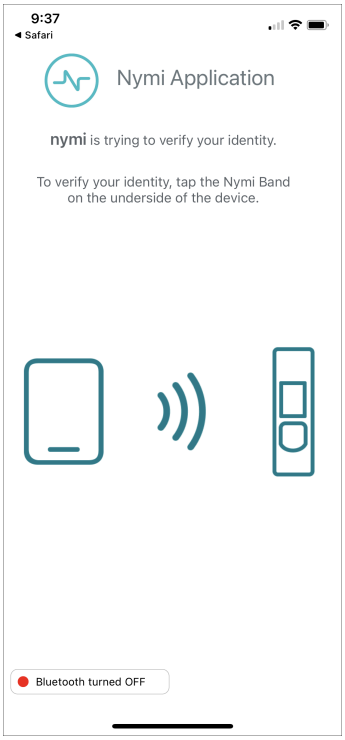


Figure 18: Nymi Application - Cannot Access Bluetooth Adapter

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.

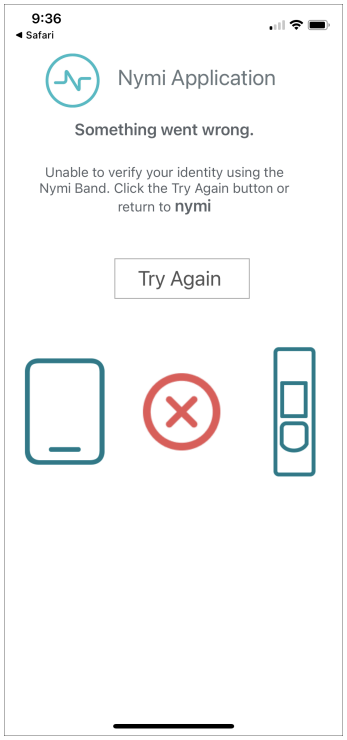


Figure 19: Nymi Application Timeout

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.

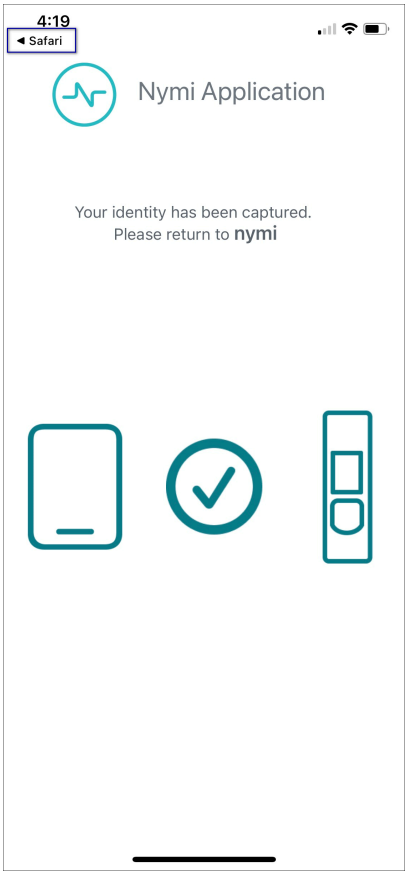


Figure 20: Nymi Application Success

9.1 - Overriding the Nymi Band Tap Configuration

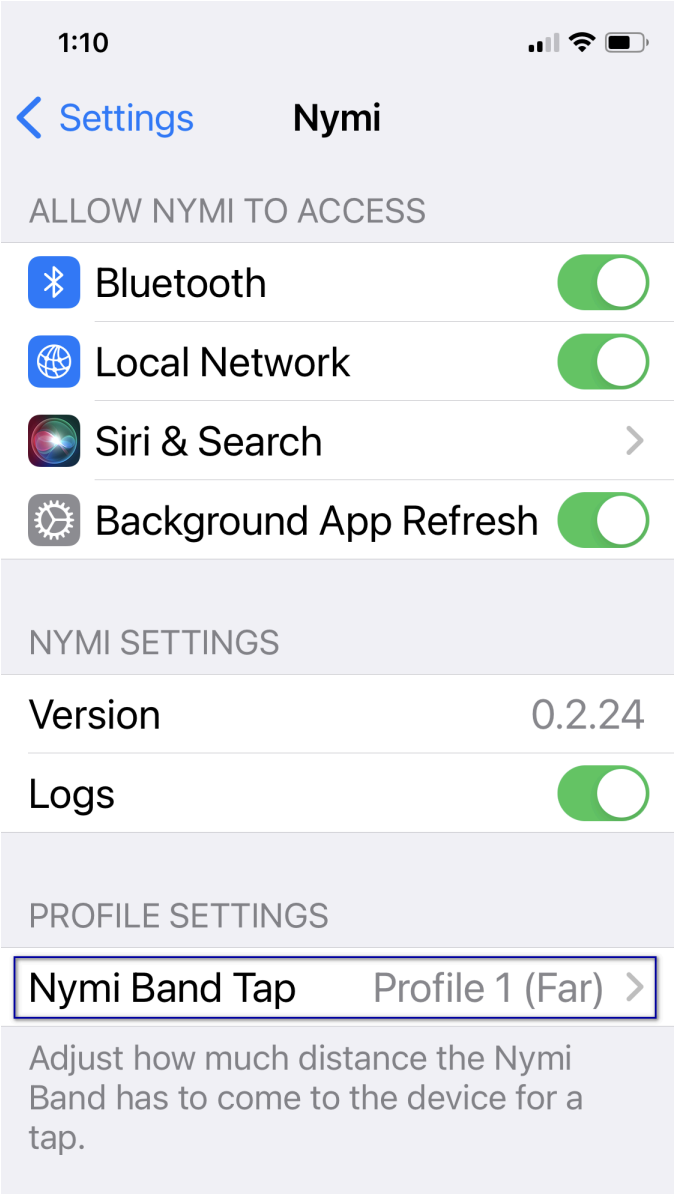
The MDM device profile defines the positioning of the Nymi Band near the Bluetooth adapter that the Nymi Application requires to complete an authentication task.

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.



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.

10 - 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, 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.

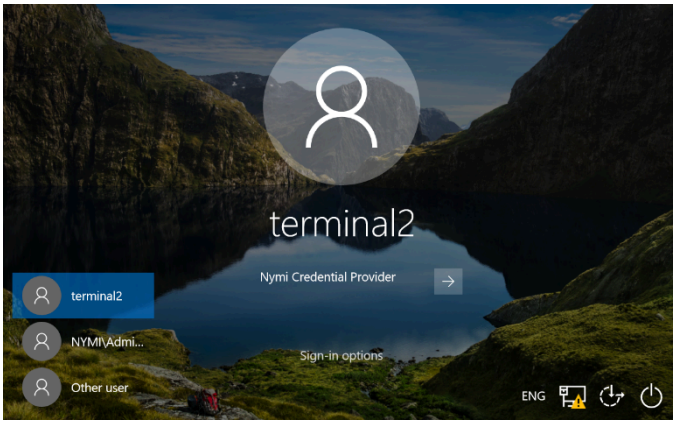


Figure 21: User Terminal Log in Screen with Nymi Lock Control

10.1 - 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* in the *Nymi Connected Worker Platform—Deployment Guide*.
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. The *Editing the nbe.toml File* section in the *Nymi Connected Worker Platform—Deployment Guide* provides more information. • 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.

Option	Description
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 Band 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.

10.2 - Edit the Nymi Bluetooth Endpoint Configuration File

The Nymi Bluetooth Endpoint application enables BLE functionality for Nymi Lock Control and BLE tap. Editing the Nymi Bluetooth Endpoint configuration file adjusts the behavior of these features.

Note: Nymi Lock Control functions with a BLE radio antenna or NFC reader. The settings described in this section refer to Nymi Lock Control with a BLE adapter only, and not an NFC reader.

Nymi Lock Control and BLE tap behavior is dependent on the distance between the Nymi Band and the BLE radio antenna. The distance between the radio antenna and the Nymi Band is represented by changes in the Received Signal Strength Indication (RSSI) value, and is determined by measuring the radio signals received by the BLE radio antenna. Close distances between the Nymi Band and BLE radio antenna result in stronger signals, and far distances result in weak signals. BLE tap and Nymi Lock Control actions occur when the trends in changing RSSI values reach a certain threshold defined in the Nymi Bluetooth Endpoint configuration settings.

The default RSSI values used by Nymi Bluetooth Endpoint may not be optimal for certain users. For example, under default settings the user terminal may unlock when the user is too far away, or the user terminal may accidentally lock while the user is present. In these cases, the BLE radio antenna is too sensitive, not sensitive enough, or the placement of the BLE adapter prevents the Nymi Band from being read consistently. Edit the Nymi Bluetooth Endpoint configuration settings on a user terminal to adjust for these discrepancies.

To adjust the sensitivity of BLE taps and Nymi Lock Control, edit the Received Signal Strength Indication (RSSI) values in the Nymi Bluetooth Endpoint configuration file, *nbe.toml*.

Note: The *nbe.toml* file described in this section is only used to apply adjustments to Nymi Lock Control and BLE tap behavior with a BLE radio antenna (ex. USB adapter). If the *nbe.toml* file is renamed or deleted, Nymi Lock Control and BLE taps behave under the default settings.

10.2.1 - Tuning Nymi Band Tap Behaviour For Nymi Lock Control

Nymi Bluetooth Endpoint uses the Bluetooth adapter to detect nearby Nymi Bands. NBE evaluates the signal strength of a Nymi Band against predefined RSSI settings to decide if a Nymi Band tap has occurred. .

To change how close a user needs to place the Nymi Band near the Bluetooth adapter for Nymi Bluetooth Endpoint to detect a tap, you can adjust the RSSI settings.

How you modify the RSSI parameters depends on the operating system:

- On Windows thick clients, edit the *C:\Nymi\Bluetooth_Endpoint\nbe.toml* file in administrator mode.
- On HP Thin Pro, edit the */usr/bin/nbe.toml* file.
- On IGEL, in UMS, navigate to **`System > Firmware Customization > Custom Partition > Partition`** and define the partition parameters.

Note: On Windows and HP Thin Client, when the *nbe.toml* file is not present, Nymi Bluetooth Endpoint uses the default values. On IGEL, when you do not define the parameters in UMS, Nymi Bluetooth Endpoint uses the default values.

There are two types of RSSI parameters that define tap behaviour:

- Tap Windows parameters—Evaluates a defined number of RSSI measurements captured by the Bluetooth Adapter to determine a rolling average. The average allows the Nymi Bluetooth Endpoint to smooth out signal fluctuations and ignore outliers.
- Tap Threshold parameters—Define the specific RSSI levels that trigger an event. For example, when the average RSSI from the tap window parameters exceeds the tap threshold, Nymi Bluetooth Endpoint detects a tap.

The following table provides a list of supported RSSI parameters, their default values and the purpose of each parameter.

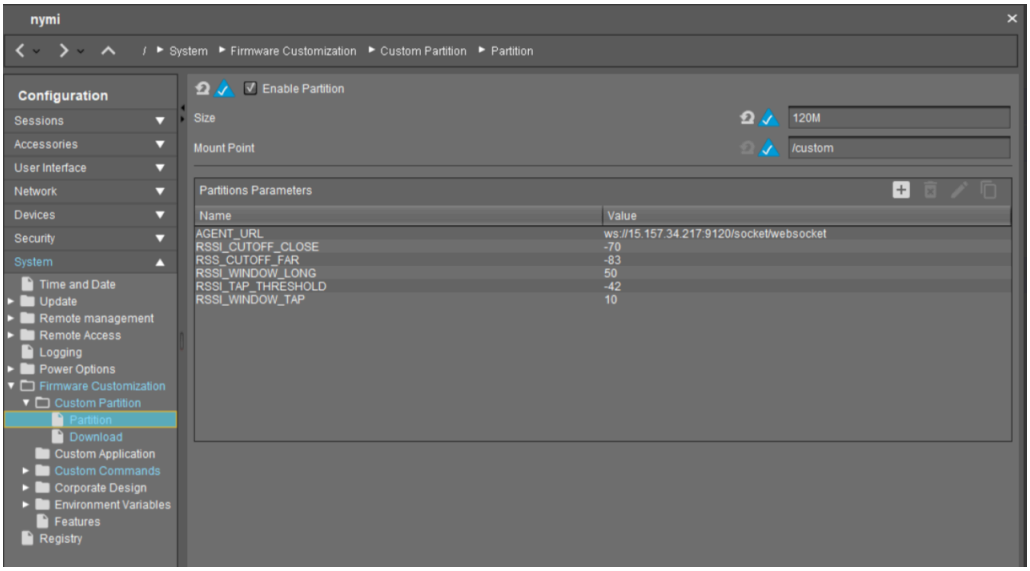
Note: For IGEL, specify all RSSI parameter names in capital letters.

