

Administration Guide

Nymi Connected Worker Platform

v5.0

2021-05-03

Contents

- Preface..... 6**

- Overview.....8**
 - Connected Worker Platform Components.....8
 - Nymi Band 3.0.....11
 - Nymi Lock Control.....13
 - NFC support.....13
 - Nymi-Verified NFC Readers.....13
 - Configuring Unverified NFC Readers.....14
 - Bluetooth Adapter Placement.....14
 - Nymi Band Enrollment Process.....15
 - Authentication After Enrollment.....15

- Plan Your Configuration.....17**
 - Minimum requirements for the Nymi Band Application.....17
 - Minimum Requirements for Nymi Lock Control.....17
 - Authentication method.....18
 - One-time password (OTP) for Nymi application certificates.....18

- Checklist for Nymi Band Distribution and Enrollment.....20**

- Install Nymi Applications and Configure the User Terminals..... 21**
 - User terminal for Nymi Band Enrollment.....21
 - Nymi Band Application Installation.....21
 - Setting the NES URL.....22
 - User terminal for NEAs.....22
 - Prepare User terminals for Nymi-enabled Applications.....23
 - Install Nymi Runtime.....25
 - Install and Configure Nymi Lock Control.....26
 - Install Nymi Runtime.....31
 - User terminal for NES administration.....32

- Connect to NES for the First Time.....33**
 - Accessing NES Administrator Console.....33

Configure a Group Policy.....	34
Modifying the default group policy.....	34
Creating a new policy.....	38
Customizing the Nymi Band Application certificate creation.....	39
Updating the Nymi Band with Group Policy Changes.....	42
Nymi Band Enrollment.....	43
Assigning the Nymi Band to the Enterprise.....	43
Fingerprint Capture.....	44
Assigning the Band Label.....	46
Preview Band Label.....	47
Customize Band Label.....	47
Applying Policy Settings.....	49
Completing Enrollment.....	50
Interacting with the Nymi Band.....	51
Viewing Nymi Band Text.....	51
Viewing Nymi Band Screens.....	51
Viewing the Band Label.....	53
Nymi Band Dashboard.....	54
Nymi Band Vibration.....	55
Tapping the Nymi Band.....	55
Using Nymi Lock Control.....	57
Confirming Nymi Lock Control Recognizes the Nymi Band.....	57
Unlocking with an NFC or BLE Tap.....	58
Unlocking with Nymi Credential Provider.....	58
Unlocking a Nymi Lock Control User Terminal Without a Nymi Band.....	59
Locking the User Terminal.....	60
Stopping Nymi Lock Control.....	60
Nymi Band Management.....	61
Removing the Nymi Band.....	61
Storing the Nymi Band.....	61
Charging the Nymi Band.....	61
Managing Battery Life.....	63
Exiting Sleep Mode.....	63
Authenticating User Identity to the Nymi Band.....	64
Authentication by fingerprint.....	64
Authentication by corporate credentials.....	65
Cleaning the Nymi Band.....	65

Restarting the Nymi Band.....	66
Nymi Band Firmware Update Utility.....	66
Determining Nymi Band Firmware Version.....	67
Before you perform a firmware update.....	67
Updating Nymi Band Firmware Overview.....	68
Firmware updater log files.....	68
Administrative Actions.....	70
Policy Management.....	70
Editing policies.....	70
Changing the active policy.....	70
Deleting policies.....	70
Nymi Band User Management.....	71
NFC (Unique Identifier) UID Management.....	71
Searching for User or Nymi Band Information.....	71
Issuing a temporary Nymi Band to a user.....	76
Restoring the Nymi Band.....	77
Replacing the Nymi Band for a user.....	77
Suspending the primary Nymi Band for a user.....	78
Disconnecting the Nymi Band from a user in NES.....	79
Deleting User Data.....	79
Reassigning a Nymi Band.....	79
Resetting an Expired Password.....	80
NES Audit Logging.....	82
Viewing all Audit Log data using SQL Queries.....	82
Viewing audit tables.....	83
Querying audit tables.....	83
Log Files.....	84
Nymi Band Application log files.....	84
Saving Nymi Band Application log files.....	84
Viewing Nymi Band Application log files.....	84
NES log files.....	84
Enabling debug mode.....	84
NES web service log file locations.....	85
Submitting a support request.....	86
Nymi Support Tool.....	86
Manage the Connected Worker Platform Environment.....	88
Manage NES.....	88
NES Backup and Recovery.....	88
Upgrading NES.....	88

Uninstalling NES Installer.....	90
System Diagnostics.....	91
Accessing NES Administrator Console.....	91
System Diagnostics Information.....	91
Certificate Management.....	94
Check certificate expiration dates.....	94
Renewing the L2, L1, and Root Certificates.....	97
Manage Nymi Band Application and Nymi Runtime.....	101
Upgrading the Nymi Band application.....	101
Performing a silent Nymi Band application installation or upgrade.....	101
Performing a Nymi Band application upgrade by using the installation wizard.....	101
Uninstalling the Nymi Band Application.....	102
Uninstalling Nymi Lock Control.....	102
Upgrading the Nymi Runtime.....	102
Performing a customizable Nymi Runtime installation or upgrade.....	102
Performing a silent installation or upgrade of Nymi Runtime.....	103
Uninstalling the Nymi Runtime.....	103
Audit Log Appendix.....	104

Preface

Nymi™ provides periodic revisions to the Nymi Connected Worker Platform. Therefore, some functionality that is described in this document might not apply to all currently supported Nymi products. The product 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
5.0	May 3, 2021	Update to reflect Nymi Enterprise Edition rebrand to Connected Worker Platform. This update includes Windows Lock Control and Smart Distancing and Contact Tracing. Major updates to instructions on Modifying the Group Policy.
4.0	February 26, 2021	Update to include changes for Nymi Enterprise Edition 3.4.0. This includes authentication lockout.