Table 4: RSSI Values

RSSI Parameter	Default Value	Description
rssi_window_tap	10	Defines how long the user must keep their Nymi Band within the tap threshold distance of the Bluetooth Adapter to complete a Nymi Band tap. A larger value increases the amount of time that a user must keep their Nymi Band within bluetooth range of the Bluetooth Adapter and decreases the sensitivity.
rssi_window_long	Bluegiga: 50	Defines how often the Nymi Bluetooth Endpoint service checks the distance between the Bluetooth Adapter and the Nymi Band. This helps determine proximity. Nymi Bluetooth Endpoint tracks trends in these changes to trigger a Nymi Lock Control action, such as **`keep unlocked when present`**, **`lock when away`**, or **`unlock when present`**.
rssi_tap_threshold	Bluegiga: -42 (must be 0 or negative)	Determines the range at which a tap event will occur. A smaller negative value means a closer distance to the BLE antenna. BLE tap is disabled by default (value = 0). **Enter a non-zero, negative number to enable BLE tap**. If the Nymi Band maintains a minimum distance specified by *rssi_tap_threshold*, for the duration of time that is defined by *rssi_window_tap*, a BLE tap is performed.

RSSI Parameter	Default Value	Description
rssi_cutoff_close	Bluegiga: -70 (must be 0 or negative)	This determines the outer range of the close distance-threshold (excluding tap distance) for Nymi Lock Control. Enter 0 to bypass the proximity functionality of Nymi Lock Control. If the Nymi Band maintains a close distance to the BLE radio antenna and the RSSI values measured are within the *rssi_cutoff_close* value, Nymi Lock Control keeps the user terminal unlocked. If the Nymi Band moves away from the BLE radio antenna, and the RSSI values measured are on a decreasing trend and goes from the *rssi_cutoff_close* value to the *rssi_cutoff_far* value, Nymi Lock Control locks the user terminal.
rssi_cutoff_far	Bluegiga: -83 (must be negative)	This determines the outer range of the far distance-threshold (excluding tap distance) for Nymi Lock Control. If the Nymi Band moves towards the BLE radio antenna, and the RSSI values measured are on an increasing trend and goes from the *rssi_cutoff_far* value to the *rssi_cutoff_close* value, Nymi Lock Control unlocks the user terminal.

The following figure provides an example of the Partition Parameters window in UMS with each RSSI value.



After you save the changes, restart the Nymi Bluetooth Endpoint, which reloads the parameter settings.

10.3 - 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.

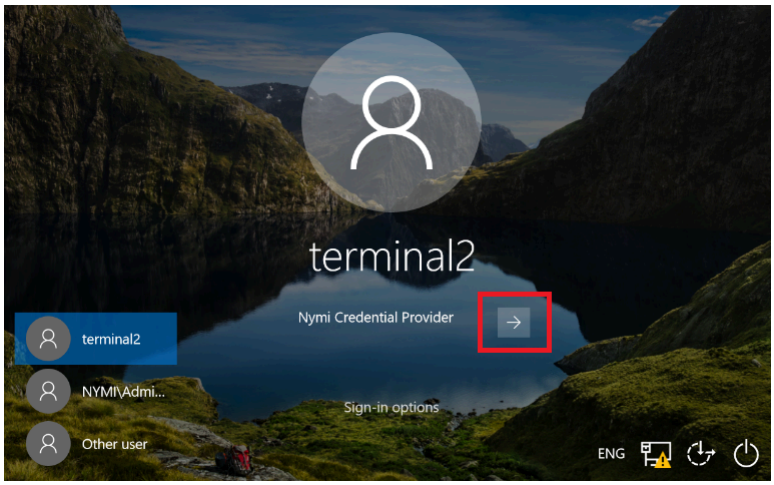


Figure 22: Nymi Credential Provider button

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

10.4 - 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.

10.5 - 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.

10.6 - 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.

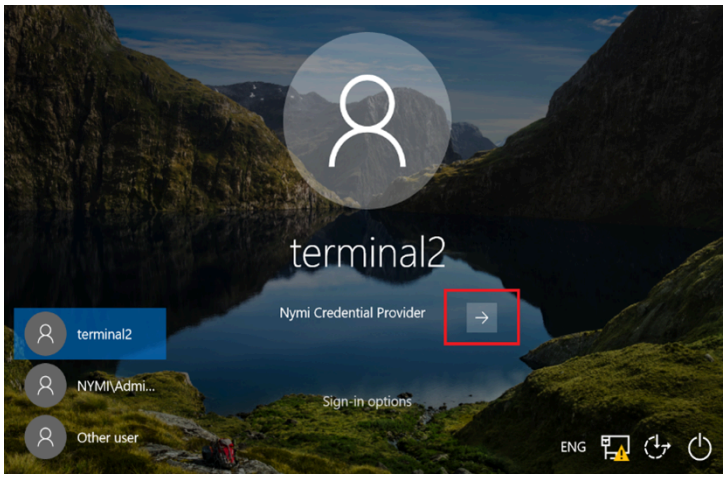


Figure 23: Nymi Credential Provider Submit button

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

10.7 - 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.

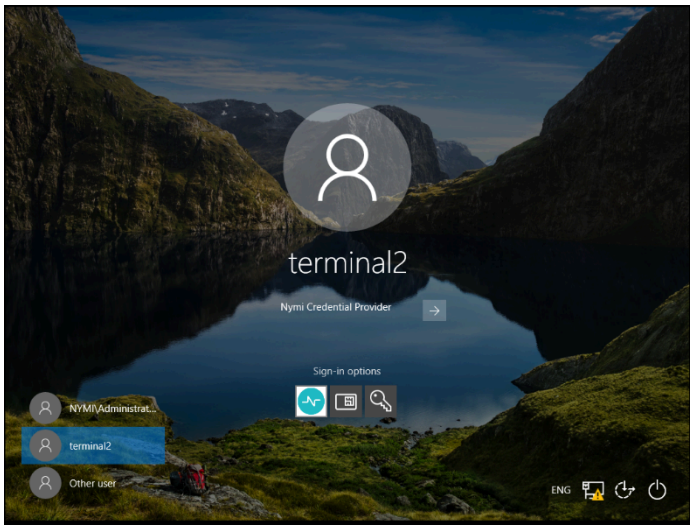


Figure 24: Sign-on Options screen

10.8 - 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.

10.9 - 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`**.

11 - Using Nymi Connect for Android

Nymi Connect for Android is an application that allows users to tap their authenticated Nymi Band on or near the builtin Bluetooth Adapter of an Android device to complete authentication tasks such as log in and e-signatures.

To use Nymi Connect for Android, Android devices must register as a client with Nymi Enterprise Server (NES). Dynamic client registrations require an initial access token (IAT), also called a client registration token (CRT). This chapter provides information about how to create a CRT, manage a CRT and manage clients that are registered in NES.

The *Nymi Connect for Android - Deployment and Administration Guide* provides detailed information about how to deploy and use Nymi Connect for Android.

11.1 - Generating the Client Registration Token

To establish secure communications between Nymi Connect for Android and Nymi Enterprise Server(NES), Nymi Connect for Android uses a client registration token (CRT) to dynamically register the client with NES.

Before you begin

Determine your token distribution policy. You can use the same token for all Android devices or create separate tokens for different Android devices.

About this task

Perform the following steps to generate the client registration token (CRT) in NES, which you must provision to every Android device that uses Nymi Connect.

Procedure

1. Log in to the NES Administrator Console as an NES Administrator.
2. From the **`Clients`** menu, select `Manage Client Registration Tokens` tab,

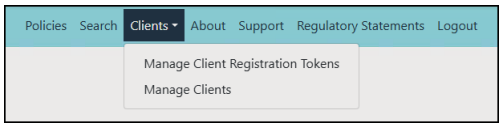


Figure 25: NES Clients menu

3. Click **`Generate New Token`**, as shown in the following figure.

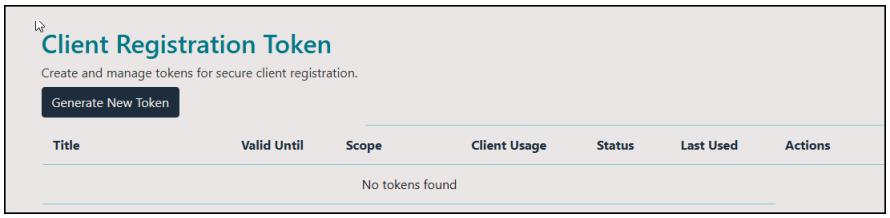


Figure 26: Generate New Token

The `Generate Client Registration Token` window appears.

4. In the `Generate Client Registration Token` window, perform the following actions:
   a) In the **`Title`** field, specify a unique and descriptive name.
   b) In the **`Expiry Date/Time`** field, click the **`Calendar`**, and then select an expiration date for the token.

      Choose a date and time that allows your Software Administrator sufficient time to install and register all the Android devices.
   c) In the **`Scope`** section, leave the default value **`Nymi Connect`** selected.
   d) Optionally, in the **`Description`** section, provide descriptive information up to 4000 characters.
   e) In the **`Max client limit`** field, specify the maximum number of Android devices that can use this token to dynamically register with NES. A value of 0 means that there is no limit on the number of clients that can use this token to perform a dynamic registration.
   f) Click **`Generate token`**.

   The following figure provides an example of the `Generate Client Registration Token` window.

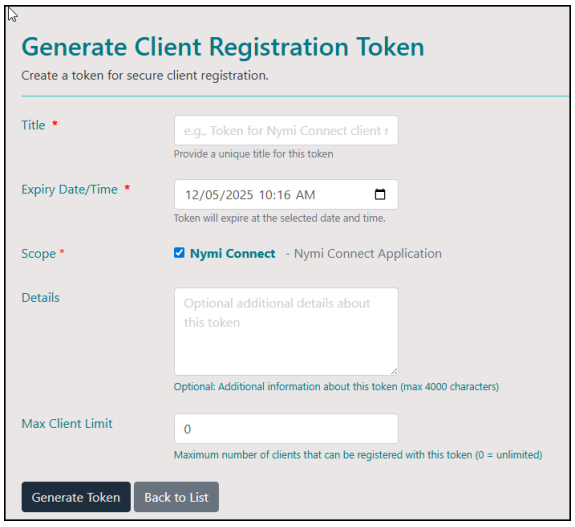


Figure 27: Generate Client Registration Token window

The `Token Generated Successfully` window appears.

5. On the `Token Generated Successfully` window, the JWT token appears. Retrieve the token in one of the following ways:

   - When you use a Mobile Device Management (MDM) to push Nymi Connect for Android to Android devices:

     a. Click **`Copy JSON`**.
     b. Open a text editor and paste the JSON string.
     c. Save the file.

   - When you manually install and configure Nymi Connect for Android on an Android device, click **`Download QR Code`**. NES saves an image of the QR Code in *PNG* format in the *Downloads* folder of the current user.

   The following figure provides an example of the `Token Generated Successfully` window.

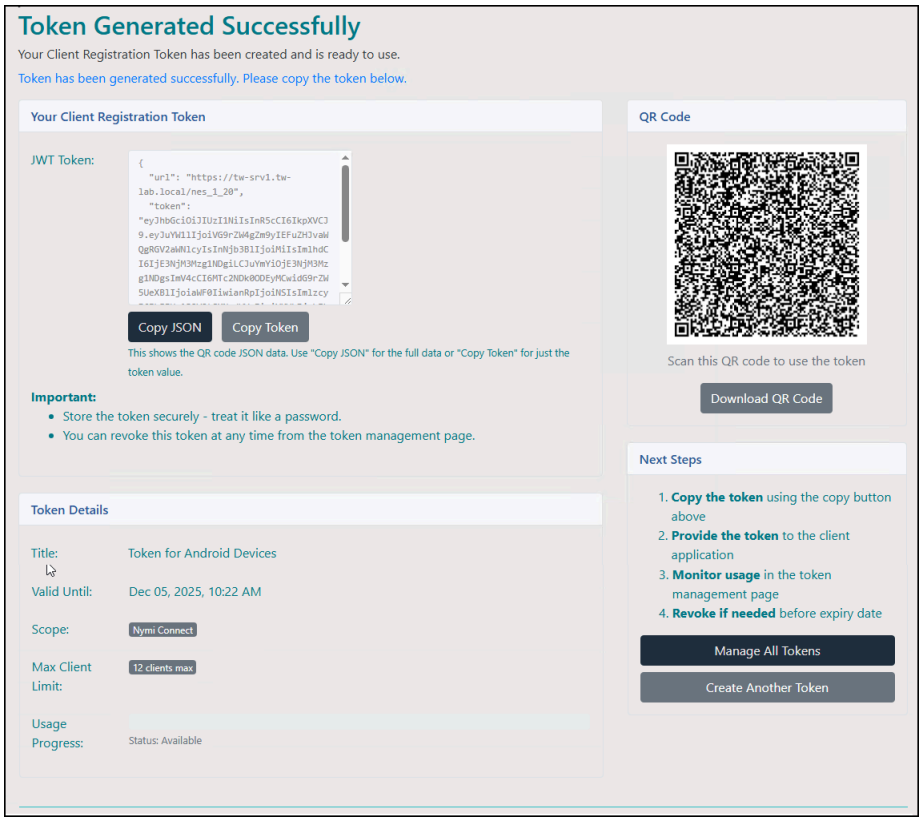


Figure 28: Token Generated Successfully window

6. Provide the copy of the token to your software management system administrator.

What to do next

Ensure that you store the copy of the token securely.