Version	Date	Revision history
3.0	December 18, 2020	Update to include policy changes based on the Nymi Enterprise Edition 3.3.0 release. <ul style="list-style-type: none"> • Updates to Upgrading NES • Updates to Configure a Group Policy sections • Updates to Certificate Management
2.0	September 18, 2020	Update of this document for the Nymi Enterprise Edition 3.2.0 release.
1.0	April 15, 2020	First release of this document for Nymi Enterprise Edition 3.1.0

How to get product help

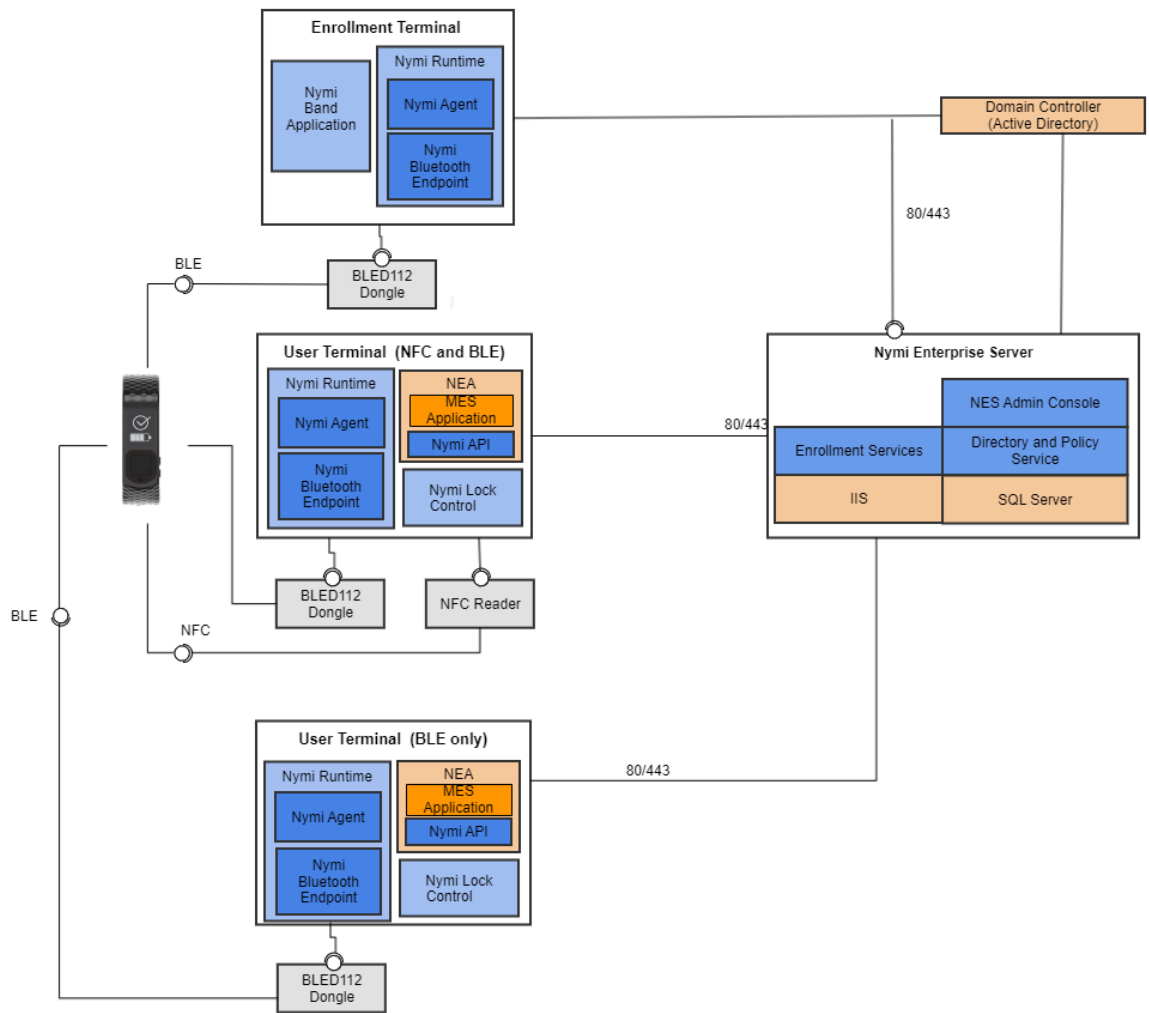
If the Nymi software or hardware does not function as described in this document, contact your administrator for immediate support. Alternatively, you can submit a [support ticket](#) to Nymi, or email support@nyimi.com

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@nyimi.com

Connected Worker Platform Components

The Connected Worker Platform enables administrators and users to manage Nymi Bands in an enterprise setting. The Connected Worker Platform is comprised of Nymi-specific components and enterprise components, as shown in the following figure.



This guide Connected Worker Platform consists of the following components. Smart Distancing and Contact Tracing components are described in the Nymi Smart Distancing and Contact Tracing Installation and Configuration Guide.