11.2 - Managing Client Registration Tokens

Use the NES Administrator Console to manage your client registration tokens (CRTs).

From the **`Clients`** menu, select **`Manage Client Registration Tokens`**. A window similar to the following appears.

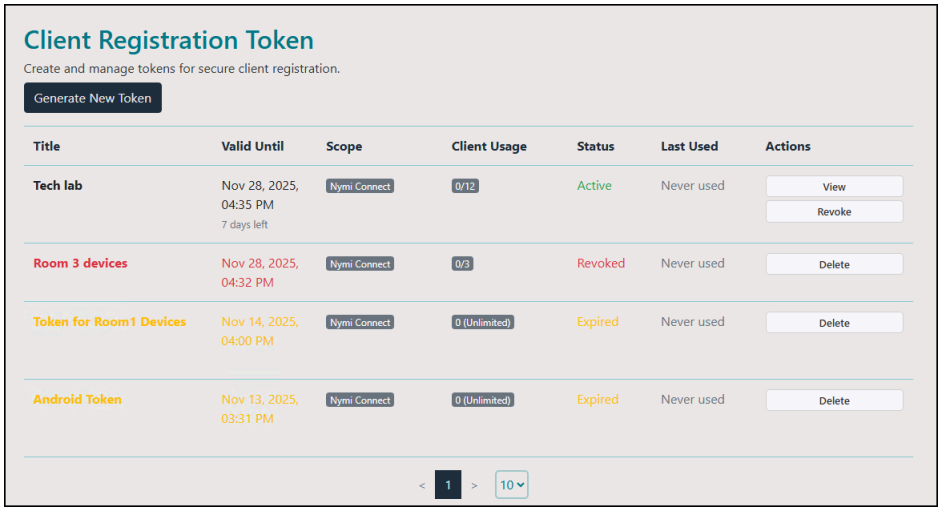


Figure 29: Manage Client Registration Tokens

The `Manage Client Registration Tokens` table provides a summary of each client registration token with the following information:

Column	Description
Title	Displays the descriptive name of the CRT.
Scope	Displays the Nymi application that is associated with the token.
Client Usage	Displays how many clients have used the CRT to perform a client registration in Nymi Enterprise Server(NES), followed by the number of clients that can use the CRT for dynamic registration in brackets.
Status	Displays the Status of the CRT including Active, Expired, and Revoked.
Last Used	Displays the most recent date that a device used the CRT to complete a client registration in NES.
Actions	Provides the user with two buttons to perform management actions on the CRT: • View the properties of the CRT. • Revoke the CRT. • Delete an expired or revoked CRT.

Viewing CRTs

View the details of an CRT to copy the token, copy the JSON string or download the QR code of the token.

1. In the **Manage Client Registration Tokens** table, from the **Actions** column of the CRT, click **View**.
2. On the Token Details window, perform the appropriate action. The following figure provides an example of the Token Details window.

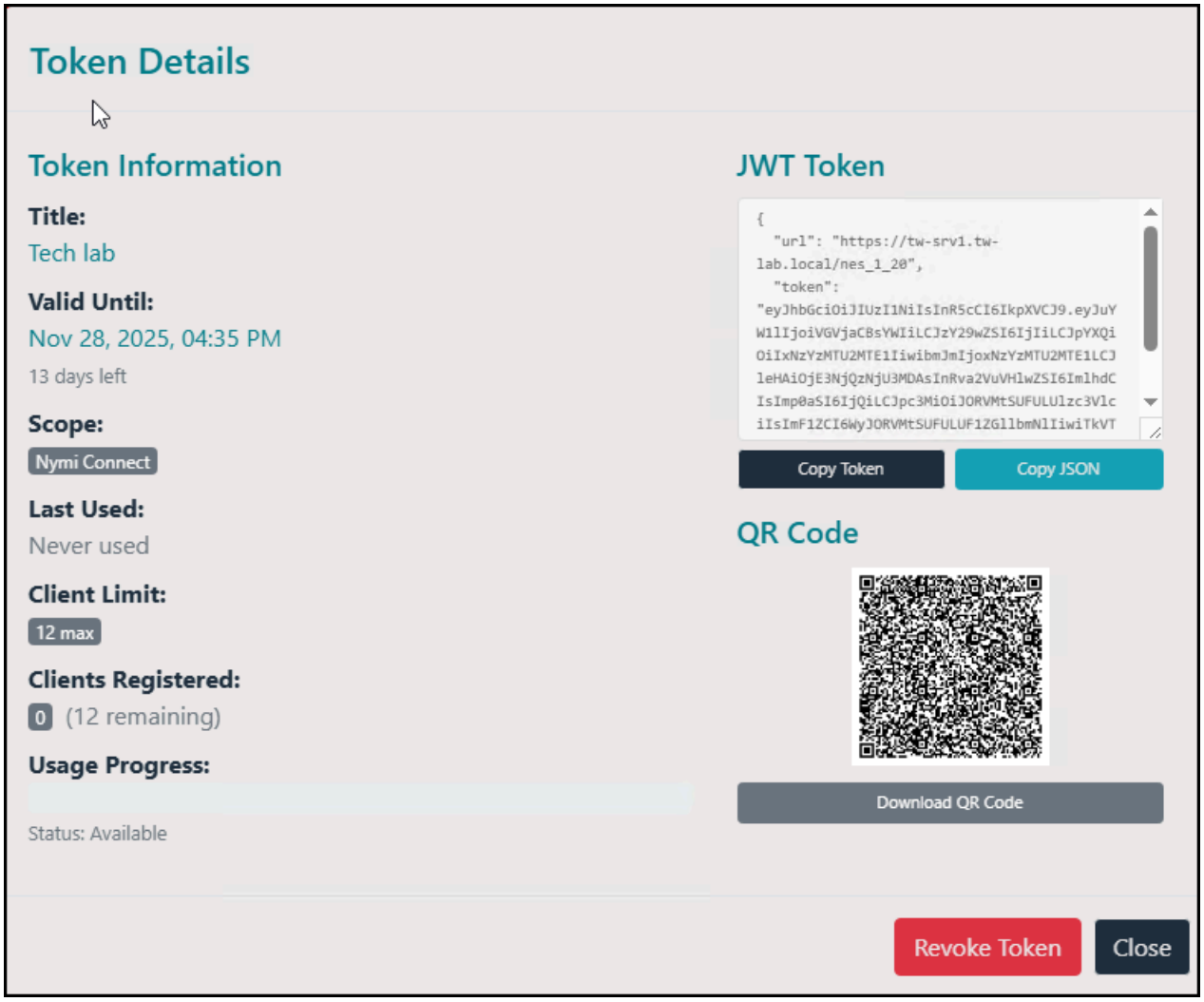


Figure 30: Token Details window

Revoking CRTs

Revoke an CRT to prevent unauthorized access and misuse. When you revoke an CRT, a new device cannot use the CRT to dynamically register with NES.

1. In the **Manage Client Registration Tokens** table, from the **Actions** column of the CRT, click **Revoke**.
2. On the Revoke token popup, click **Revoke Token**. The status of the token in the table displays *Revoked*.

Deleting CRTs

Optionally, delete an expired or revoked CRT to remove the CRT entry from the **Manage Client Registration Tokens** table. When you delete an CRT, the action removes the CRT from the **Manage Client Registration Tokens** table but not the NES database.

1. In the **Manage Client Registration Tokens** table, from the **Actions** column of the CRT, click **Delete**.
2. On the Delete token popup, click **Delete Token Permanently**.

11.3 - Managing Clients that use Client Registration Tokens

Use the NES Administrator Console to manage clients that use client registration tokens (CRTs).

Viewing Clients

You can view information about the clients in your environment, including the hostname, OS type, and the date that of the client registration.

From the **Clients** menu, select **Manage Clients**. A window similar to the following appears.

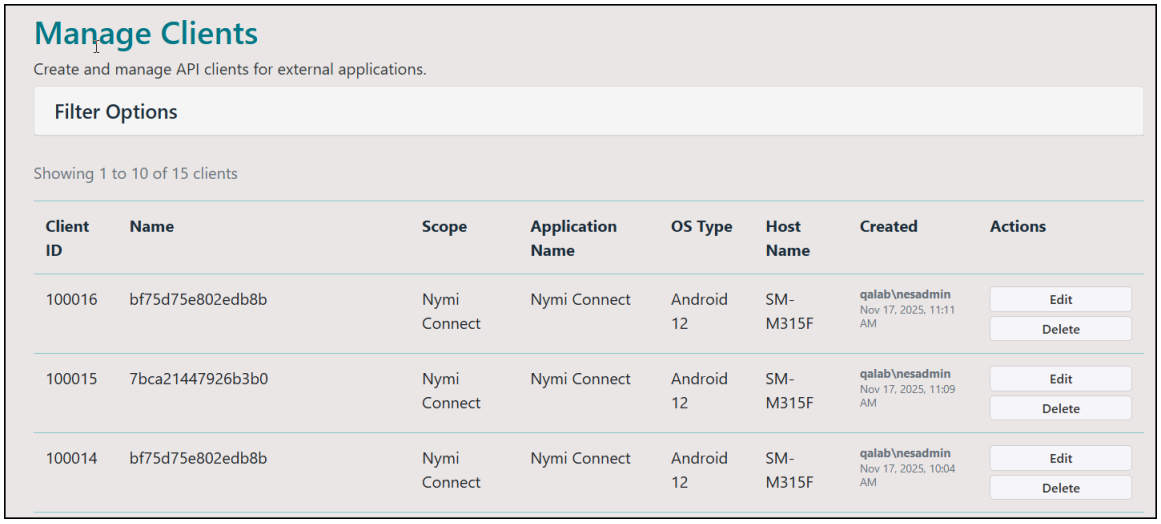


Figure 31: Manage Clients window

The Manage Clients table provides a summary of each client with the following information:

Column	Description
Client ID	Displays a unique identifier for the client.
Name	Displays the Android ID of the device.

Column	Description
Scope	Displays the Nymi application that is used by the client.
OS Type	Displays the operating system of the client.
Hostname	Displays the hostname of the client.
Created	Displays the date that the client was dynamically registered in NES and the user that performed the action.
Actions	Provides the user with two buttons to perform management actions on the client: • Edit the client. • Delete the client.

Editing Clients

You can edit a client to change the client name.

1. In the **`Manage Clients`** table, from the **`Actions`** column of the appropriate client, click **`Edit`**.
2. On the `Edit Client` window, in the **`Client Name`** field, update the name.
3. Click **`Save`**.

The following figure provides an example of the `Edit Client` window.

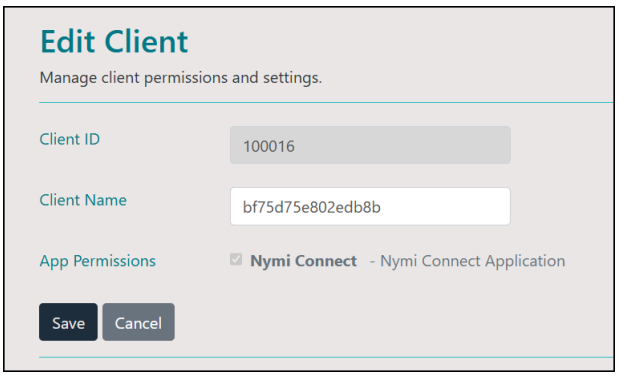


Figure 32: Edit Client window

Deleting Clients

Delete a client to prevent the use of Nymi Connect and a Nymi Band to complete authentication tasks in all target applications on a device.

1. In the **`Manage Clients`** table, from the **`Actions`** column of the appropriate client, click **`Delete`**.
2. On the `Delete client` popup, click **`Delete`**. When you delete an client, the action removes the client from the NES Administrator Console but not the NES database. To allow

a client to use Nymi Connect and a Nymi Band, you must push an CRT to the client and complete dynamic registration.

12 - Nymi Bands Management in NES

You can manage Nymi Bands for each user in the NES Administrator Console.

12.1 - 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.

12.1.1 - 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.

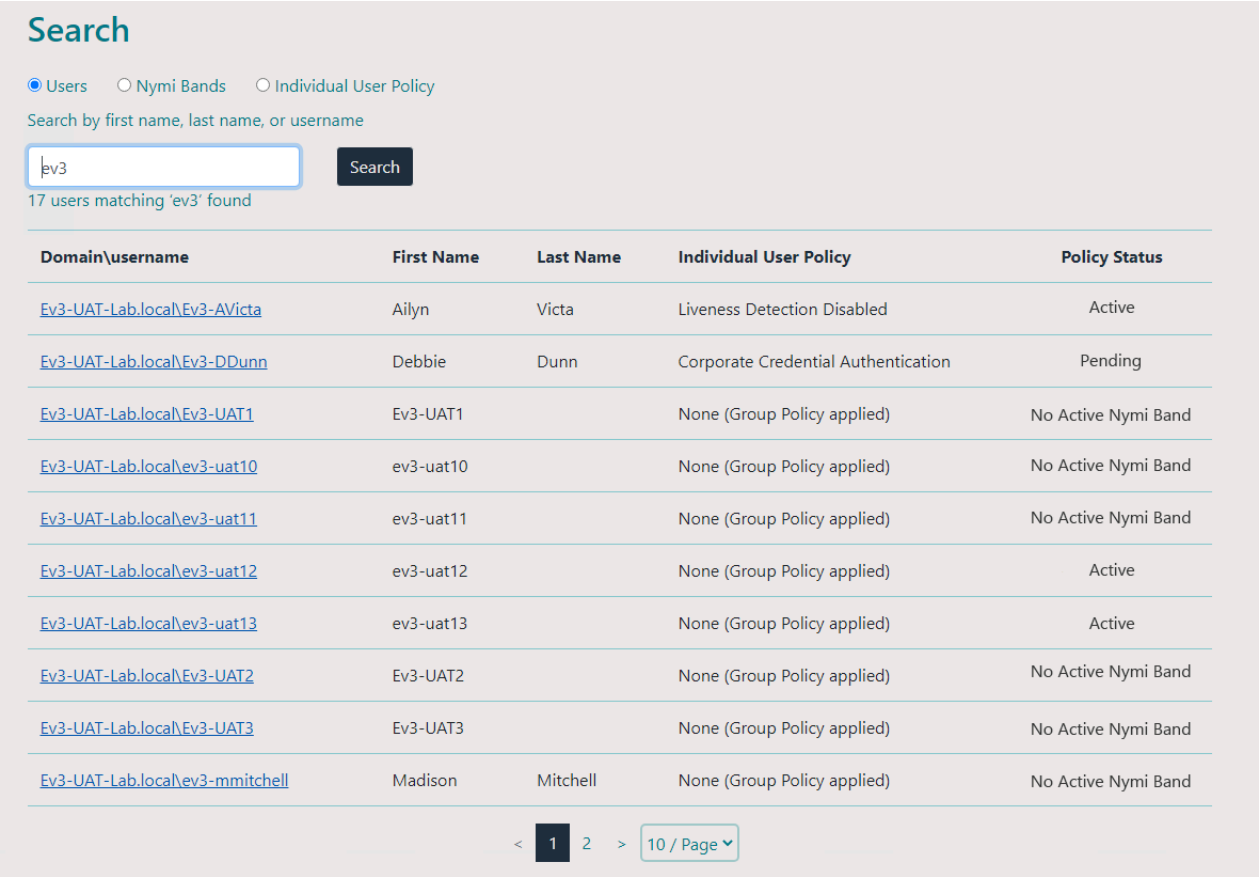


Figure 33: Users Search Results Page

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.

12.1.1.1 - 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.

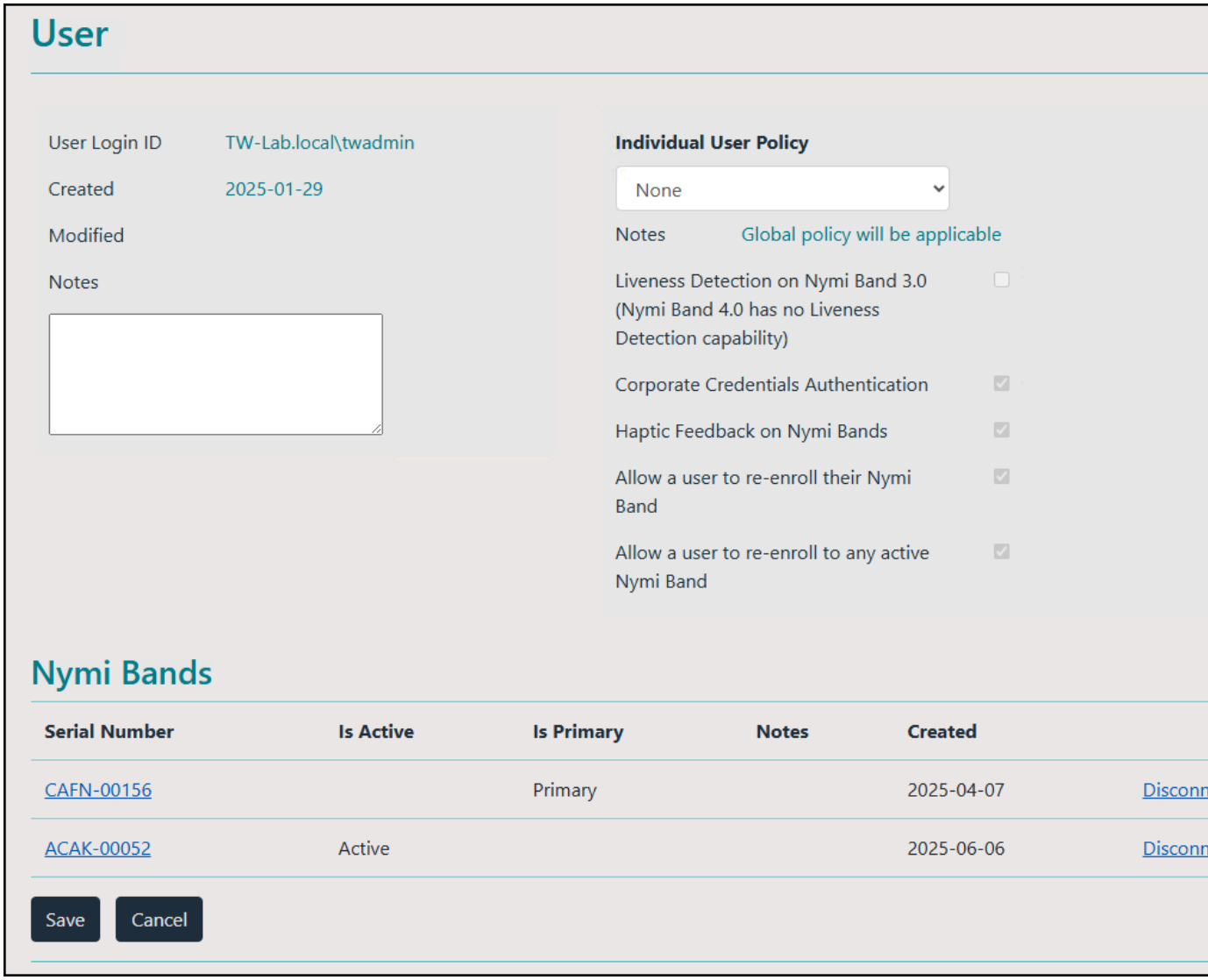


Figure 34: User Details Page

Table 5: 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.

Field	Description
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.

12.1.2 - 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.

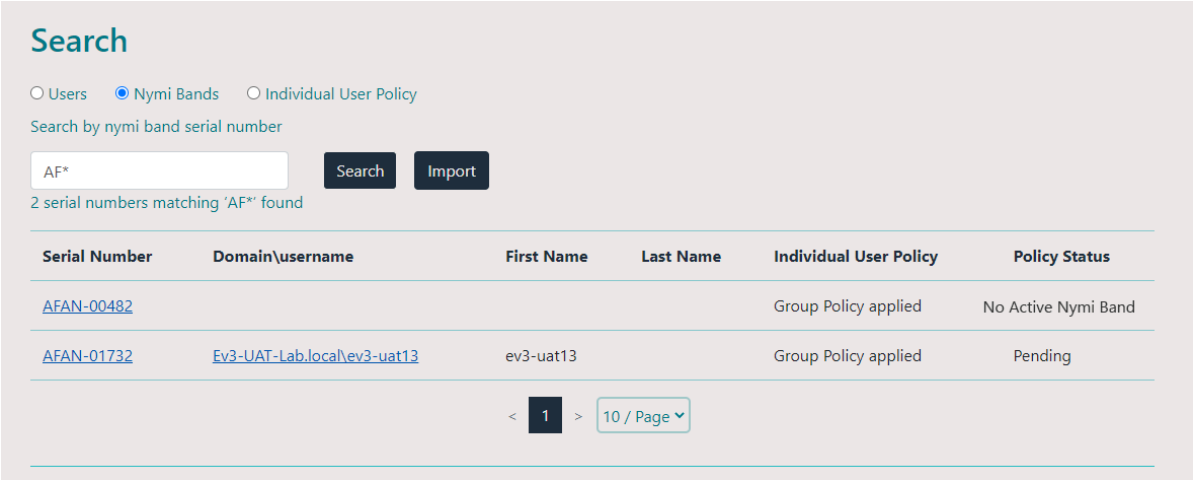


Figure 35: Nymi Band Search Results Page

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.

12.1.2.1 - Nymi Band Details Page

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

Table 6: 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. 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.
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 Nymi Enterprise Server(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**.
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**.

Field	Description
Band Label	Displays the Band Label assigned to the Nymi Band. Band Labels can only be assigned to Nymi Band, 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. 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 CWP 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 the informative message that a CWP Administrator entered about the Nymi Band.

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

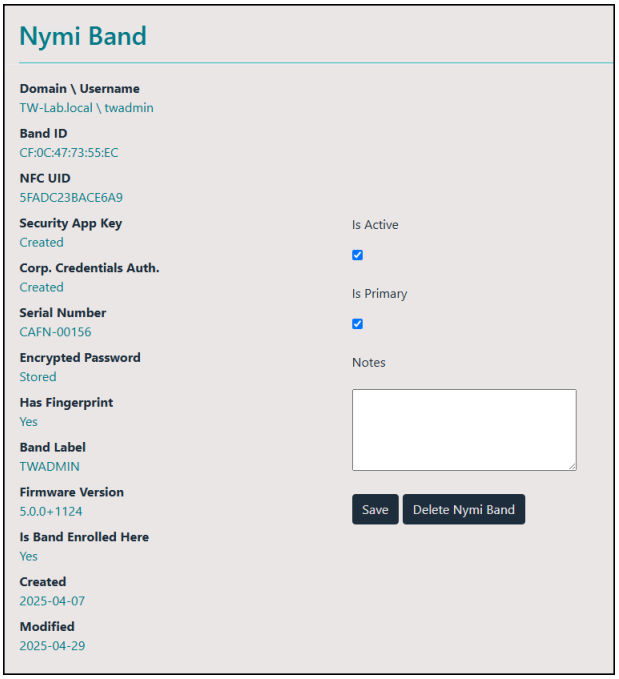


Figure 36: Nymi Band Details page

12.1.3 - 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.

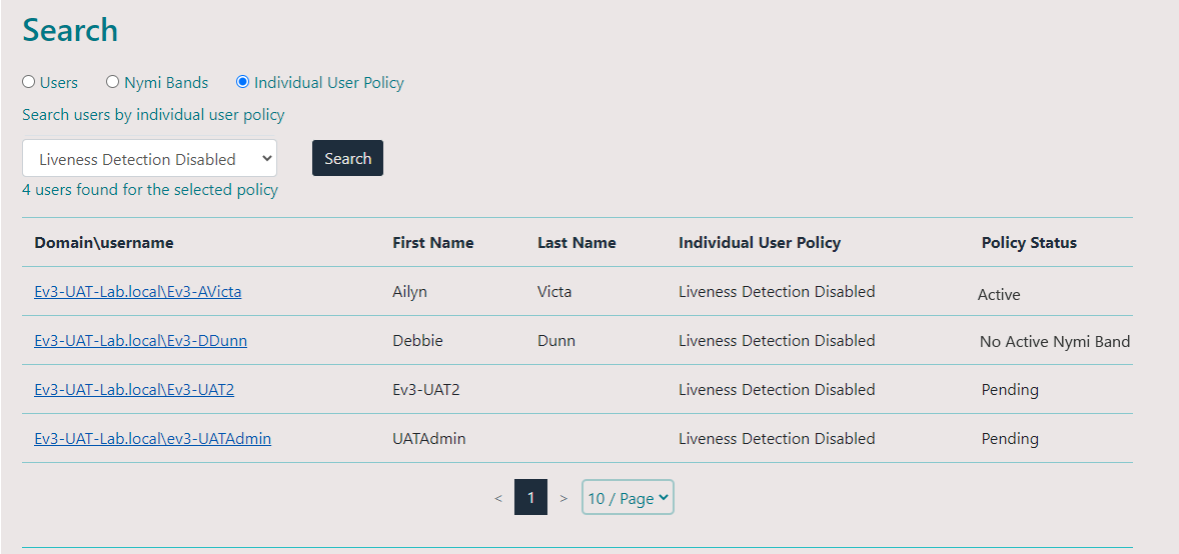


Figure 37: Individual User Policy Search Results

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.

12.2 - 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.