Table 2: Connected Worker Platform Components Covered in this Guide

Component	Description
Enrollment Terminal	Windows 10 machine that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal and is used to enroll a new user and link them to their Nymi Band. The Nymi Band Application requires the Nymi Runtime application.
Nymi Runtime	A Windows application that you install on the enrollment terminal and user terminals. Nymi Runtime includes the Nymi Agent and Nymi Bluetooth Endpoint components. Nymi Runtime supports communication between NES, the Nymi Band, NEAs, the Nymi Band Application and Nymi Lock Control.
User Terminal	Windows 10 machine on which you install Nymi components that allow users to perform authentication tasks with the Nymi Band.
Nymi Band	A wearable device that is activated by the assigned user's biometrics. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled. See the Nymi Band section in this guide for more information.
Nymi-enabled Application	Developers can create corporate applications that integrate with Connected Worker Platform by using the Nymi API. These applications are called Nymi-enabled Applications (NEAs) and include Manufacturing Execution Systems (MES), Single Sign-On (SSO), and Human Machine Interface (HMI) applications. An NEA requires the Nymi Runtime software.
Nymi Lock Control	A Windows application that allows the user to unlock their terminal without entering their username and password.

Component	Description
Nymi Enterprise Server (NES)	A management server and collection of services, NES coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory). NES administrators access the NES Administrator Console to manage policies and certificates.
Domain Controller (DC)	Windows server with external directory and database systems, such as Active Directory.

Nymi Band 3.0

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

Nymi Band Physical Features

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

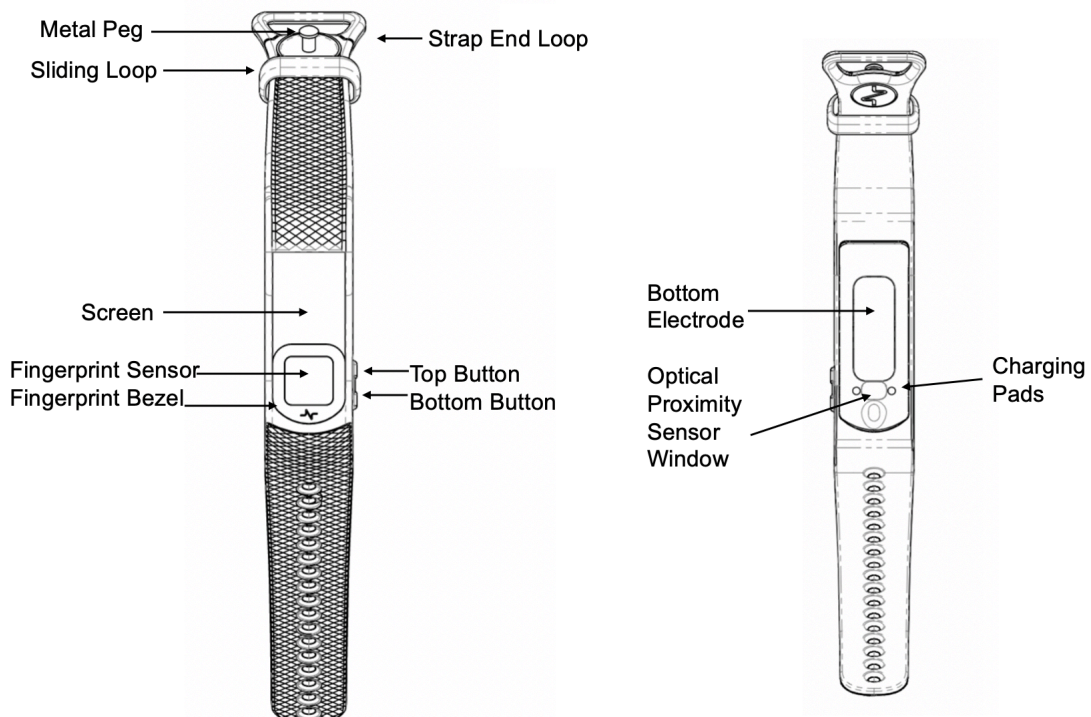


Figure 2: Nymi Band front and back

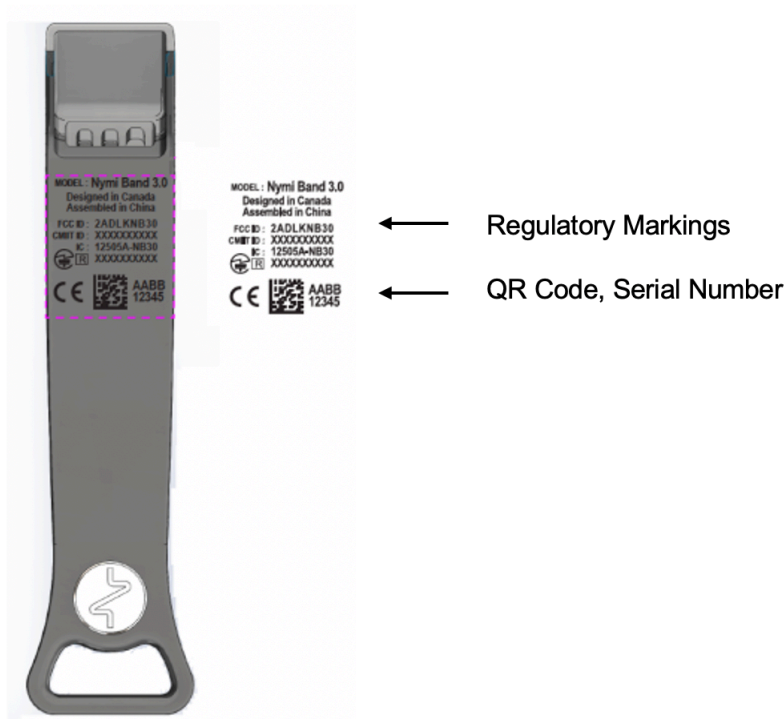


Figure 3: Nymi Band Strap

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

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

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

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

Nymi Lock Control

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

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

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

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

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.