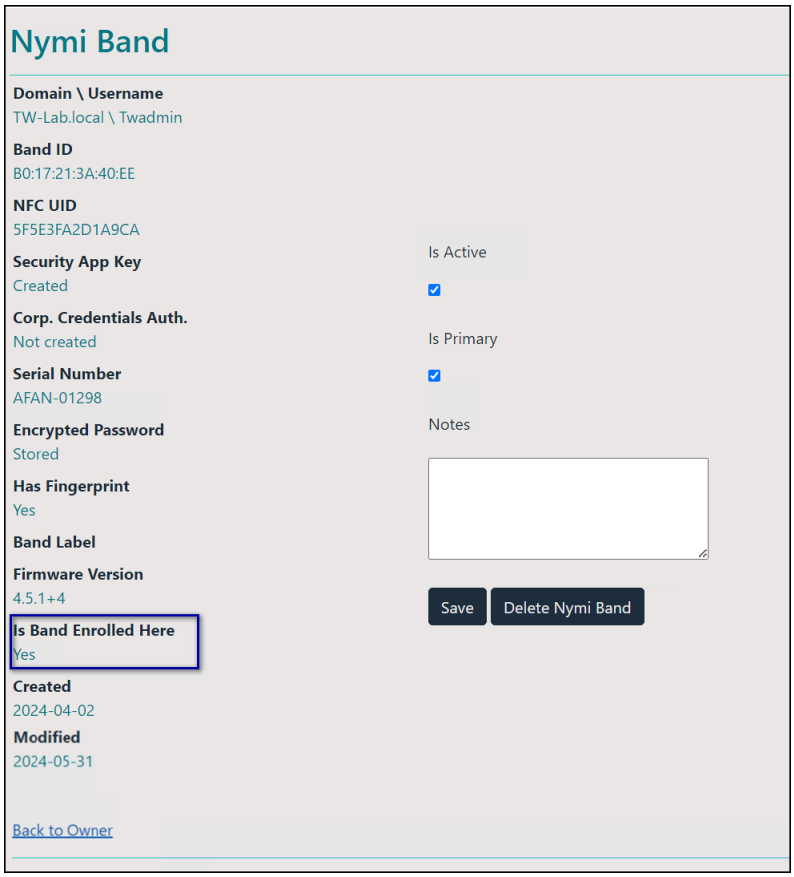


Figure 38: Nymi Band properties page

12.3 - 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.

12.3.1 - 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 in the *Nymi Connected Worker Platform—Administration Guide* 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. For Secure NFC only, you must blacklist and delete the RFID entry for the Nymi Band in the Evidian EAM Management Console.
3. 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.
4. 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.

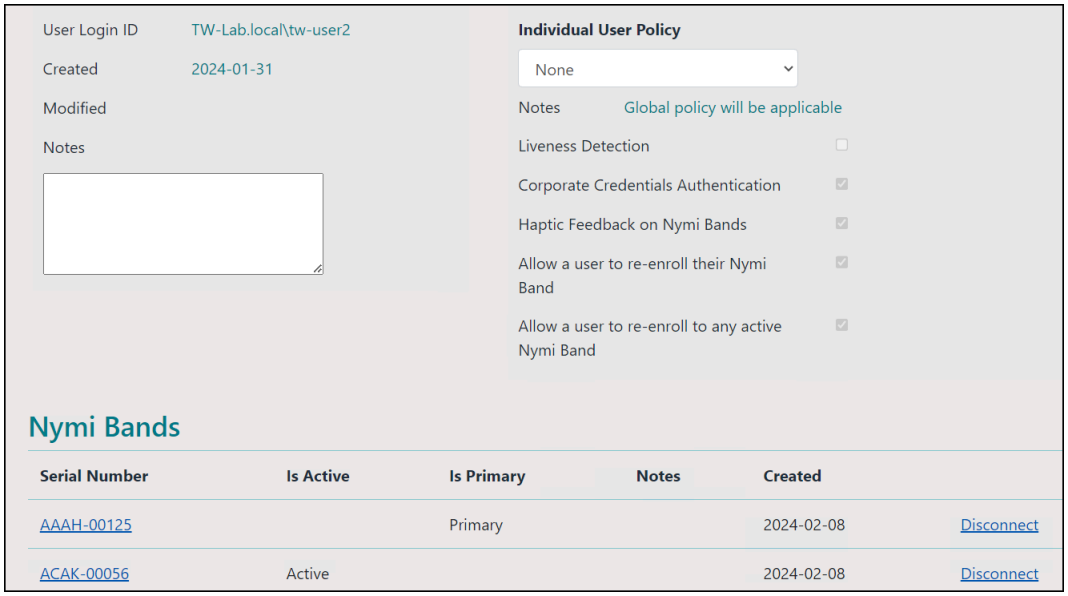


Figure 39: User with multiple Nymi Bands after self-service re-enrollment.

12.3.2 - 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.

12.3.2.1 - 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.

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 *Storage of NES Data*.

About this task

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

This process involves two main steps:

- Suspending or disassociating the user's existing Nymi Band.
- Enrolling the Nymi Band to the user.

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

12.3.2.2 - 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 Nymi Enterprise Server(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.

12.4 - 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 *Nymi Band User Guide* for more information about how to perform the Delete User Data process in the 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`**.

12.5 - 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 Nymi Enterprise Server(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**.

13 - 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.

13.1 - 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.

13.1.1 - 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.

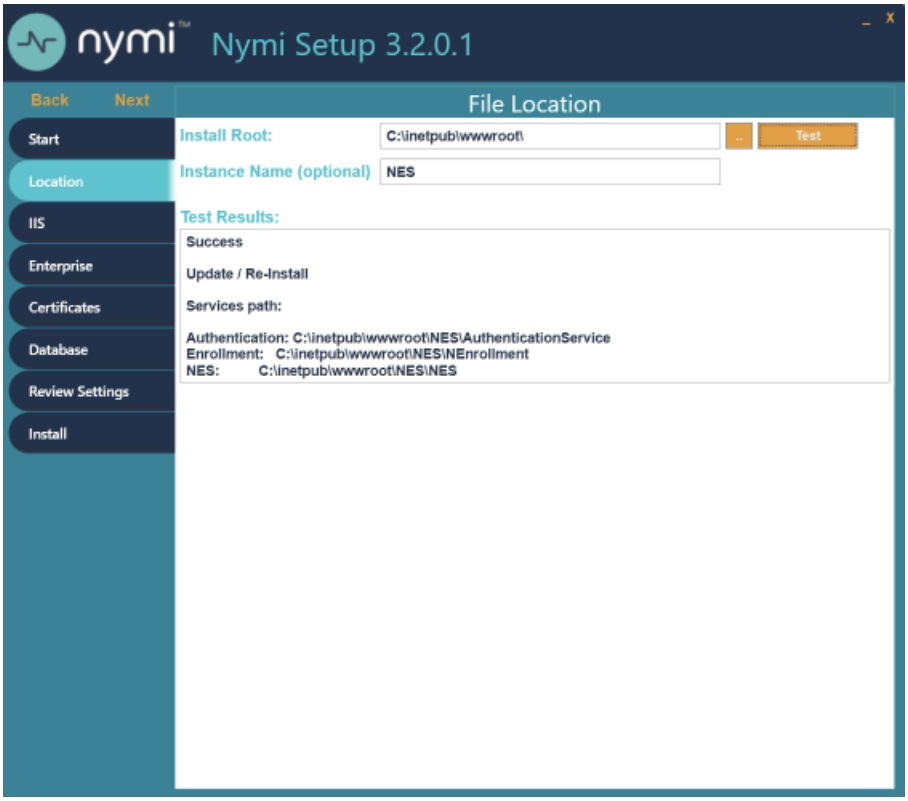


Figure 40: Update / Reinstall installation type

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.

13.1.2 - 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.