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).

Nymi-Verified NFC Readers

Nymi only supports PC/SC NFC readers. The following technical requirements are required for NFC readers that will be used with the Connected Worker Platform:

- ISO14443A compatibility.

- PC/SC compatibility.
- Operation frequency of 13.56 MHz.

Nymi recommends the HID 5022 USB Reader for its superior performance. It is fully compatible with the Nymi Band and also supports many other smart card technologies and NFC-enabled devices. Should this reader not address your organization's use case in some way, please contact your Nymi Solution Consultant for additional options.

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.

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.

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

```

    }
    {
        "supportedReader" : "Omnikey 5x25"
    }
  }

```

Bluetooth Adapter Placement

The Bluetooth Low Energy (BLE) radio antenna in a BLED112 USB Adapter provides seamless Bluetooth capability between the Nymi Band and devices such as a laptop computer.

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

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

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

Nymi Band Enrollment Process

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

The enrollment process performs the following actions:

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

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

The Nymi Connected Worker Platform provides an additional method of authentication called a corporate credential authenticator. If the enterprise policy permits it, the Nymi Band Application creates a corporate credential authenticator in addition to the fingerprint authenticator. With a corporate credential authenticator, the Nymi Band trusts the enterprise to validate the user credentials, such as an AD username and password, before bringing the Nymi Band into an authenticated state.

Authentication After Enrollment

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

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

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

Plan Your Configuration

NES Administrators use the NES Administrator Console to manage the Connected Worker Platform by creating policies.

A policy enables you to customize the enrollment and registration process by configuring the settings that are optional or mandatory for all Nymi Band users.

Minimum requirements for the Nymi Band Application

The section summarizes the minimum software and hardware requirements for the Nymi Band Application.

Software requirements

- Windows 10, 64-bit
- Windows 7, 64-bit

Note: It is recommended to use 125% scaling and 1920 x 1080 screen resolution for the terminal hosting the Nymi Band Application.

Hardware requirements

- 4GB RAM
- 5GB free disk space
- 2 core CPU (recommended)
- 1 USB 2.0 port
- Bluetooth Low Energy (BLE) radio antenna, present in Bluegiga BLED112 BLE adapter.

Minimum Requirements for Nymi Lock Control

Nymi Lock Control supports the following operating system versions:

- Windows 10, 64-bit

Nymi Lock Control supports the following NFC readers:

- HID Omnikey 5022

Other considerations:

- Nymi Lock Control is a single domain solution. All terminals must be on the same domain as the Nymi Enterprise Server host, not across separate domains.
- Nymi Lock Control is only supported on thick clients.
- Nymi Lock Control will only lock and unlock the desktop of a local terminal, not remotely (ex. remote desktop, or Citrix).

- Each user terminal requires a connected Bluetooth Low Energy (BLE) radio antenna, such as a Bluegiga BLE adapter.

Authentication method

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 configuration option advantages and disadvantages

Settings	Advantage	Disadvantage
Fingerprint Required only	<ul style="list-style-type: none"> • Biometric guarantee of the user's identity. 	<ul style="list-style-type: none"> • Authentication might fail when the fingerprint is dirty or cut, or when the fingerprint sensor is not clean.
Fingerprint or Corporate Credentials	<ul style="list-style-type: none"> • Allows a user to authenticate by fingerprint, or corporate credentials when the fingerprint is dirty or cut. 	<p>When corporate authentication occurs there is:</p> <ul style="list-style-type: none"> • no biometric guarantee of the user's identity. • no guarantee of the user who supplied password is the correct user.

One-time password (OTP) for Nymi application certificates

Nymi applications, such as the `Nymi Band Application` and any Nymi-enabled Application (NEA) that is developed by using the Nymi API, establish secure communications with Nymi Bands through mutual certificate validation. Each Nymi Band comes with a factory-installed Nymi Band Certificate. Nymi applications obtain a certificate from the Nymi Enterprise Server (NES) the first time that a user opens the application on a machine, through a process called certificate enrollment. The certificates are installed in the `%APPDATA%` directory for the user or service that runs the Nymi-enabled Application. Each time that the Nymi-enabled Application starts, the application performs a certificate check. If the `%APPDATA%` directory for the user or service that runs the application does not contain the certificates, the application initiates the certificate enrollment process.

A certificate from the NES must be obtained for each new user. After a user obtains a certificate in the `%APPDATA%` directory in their machine, they will not need to re-obtain the certificate (unless the certificate or `%APPDATA%` was removed). This means a user will only need certificate enrollment once per application, per machine.

To have greater control over who can install and run a Nymi-enabled Application (NEA), you can enable the **Manual NEM OTP Mode** (Nymi Enterprise Manager One-time Password) setting in the active group policy. Typically, a certificate is automatically obtained from the NES before the certificate

enrollment process begins for the new user. With this mode enabled, a new user must enter their one-time password (OTP) before the certificate can be retrieved from the NES.

To perform the certificate enrollment process, the user with OTP enabled for their account must log in to the Nymi-enabled Application and type their OTP. The OTP has a default expiration time of 1 hour, and is generated by the administrator. Once the password has been verified for the new user, NES issues the application certificate to the Nymi-enabled Application (to the %APPDATA% directory). Certificate enrollment fails and an error message appears if the user incorrectly entered their OTP.

To require a user to type an OTP to start the certificate enrollment process, you must perform the following configuration changes:

- Select the **Manual NEM OTP Mode** option for the active group policy.
- Edit a user and create an OTP for each Nymi-enabled Application instance that is installed on a terminal. The selected user does not have to be an administrator. You can only use an OTP once for each Nymi-enabled Application on each terminal. After the user uses the OTP, the administrator must generate a new OTP for a Nymi-enabled Application on another terminal.

The following table summarizes the advantages and disadvantages of using or not using the **manual OTP mode** option in the OTP.

Table 4: Manual OTP Mode option advantages and disadvantages

Option	Advantage	Disadvantage
<p>Manual NEM OTP mode=Yes</p> <p>The first time that a user logs into the application, they must type a valid OTP before NES issues an application certificate.</p>	<ul style="list-style-type: none"> • Provides additional accountability for application certificate enrollment. • Prevents any user from installing a Nymi-enabled Application on any machine. Only certain users can install a Nymi-enabled Application. • Binds the password to a user and an application. For example, a user cannot use an NEM OTP to install an NEA. 	<ul style="list-style-type: none"> • Before users can enroll a Nymi Band, a designated user must type an OTP in the Nymi Band Application. • Before certificate enrollment can succeed, an NEA must provide an interface that supports typing a OTP. • If a new user logs into Windows and the %APPDATA% directory for the user does not contain the certificates, the Nymi Band Application prompts the first user that logs into the application to provide an OTP.
<p>Manual NEM OTP mode=No</p> <p>NES automatically issues an application certificate the first time that a user logs into the application.</p>	<ul style="list-style-type: none"> • Allows fully-automated application deployment. • Anyone can install the Nymi Band Application on their machine and use it to enroll their Nymi Bands. 	<ul style="list-style-type: none"> • All domain users can obtain the application certificate. • Less control over who can install and use the application.

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 5: Nymi Band configuration checklist for users

Completed?	Task
	Remove the Nymi Bands and charging cradles from the box. The Nymi Band, contains enough battery charge to get you through the enrollment activities. The Nymi Band arrives in ship mode, to wake the Nymi Band, press the top bottom. After enrollment, charge the Nymi Bands for at least 2 hours for a full charge. A fully charged Nymi Band battery will typically have a 3-day battery life based on 300 BLE or NFC taps over 10 hours per day.
	Use the NES Administrator Console to Configure a group policy.
	<p>On the enrollment terminal that you will use to enroll users:</p> <ul style="list-style-type: none"> • Install the Nymi Band Application. • Plug the Nymi-provided Bluetooth Adapter (BLED112) into a USB port. • Import the root certificate into the Trusted Root Certificate Authorities store (if the certificate is not already in the store).
	<p>On each user network terminal:</p> <ul style="list-style-type: none"> • Install the Nymi Band Application, or install Nymi Runtime and the Nymi-enabled Application. • If Manual NEM OTP Mode is enabled, log into the application and provide the OTP to complete the certificate enrollment process. • Plug the Bluetooth adapter (BLED112) into a USB port. • Import the root certificate into the Trusted Root Certificate Authorities store (if the certificate is not already in the store).
	<ul style="list-style-type: none"> • 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.
	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.

Install Nymi Applications and Configure the User Terminals

There are generally three functions of user terminals. User terminals are devices in the environment that people use to:

- A user terminal where a user performs repetitive tasks that require authentication, possibly by using an NEAs, such as an MES applications. The user terminal can also be locked or unlocked using Nymi Lock Control.
- A user terminal where users enroll their Nymi Bands using the Nymi Band Application.
- A user terminal where NES Administrators can connect to the NES Administrator Console to manage NES.

The following sections describes the tasks that you need to perform to prepare each user terminal.

User terminal for Nymi Band Enrollment

Before a user can enroll and authenticate the Nymi Band, the NES Administrator must perform the following actions on at least one machine in the environment (the enrollment terminal):

1. Insert the Nymi-supplied Bluetooth adapter into an available USB port.
2. Import the Root CA certificate on the network device, as described in the *Importing the Root CA certificate* section.
3. Install the Nymi Band Application as described in the *Installing the Nymi Band Application* section. The Nymi Band user requires physical access to the network terminal.

Note: The Nymi Band Application includes the `Nymi Runtime` software.

Nymi Band Application Installation

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

You can perform a customizable installation, or if the installation does not require an OTP, a silent installation.

Note: The BLE driver is installed with the installation of Nymi Runtime. The BLE driver may also be installed separately by going to the Nymi SDK package and installing the *BleDriver.msi* file.

Performing a customizable Nymi Band Application installation

Perform the following steps to install the Nymi Band Application on a network device.

1. Download the Nymi Band Application package.
2. Double-click to run the `Nymi-Band-App-installer-v_version.exe` installer.
3. Follow the prompts in the Nymi Band Application installation wizard and when prompted, install all the prerequisite packages and BLE device driver from Silicon Labs.