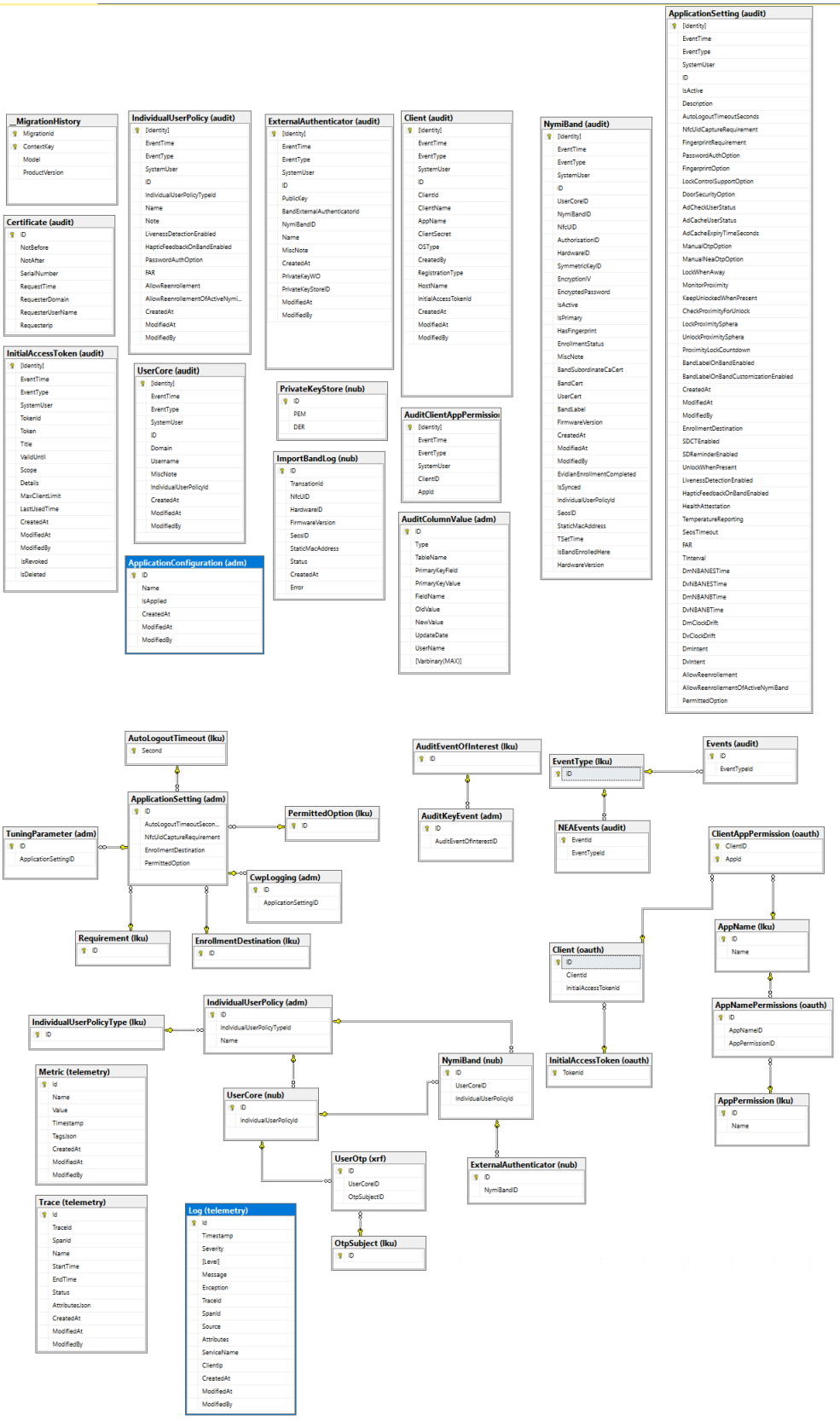

__MigrationHistory
MigrationId
ContextKey
Model
ProductVersion
IndividualUserPolicy (audit)
[Identity]
EventTime
EventType
SystemUser
ID
IndividualUserPolicyTypeId
Name
Note
LivenessDetectionEnabled
HapticFeedbackOnBandEnabled
PasswordAuthOption
FAR
AllowReenrollement
AllowReenrollementOfActiveNymi...
CreatedAt
ModifiedAt
ModifiedBy
ExternalAuthenticator (audit)
[Identity]
EventTime
EventType
SystemUser
ID
PublicKey
BandExternalAuthenticatorId
NymiBandID
Name
MiscNote
CreatedAt
PrivateKeyWO
PrivateKeyStoreID
ModifiedAt
ModifiedBy
Client (audit)
[Identity]
EventTime
EventType
SystemUser
ID
ClientId
ClientName
AppName
ClientSecret
OSType
CreatedBy
RegistrationType
HostName
InitialAccessTokenId
CreatedAt
ModifiedAt
ModifiedBy
NymiBand (audit)
[Identity]
EventTime
EventType
SystemUser
ID
UserCoreID
NymiBandID
NfcUID
AuthorisationID
HardwareID
SymmetricKeyID
EncryptionIV
EncryptedPassword
IsActive
IsPrimary
HasFingerprint
EnrollmentStatus
MiscNote
BandSubordinateCaCert
BandCert
UserCert
BandLabel
FirmwareVersion
CreatedAt
ModifiedAt
ModifiedBy
EvidianEnrollmentCompleted
IsSynced
IndividualUserPolicyId
SeosID
StaticMacAddress
TSetTime
IsBandEnrolledHere
HardwareVersion
ApplicationSetting (audit)
[Identity]
EventTime
EventType
SystemUser
ID
IsActive
Description
AutoLogoutTimeoutSeconds
NfcUidCaptureRequirement
FingerprintRequirement
PasswordAuthOption
FingerprintOption
LockControlSupportOption
DoorSecurityOption
AdCheckUserStatus
AdCacheUserStatus
AdCacheExpiryTimeSeconds
ManualOtpOption
ManualNeaOtpOption
LockWhenAway
MonitorProximity
KeepUnlockedWhenPresent
CheckProximityForUnlock
LockProximitySphera
UnlockProximitySphera
ProximityLockCountdown
BandLabelOnBandEnabled
BandLabelOnBandCustomizationEnabled
CreatedAt
ModifiedAt
ModifiedBy
EnrollmentDestination
SDCTEnabled
SDReminderEnabled
UnlockWhenPresent
LivenessDetectionEnabled
HapticFeedbackOnBandEnabled
HealthAttestation
TemperatureReporting
SeosTimeout
FAR
TInterval
DmNBANESTime
DvNBANESTime
DmNBANBTime
DvNBANBTime
DmClockDrift
DvClockDrift
DmIntent
DvIntent
AllowReenrollement
AllowReenrollementOfActiveNymiBand
PermittedOption
Certificate (audit)
ID
NotBefore
NotAfter
SerialNumber
RequestTime
RequesterDomain
RequesterUserName
RequesterIp
InitialAccessToken (audit)
[Identity]
EventTime
EventType
SystemUser
TokenId
Token
Title
ValidUntil
Scope
Details
MaxClientLimit
LastUsedTime
CreatedAt
ModifiedAt
ModifiedBy
IsRevoked
IsDeleted
UserCore (audit)
[Identity]
EventTime
EventType
SystemUser
ID
Domain
Username
MiscNote
IndividualUserPolicyId
CreatedAt
ModifiedAt
ModifiedBy
PrivateKeyStore (nub)
ID
PEM
DER
ImportBandLog (nub)
ID
TransationId
NfcUID
HardwareID
FirmwareVersion
SeosID
StaticMacAddress
Status
CreatedAt
Error
AuditClientAppPermissio
[Identity]
EventTime
EventType
SystemUser
ClientID
AppId
AuditColumnValue (adm)
ID
Type
TableName
PrimaryKeyField
PrimaryKeyValue
FieldName
OldValue
NewValue
UpdateDate
UserName
[VarbinaryMAX]
ApplicationConfiguration (adm)
ID
Name
IsApplied
CreatedAt
ModifiedAt
ModifiedBy
AutoLogoutTimeout (lku)
Second
ApplicationSetting (adm)
ID
AutoLogoutTimeoutSecon...
NfcUidCaptureRequirement
EnrollmentDestination
PermittedOption
PermittedOption (lku)
ID
TuningParameter (adm)
ID
ApplicationSettingID
CwpLogging (adm)
ID
ApplicationSettingID
Requirement (lku)
ID
EnrollmentDestination (lku)
ID
AuditEventOfInterest (lku)
ID
AuditKeyEvent (adm)
ID
AuditEventOfInterestID
EventType (lku)
ID
Events (audit)
ID
EventTypeId
NEAEvents (audit)
EventId
EventTypeId
ClientAppPermission (oauth)
ClientID
AppId
AppName (lku)
ID
Name
Client (oauth)
ID
ClientId
InitialAccessTokenId
AppNamePermissions (oauth)
ID
AppNameID
AppPermissionID
AppPermission (lku)
ID
Name
InitialAccessToken (oauth)
TokenId
IndividualUserPolicyType (lku)
ID
IndividualUserPolicy (adm)
ID
IndividualUserPolicyTypeId
Name
NymiBand (nub)
ID
UserCoreID
IndividualUserPolicyId
Metric (telemetry)
Id
Name
Value
Timestamp
TagsJson
CreatedAt
ModifiedAt
ModifiedBy
UserCore (nub)
ID
IndividualUserPolicyId
UserOtp (xrf)
ID
UserCoreID
OtpSubjectID
ExternalAuthenticator (nub)
ID
NymiBandID
Trace (telemetry)
Id
TraceId
SpanId
Name
StartTime
EndTime
Status
AttributesJson
CreatedAt
ModifiedAt
ModifiedBy
Log (telemetry)
Id
Timestamp
Severity
[Level]
Message
Exception
TraceId
SpanId
Source
Attributes
ServiceName
ClientIp
CreatedAt
ModifiedAt
ModifiedBy
OtpSubject (lku)
ID

Table 7: 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 setting in the policy.
adm.AuditColumnValue	Legacy table.
adm.AuditKeyEvent	Legacy table.
adm.CwpLogging	Contain master data which NES writes to a Nymi Band.
adm.IndividualUserPolicy	Contains a entry for each individual user policy and the values that are currently assigned to each setting in the policy.
adm.TuningParameter	Contains master data which NES writes to a Nymi Band.
nub.ExternalAuthenticator	Contains an entry for Nymi Band that contains an external authenticator.
nub.ImportBandLog	
nub.NymiBand	Contains current information about each Nymi Band that has been enrolled on the NES server. The columns are identical to the audit.NymiBand table.
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. The columns are identity to the audit.UserCore table.

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 8: lku schema

Table Name	Purpose
lku.AppName	Defines a list of Nymi-Enabled Applications (NEAs) that participate in OAuth and register as clients. In this release, the only supported application is Nymi Connect for Android.
lku.AppPermission	Defines all supported permission scopes for an NEA.
lku.AuditEventsOfInterest	Legacy option.
lku.AutoLogoutTimeout	Displays a acceptable values for the **`Auto Logout Timer`** setting in a group policy.
lku.EnrollmentDestination	Defines a list of acceptable values for the **`Enrollment Destination`** setting in a group policy.
lku.IndividualPolicyType	Defines a list of acceptable values for the **`Enrollment Destination`** setting in an individual user policy.
lku.OtpSubject	Legacy option.
lku.Requirement	Defines a list of acceptable values for the **`NfcUIDCapture`** setting.
lku.AuditLogoutTimeout	Defines a list of acceptable values for the **`Auto Logout Timeout`** setting.
lku.EventType	Defines a list of acceptable values for events.
lku.Requirement	Legacy option.

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, oauth, 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 9: 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 10: 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 Administrator 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 11: 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.
HardwareVersion	Version of the Nymi Band. Values that can appear: • NULL—Undetermined, instruct the user to log into Nymi Band Application while wearing their authenticated Nymi Band to update the value in the SQL database. • 10.00—Nymi Band 3 • 14.00 or greater—Nymi Band 4

`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 12: 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.
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.

Column Name	Description
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.
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.

Column Name	Description
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.
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.

Column Name	Description
TInterval	Used for authenticated Bluetooth tap operations. The time interval for PAC message rotation. Default: 1 second
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 NES 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 NES 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 NES 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 NES Administrator to first disassociate the Nymi Band for the user.

audit.ExternalAuthenticator SQL Schema

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

Table 13: 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 14: 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 15: 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 individual user policy was created on the Nymi Band. • U—when the properties of individual user policy was updated. • D—when the individual user policy was deleted on the Nymi Band.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	Unique identifier for the schema entry.
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 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.
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.

`audit.client Schema`

Stores information about clients that were dynamically registered in NES with an intial access token (IAT), which is also known as a client registration token (CRT). Each attribute name that is listed in the Column Name is prefaced with Identity.

Table 16: audit.client 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 client was created in the NES. • U—when the client was updated in NES • D—when the client was deleted in NES.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	Identifier in the oauth.client table.
ClientID	Unique identifier that NES assigned to the client.
ClientName	Logical name of the device as defined by Nymi Connect at the time of registration.
AppName	Name of Nymi application that runs on the device, for example Nymi Connect.
ClientSecret	Randomly generated secure secret key which NES and the client use for token requests.
OSType	Operating system of the client. For example, Linux, Windows, Android, and MacOS
CreatedBy	Machine name of the NES server that performed the client registration.
RegistrationType	Type of client registration. In this release, NES only supports dynamic client registrations.
HostName	Host name or device name of the client.
InitialAccessTokenID	Hashed copy of the client registration token that Nymi Connect used to register the client.
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.

audit.InitialAccessToken Schema

Stores information about client registration tokens (CRTs)in NES. Each attribute name that is listed in the Column Name is prefaced with Identity.

Table 17: audit.IntialAccessToken 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	• C—when the CRT was created in NES Administrator Console. • U—when the CRT was modified in the NES Administrator Console. • R—when the CRT was revoked in NES Administrator Console. • D—when the CRT was deleted in the NES Administrator Console.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
TokenID	Unique identifier that NES assigned to the CRT.
Token	Hashed copy of the client registration token.
Title	User-defined title of the CRT.
ValidUntil	Expiration date and time of the CRT.
Scope	Application associated with the CRT. Values include: • 2—Nymi Connect for Android
Details	User-defined notes about the CRT.
MaxClientLimit	User-defined value that defines how many devices can use the CRT to register with NES. A value of 0 means that there is no limit on the number of devices that can use the CRT.
LastUsedTime	Date of the last time a client used the CRT to register with NES.
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.
IsRevoked?	Status of validity of the CRT. Values that can appear: • 0—Token is valid. • 1—Token is revoked.

Column Name	Description
IsDeleted?	Status of the presence of the CRT in the NES Administrator Console. Values that can appear: • 0—Token appears in NES Administrator Console. • 1—Token deleted from NES Administrator Console.

oauth Schema

Transactional tables that contain current information for each registered client and each client registration token.

Table 18: oauth schema

Table Name	Purpose
oauth.Client	Stores information about all registered OAuth clients, including Nymi Connect for Android devices.
oauth.ClientAppPermission	Defines which permissions (scopes) each registered client receives from NES.
oauth.InitialAccessToken	Stores Client Registration Tokens (CRT) that NES uses to perform dynamic client registrations.

Telemetry Schema

Transactional table that contains the information about audit events, such as Nymi Band taps that occur on devices that use Nymi Connect.

Table 19: Telemetry.log Schema

Field	Description
ID	Unique identifier for the schema entry.
TimeStamp	Date and time that the log event was recorded in UTC timezone format.
Severity	Severity level of the log event. Values that can appear: • Error • Warning • Information
[Level]	Application-defined level or category for the log event. Values that can appear: • Error • Warning • Information

Field	Description
Message	Description of the log event.
Exception	For logs events that have an Error severity level, contains exception details or stack trace. For log events that have a Warning of Information severity level, the value is NULL.
TraceId	Placeholder for future functionality, in this release the value that appears in NULL.
SpanId	Placeholder for future functionality, in this release the value that appears in NULL.
Source	Name of the component or subsystem that generated the log event. For example, JWTAuthenticationFilter and ClientRegService.

Field	Description

Attributes	JSON-formatted object that contains contextual data that is related to the log event. Data includes:
	• ClientName
	• AppName
	• HostName
	• OSType
	• EventType
	• EventTime—The date and time when the event happened on the client device in the UTC format [YYYY]-[MM]-[DD]T[hh]:[mm]:[ss.sss]z.
	For example, 2025-10-20T22:54:t6.365Z
	• Category—The category of the event. In this release the only value is *Audit*.
	• SubCategory—The sub-category of the event. Values that can appear:
	  • Authentication
	  • Registration
	• Producer—The application or service responsible that generated the audit event. In this release the only value is *NCA* (Nymi Connect for Android
	• ProducerVersion—The version of the Nymi Connect for Android component or client application that generated the event.
	• OSType—Operating system on which the event originated. In this release, the only value that appears in *Android*
	• HostId—AndroidId of the device from which the event originated.
	• UserId—Identity of the user who initiated the authentication or event, in the format *domain\username*.
	• AuthenticatorId—Primary authenticator identifier that was used during the event. This identifier represents the device or technology that was used to perform user validation. For example:
	  • BLE_MAC_00:1A:7D:DA:71:13— BLE-based Nymi Band MAC address.
	  • NFC_3B8F7E2100—NFC tag identifier.
	  • RFID_7A45C923—RFID card ID.
	• SecondaryAuthenticatorId—Identifier that provides additional verification context, for example, when the event involves multiple authentication factors.
	• AppProcessName—Identifies which process performed the authentication or triggered the audit log. For example:
	  • chrome.exe—Chrome browser
	  • msedge.exe—Edge browser
	• AppURL—URL of the web application in which the user performed the authentication event.
	• AppWinTitle—Title of the application window in which the user performed the authentication event.
	• TotalElapsedTime—Time in milliseconds that elapsed during the operation or event.
	• Details

Field	Description
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.
ClientIp	IP address of the client device.

13.1.3 - 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.

13.1.4 - 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`**.

Display list of all currently enrolled users

The Nymi.**instance_name**.nub.UserCore schema contains current information that is specific the users in the CWP environment. The Nymi.**instance_name**.nub.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 current details about a user and their associated Nymi Band.