4. In the Windows Services applet, confirm that you can see the Nymi Agent and Nymi Bluetooth Endpoint services, and that the status of each service is *Running*.
5. Close the Nymi Band Application.

Performing a silent Nymi Band application installation or upgrade

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

1. Download the Nymi Band Application package.
2. Launch the command prompt as administrator.
3. From the folder that contains the Nymi Band Application, type *Nymi-Band-App-installer-v_version.exe /xenoui /q*

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

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

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

Setting the NES URL

After you install the Nymi Band Application, ensure that the enrollment process uses the correct NES URL.

1. Run *regedit.exe*
2. On the User Account Control window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.
4. Right-click **NES**, and then select **New > String value**.
5. In the **Value** field, type URL.
6. Double-click **URL** and in the **Value Data** field, type `https://nes_server/NES_service_name/` or `http://nes_server/NES_service_name` depending on the NES configuration
where:
 - *nes_server* is the FQDN of the NES host.
 - *NES_service_name* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but it is recommended that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
7. Click **OK**.

User terminal for NEAs

User terminals are machines that users use to perform daily tasks with the Nymi Band.

Prepare User terminals for Nymi-enabled Applications

Before a user can use a Nymi-enabled Application, the NES Administrator must perform the following actions on the user terminal:

1. Insert the Nymi-supplied Bluetooth Adapter into an available USB port. The Bluetooth Adapter is used to detect Nymi Bands as they move in and out of Bluetooth signal range, and is primarily used for communication with the band during enrollment, Windows unlock, MES signing, as well as monitoring signal strength for presence.
2. Attach a Nymi-verified NFC reader into an available USB port.
3. Import the Root CA certificate.
4. (Optional) Install Nymi Lock Control. Includes automatic installation of Nymi Runtime.
5. Install Nymi Runtime.
6. Install the NEA.

Importing the Root CA certificate

Perform the following steps only if the Root CA issuing the NES TLS server certificate is not a Trusted Root CA (for example, if a self-signed TLS server certificate is used for NES). Install the Root CA on each computer that establishes a connection with the NES host.

While logged into the user terminal as a local administrator, use the `certlm` application to import the root CA certificate into the Trusted Root Certification Authorities store. For example, on Windows 10, perform the following steps:

1. In Control Panel, select **Manage Computer Certificates**.
2. In the `certlm` window, right-click **Trusted Root Certification Authorities** and select **All Tasks > Import**.

The following figure shows the `certlm` window.

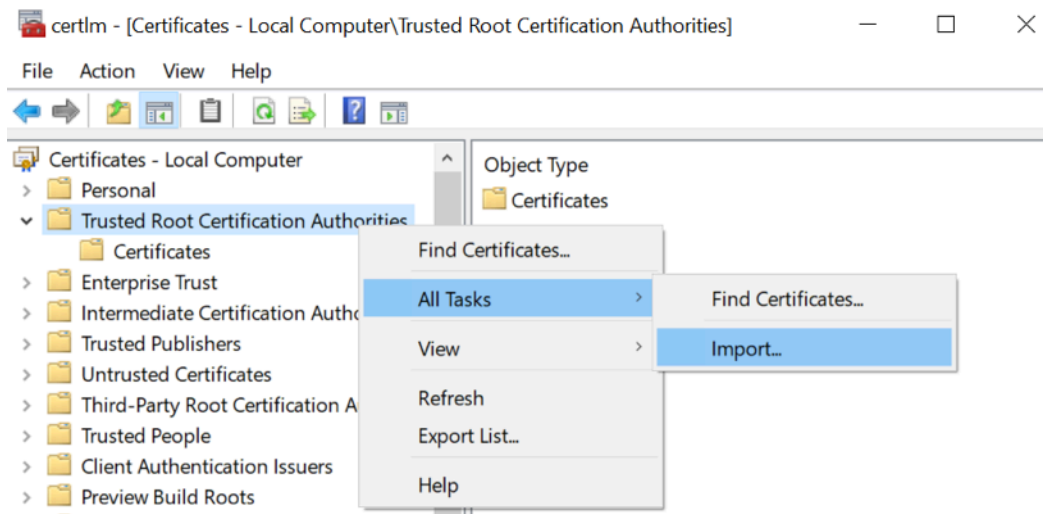


Figure 4: `certlm` application on Windows 10

3. On the Welcome to the Certificate Import Wizard screen, click **Next**.
The following figure shows the Welcome to the Certificate Import Wizard screen.