To retrieve information from the Nymi.**instance_name**.nub.UserCore and Nymi.**instance**.nub.NymiBand tables and display information about the current 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.[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].[nub].[NymiBand] AS nb
JOIN [Nymi.NES].[nub].[UserCore] AS uc
ON nb.UserCoreID = uc.ID
WHERE nb.IsActive = '1'
```

Viewing all Nymi Connect for Android user activity information for a specific user in the Telemetry log

You can view all information in the database for activities that were performed in Nymi Connect for Android user by following these steps:

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.

   Note: In the *Where* statement, replace *username* with the actual username of your user.

```
SELECT
l.[Id],
l.[Timestamp],
l.[Severity],
l.[Level],
l.[Message],
l.[ServiceName],
l.[ClientIp],
-- Extract JSON Attributes
JSON_VALUE(l.[Attributes], '$.EventTime') AS EventTime,
JSON_VALUE(l.[Attributes], '$.Category') AS Category,
JSON_VALUE(l.[Attributes], '$.SubCategory') AS SubCategory,
JSON_VALUE(l.[Attributes], '$.EventType') AS EventType,
JSON_VALUE(l.[Attributes], '$.Producer') AS Producer,
JSON_VALUE(l.[Attributes], '$.OSType') AS OSType,
JSON_VALUE(l.[Attributes], '$.HostId') AS HostId,
JSON_VALUE(l.[Attributes], '$.UserID') AS UserID,
JSON_VALUE(l.[Attributes], '$.AuthenticatorId') AS AuthenticatorId,
JSON_VALUE(l.[Attributes], '$.SecondaryAuthenticatorId') AS
SecondaryAuthenticatorId,
JSON_VALUE(l.[Attributes], '$.AppProcessName') AS AppProcessName,
JSON_VALUE(l.[Attributes], '$.AppURL') AS AppURL,
JSON_VALUE(l.[Attributes], '$.AppWinTitle') AS AppWinTitle,
JSON_VALUE(l.[Attributes], '$.TotalElapsedTime') AS TotalElapsedTime,
JSON_VALUE(l.[Attributes], '$.Details') AS Details,

-- From UserCore and NymiBand tables
uc.[Domain],
```

```
                uc.[Username],
                nb.[NymiBandID],
                nb.[NfcUID],
                nb.[FirmwareVersion],
                nb.[IsActive]
                FROM [telemetry].[log] AS l
                JOIN [nub].[NymiBand] AS nb
                ON nb.[NymiBandID] = JSON_VALUE(l.[Attributes], '$.AuthenticatorId')
                OR nb.[NymiBandID] = JSON_VALUE(l.[Attributes],
'$.SecondaryAuthenticatorId')
                JOIN [nub].[UserCore] AS uc
                ON uc.[ID] = nb.[UserCoreID]
                WHERE uc.[Username] = 'username'
                ORDER BY l.[Timestamp] DESC;
```

Viewing all Nymi Connect for Android activity information for a specific Nymi Band in the Telemetry log

You can view all information in the database for activities that were performed with a specific Nymi Band in Nymi Connect for Android by following these steps:

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.

   Note: In the *Where* statement, replace *band_id* with the actual band ID value for the Nymi Band.

```
        SELECT
        l.[Id],
        l.[Timestamp],
        l.[Severity],
        l.[Level],
        l.[Message],
        l.[ServiceName],
        l.[ClientIp],

        -- Extract JSON Attributes

        JSON_VALUE(l.[Attributes], '$.EventTime') AS EventTime,
        JSON_VALUE(l.[Attributes], '$.Category') AS Category,
        JSON_VALUE(l.[Attributes], '$.SubCategory') AS SubCategory,
        JSON_VALUE(l.[Attributes], '$.EventType') AS EventType,
        JSON_VALUE(l.[Attributes], '$.Producer') AS Producer,
        JSON_VALUE(l.[Attributes], '$.OSType') AS OSType,
        JSON_VALUE(l.[Attributes], '$.HostId') AS HostId,
        JSON_VALUE(l.[Attributes], '$.UserID') AS UserID,
        JSON_VALUE(l.[Attributes], '$.AuthenticatorId') AS AuthenticatorId,
        JSON_VALUE(l.[Attributes], '$.SecondaryAuthenticatorId') AS
SecondaryAuthenticatorId,
        JSON_VALUE(l.[Attributes], '$.AppProcessName') AS AppProcessName,
        JSON_VALUE(l.[Attributes], '$.AppURL') AS AppURL,
        JSON_VALUE(l.[Attributes], '$.AppWinTitle') AS AppWinTitle,
        JSON_VALUE(l.[Attributes], '$.TotalElapsedTime') AS TotalElapsedTime,
        JSON_VALUE(l.[Attributes], '$.Details') AS Details,