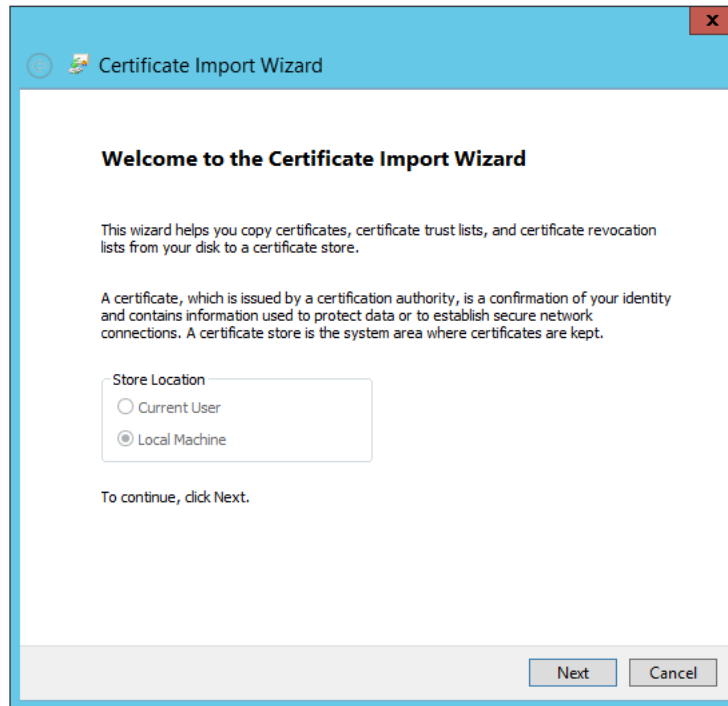


Figure 5: Welcome to the Certificate Import Wizard screen

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

5. On the `File to Import` screen, click **Next**.

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

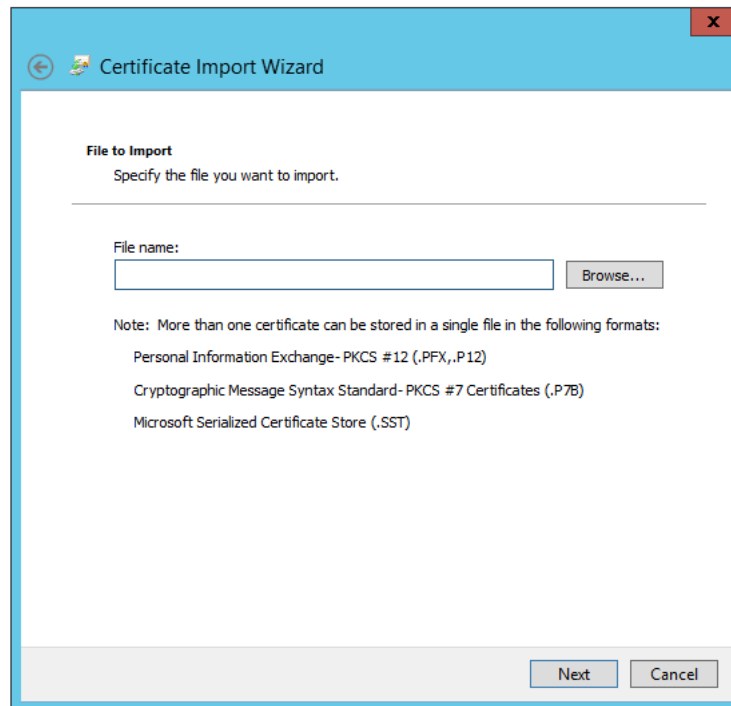


Figure 6: `File to Import` screen

6. On the `Certificate Store` screen, accept the default value **Place all certificates in the following store** with the value **Trusted Root Certification Authorities**, and then click **Next**.
7. On the `Completing the Certificate Import Wizard` screen, click **Finish**.

Install Nymi Runtime

Nymi Runtime facilitates communication between NES and the Nymi Bands.

Install the Nymi Runtime on each user terminal on which you will also install a Nymi-enabled Application. You can perform a customizable installation or a silent installation.

Note: Nymi Lock Control automatically installs Nymi Runtime.

Note: On the machine that runs the Nymi Band Application, do not make any modifications to Nymi Runtime. You can update Nymi Runtime by performing an installation or upgrade of the Nymi Band Application. For more information about installing the Nymi Band Application, see the *Nymi Band Application Installation* section of this guide.

Performing a customizable Nymi Runtime installation or upgrade

Perform the following steps to install or upgrade Nymi Runtime on a network device, on which you want to install a Nymi-enabled application.

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

2. Extract the Nymi SDK distribution package.
3. From the `..\nyimi-sdk\windows\setup` folder, run the *Nymi Runtime Installer version.exe* file.
4. On the Welcome page, click **Install**.
5. On the User Account Control page, click **Yes**.
The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the Welcome to the Nymi Runtime Setup Wizard page, click **Next**.
7. On the Nymi Runtime Setup page, click **Next**.
8. On the Service Account window, click **Next**.
9. On the Ready to install page, click **Install**.
10. Click **Finish**.
11. On the Installation Completed Successfully page, click **Close**.
12. In the Windows Services applet, confirm that you can see the *Nymi Agent* and *Nymi Bluetooth Endpoint* services, and that the status of each service is *Running*.

Performing a silent installation or upgrade of Nymi Runtime

Perform the following steps to install or upgrade the Nymi Runtime and the BLE adapter drivers silently, without user intervention.

1. Log in to the network terminal with an account that has administrator privileges.
2. Extract the Nymi API distribution package.
3. Launch the command prompt as administrator.
4. Change to the `..\nyimi-sdk\windows\runtime` folder, and then type: "*Nymi Runtime Installer version.exe*" `/exenoui /q`

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

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

The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, Nymi Runtime appears in the Program and Features applet.

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

The silent installation process creates an installation log file in the `%temp%` directory named *Nymi Runtime_version_time.log*

Install and Configure Nymi Lock Control

Perform the steps in the following section to install Nymi Lock Control on user terminals in the environment and configure NES to enable Nymi Lock Control support.