        -- From UserCore and NymiBand
```

```
uc.[Domain],
uc.[Username],
nb.[NymiBandID],
nb.[NfcUID],
nb.[FirmwareVersion],
nb.[IsActive]
FROM [telemetry].[log] AS l
JOIN [nub].[NymiBand] AS nb
ON nb.[NymiBandID] = JSON_VALUE(l.[Attributes], '$.AuthenticatorId')
OR nb.[NymiBandID] = JSON_VALUE(l.[Attributes], '$.SecondaryAuthenticatorId')
JOIN [nub].[UserCore] AS uc
ON uc.[ID] = nb.[UserCoreID]
WHERE nb.[NymiBandID] = 'band_id'
ORDER BY l.[Timestamp] DESC;
```

14 - 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.

14.1 - Enrollment Terminal Log Files

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

14.1.1 - 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`**.

14.1.2 - 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.

14.2 - 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.

14.3 - 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.

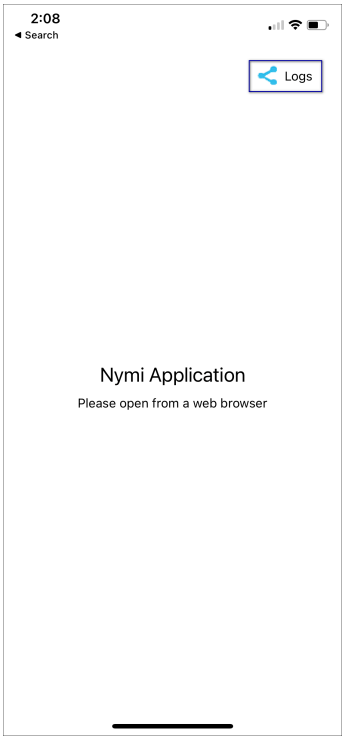


Figure 42: Nymi Application Logs

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.

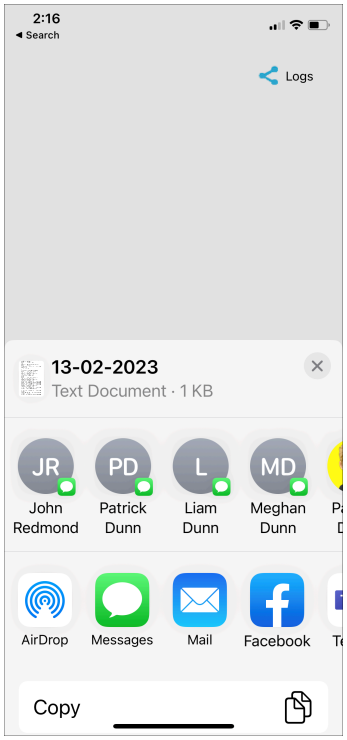


Figure 43: Nymi Application Send Options

To disable logging, navigate to **`Settings > Nymi`**, and then toggle **`Logs`** to the off position, as shown in the following figure.

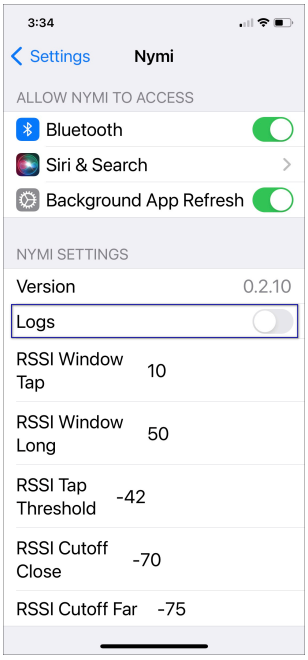


Figure 44: Disabling Nymi Application Logging

14.4 - 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.

14.5 - (CWP 1.17.0 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.

14.5.1 - (CWP 1.17.0 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\nes\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.

14.5.2 - 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*

14.5.3 - 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.

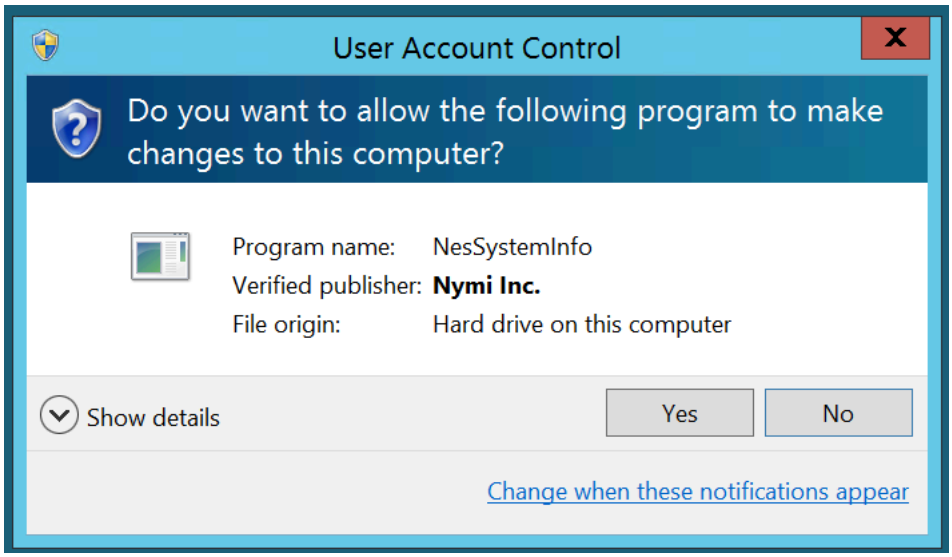


Figure 45: The User Account Control

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.

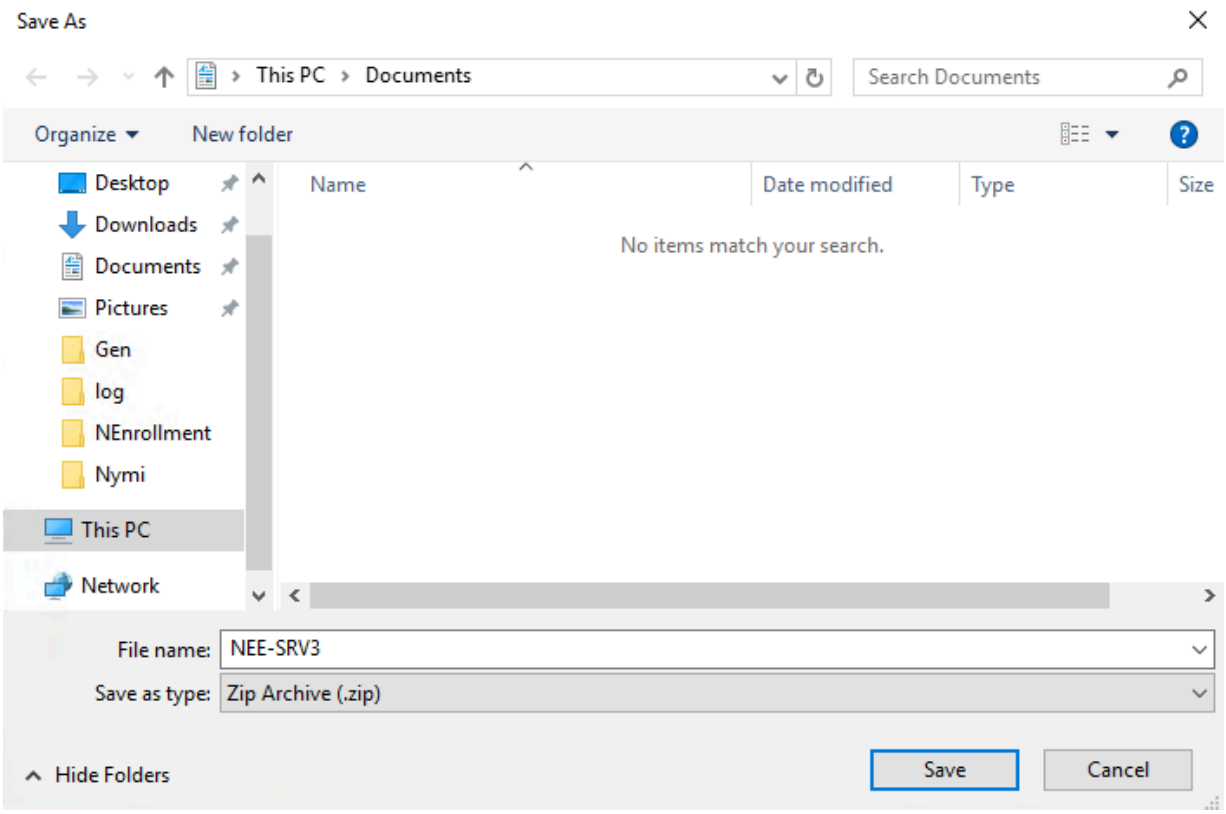


Figure 46: Saving Nymi Support Tool zip

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.

14.6 - Nymi Band Firmware Logs

About this task

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

Procedure

1. Place the Nymi Band on charge while connected to a user terminal, and then move the Nymi Band and the charger close to the Bluegiga Bluetooth adapter  . This ensure that the retrieval tool retrieves logs files 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 you installed the Nymi Band Application on the user terminal, 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.

14.7 - 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.

15 - Manage the Connected Worker Platform Environment

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

15.1 - Manage NES

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

15.1.1 - 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`**.

15.1.2 - 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.

15.1.2.1 - 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.

15.1.2.2 - 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.

15.1.2.3 - 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.

15.1.3 - 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.

15.1.3.1 - 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**.

15.1.3.2 - 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**.

15.1.3.3 - 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.

15.1.4 - Adding and Removing NES Administrator Access

Membership in Active Directory group controls the user accounts that have administrator access to the NES Administrator Console. You define the group name during the deployment of the Nymi Enterprise Server(NES) software.

Before you begin

To determine the Windows group that was defined during the NES deployment, 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 access for a user.

Procedure

1. Log in to a domain controller as an administrator.
2. Edit the AD group.
3. Add or remove the users and groups, as required.
4. Save the group.

15.1.5 - 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.

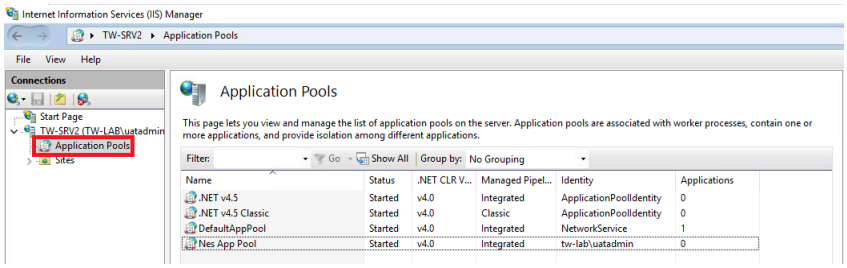


Figure 47: IIS Application Identity Pools

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`**

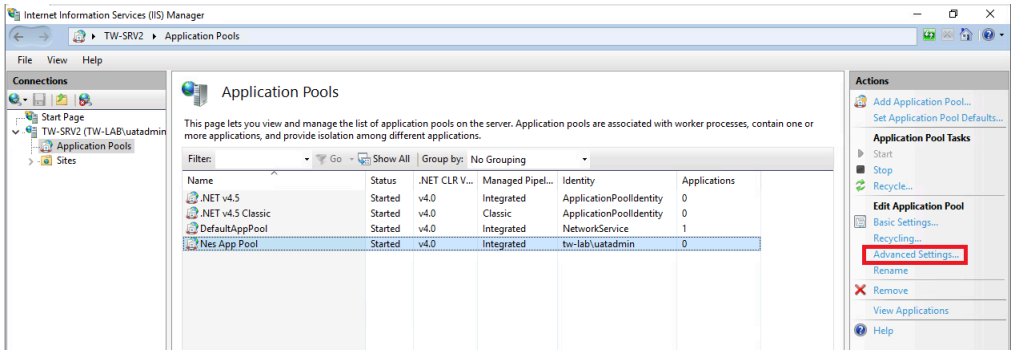


Figure 48: IIS Application Identity Advanced Settings

5. On the `Advanced Settings` window, select **`Identity`**, and then click the ellipses.

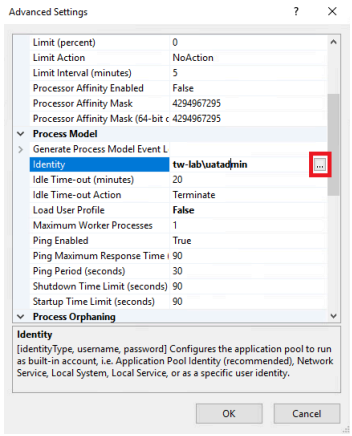


Figure 49: IIS Application Identity Advanced Settings

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.

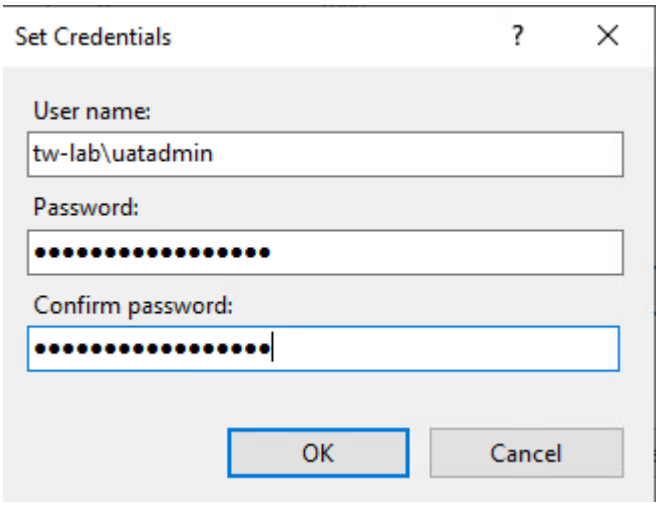


Figure 50: Set Credentials window

15.1.6 - Updating the Domain List

Run the Nymi Enterprise Server(NES) installation wizard to update the list of Active Directory domains that contain users who have the ability to enroll Nymi Bands or access the NES Administrator Console.

About this task

Perform the following steps on the NES with the account that you used to perform the NES deployment.

Procedure

1. From the directory that contains the extracted NES installation package, run *..\NesInstaller \install.exe.*
2. On the `User Access Control` window, click **`Yes`**.
3. On the `Open File - Security warning` window, click **Run**.
4. 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.
5. On the `Application Install Security Warning` window, click **`Install`**.
6. On the `Open File - Security warning` window, click **Run**.
7. If the `Install Prerequisites` dialog appears and prompts to you install SQL Express, click **`No`**.
8. 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.

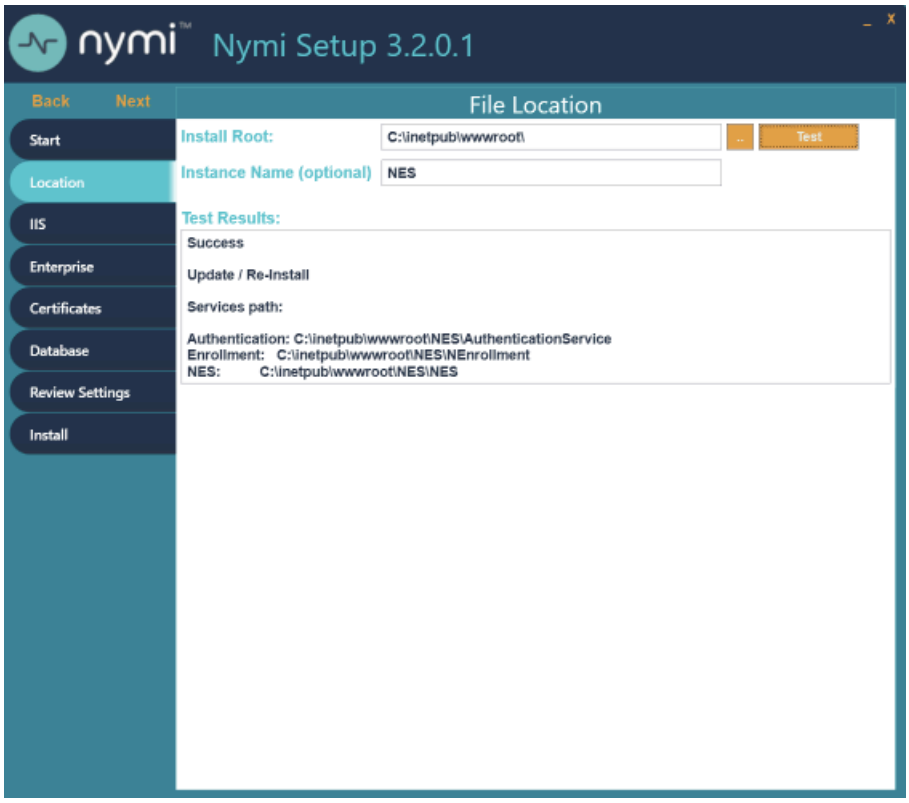


Figure 51: Update / Reinstall installation type

9. On the `Enterprise` tab, perform the following actions:
   a. In the **`Domain`** table, on an empty line, type the NetBIOS (Pre-Windows 2000) name of the domain that contains the user accounts. Refer to *Appendix—Record the CWP Variables* for your NetBIOS domain name.
   b. Type a domain username and password for the domain if the one of following conditions are met:
      - The domain is not in the same forest as the NES domain.
      - A two-way trust does not exist between the domain and the domain in which NES resides.
      - The domain is not in the same forest as the NES domain and does not have a two-way trust with the domain in which the NES service account resides.

      Note: Select a domain user whose password never expires.
   c. Press **`Enter`**.
   d. Press **`Test`** to confirm that NES can reach all domains.

10. In the left navigation pane, click `Review Settings`. The parameters for the NES installation are displayed for final review. Click **`Test`** to verify the configuration. Review the test results and address any errors if applicable.
11. On the `Install` tab, click **`Apply Settings`**.
12. When the installation completes, perform one of the following actions:
    a) Close the `NES Setup` wizard.
    b) Click **`Export Settings`** to save the NES configuration settings for future deployments.
    The section *Saving the NES configuration for silent installations* provides more information.

15.2 - 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.

15.2.1 - 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 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.

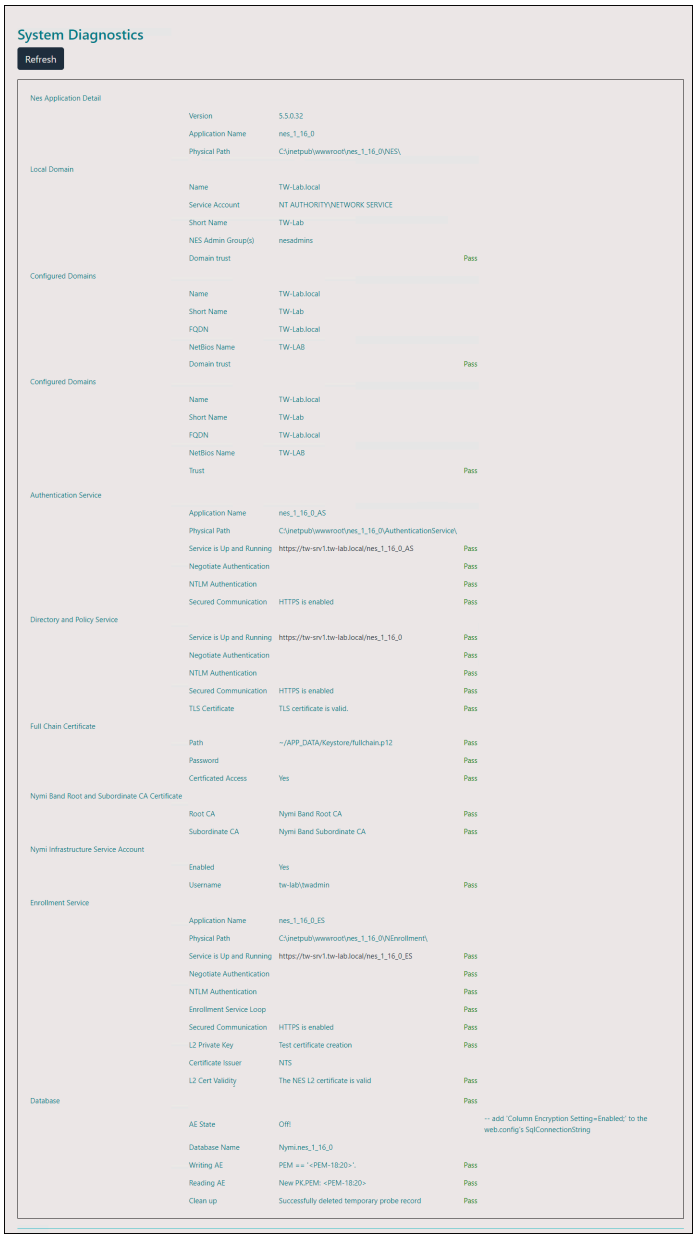


Figure 52: System Diagnostic Tests

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.

15.2.2 - 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 20: 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 21: 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 22: 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 23: 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 24: 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 25: 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 26: 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.

16 - 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.

16.1 - 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.

16.2 - 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`**.

16.3 - 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`**.

16.4 - 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.

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