Configuring and Installing Nymi Lock Control on User Terminals

On each user terminal that will use Nymi Lock Control to lock and unlock the terminals, you must create a registry key that defines the path to NES and install the Nymi Lock Control application.

Configuring User Terminals for Nymi Lock Control

Create a GPO to push the NES URL registry key to each user terminal, or perform the following steps to manually create the registry key on the user terminal.

Run *regedit* as an administrator.

1. Navigate to *HKEY_LOCAL_MACHINE\Software\Nymi\NES*.

Note: If this path does not exist, create the keys.

2. In the *NES* key, create a new string value.
3. In the **Name** field, type URL.
4. Edit the string and in the value field, type `https://nes_server/nes_service_name`

Where:

- *nes_server* is the Fully Qualified Domain name of the NES host.
- *nes_service_name* is the services mapping name of the NES web application. The default value is *nes*.

For example, `https://ev3-uat-srv1/ev3-uat-lab.local/nes`

Note: The service mapping name for NES was defined during deployment.

- Close *regedit.exe*.

Installing Nymi Lock Control

Perform the following steps on each user terminal in the environment.

1. Copy the *NymiLockControl-installer-vw.x.y.z* to a directory on the user terminal.
2. Right-click *NymiLockControl-installer-vw.x.y.z* and select **Run as administrator**.
3. On the User Account Control window, click **Yes**.
4. On the Welcome to Nymi Lock Control Setup Wizard window, click **Next**.
5. On the Select Installation Folder window, perform the following actions: optionally, click **Browse** and select a different installation folder, and then click **Next**
 - a) Optionally, click **Browse**, navigate to a new installation folder, and then click **Select Folder**
 - b) Click **Next**.
6. On the Ready to Install window, click **Install**.
7. On the Completing the Nymi Lock Control Setup Wizard window, click **Finish**.
8. A copy of configuration file, *nbe.default.toml* is installed in *C:\Nymi\Bluetooth_Endpoint*. Configure the file and rename it to *nbe.toml*.

Note: Enable BLE tap intent by providing a non-zero, negative number (ex. -42) for *rss_i_tap_threshold*. Change the other RSSI values to change the sensitivity of Nymi Lock Control.

For more information refer to [Editing the nbe.toml File](#) on page 28.

9. Enable Nymi Lock Control in the active group policy through NES.

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 described in [Editing the nbe.toml File](#) on page 28.

Editing the nbe.toml File

A backup configuration file is installed on the user terminal when the Nymi Bluetooth Endpoint is installed or updated. This file, *nbe.default.toml*, contains the default values that control BLE tap behavior with the Nymi Band and BLE adapter. Use the values in the *nbe.default.toml* file as a template for the *nbe.toml* file. These files are located in *C:\Nymi\Bluetooth_Endpoint*.

Note: Nymi Bluetooth Endpoint will only recognize RSSI values in the *nbe.toml* file. Retain a backup of a useful configuration by copying the *nbe.toml* file and renaming it.

Table 6: Default configuration settings for Nymi Lock Control and BLE tap intent

<i>nbe.toml</i> Entry	Default Value	Description
<i>agent_url</i>	"ws://127.0.0.1:9120/ socket/websocket" (do not change)	Identifies the location of the agent URL. The default value shown in this table is generated if the agent is installed locally. If the agent URL is installed centrally (via remote installation), the hostname of the URL will be different. The agent_url must be present when using an <i>nbe.toml</i> file.
<i>rss_i_window_tap</i>	10	This determines the duration the Nymi Band must be within tap-distance of the BLE radio antenna to complete a tap. A larger value increases the duration required to perform and decrease the sensitivity.
<i>rss_i_window_long</i>	50	This determines the frequency that Nymi Bluetooth Endpoint checks the distance between the BLE radio antenna and the Nymi Band. 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.
<i>rss_i_tap_threshold</i>	0 (must be 0 or negative)	This 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. Nymi recommends an RSSI value of -42. If the Nymi Band maintains a minimum distance specified by <i>rss_i_tap_threshold</i> , for a duration <i>rss_i_window_tap</i> , a BLE tap is performed.

<i>nbe.toml</i> Entry	Default Value	Description
<i>rss_i_cutoff_close</i>	-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 <i>rss_i_cutoff_close</i> 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 <i>rss_i_cutoff_close</i> value to the <i>rss_i_cutoff_far</i> value, Nymi Lock Control locks the user terminal.
<i>rss_i_cutoff_far</i>	-75 (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 <i>rss_i_cutoff_far</i> value to the <i>rss_i_cutoff_close</i> value, Nymi Lock Control unlocks the user terminal.

1. Make a copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.default.toml` file, and name the file `nbe.toml`.
2. Edit the `nbe.toml` file with a text editor.
3. Edit the RSSI values in the file. Refer to the descriptions in the table above.
4. Save the `nbe.toml` file.
5. Restart the Nymi Bluetooth Endpoint.
 - a) Press the Windows key on the keyboard, or click the start button on the toolbar. Enter "Services" in the search bar. The Services application window appears.
 - b) Search for **Nymi Bluetooth Endpoint** in the Services application.
 - c) Right-click **Nymi Bluetooth Endpoint** and restart it.

Once restarted, the Nymi Bluetooth Endpoint application will be updated with the edits made in the `nbe.toml` file. Updated BLE tap intent and Nymi Lock Control settings will be implemented on the user terminal. If the `nbe.toml` file is not present, Nymi Bluetooth Endpoint behaves under default settings.

Configuring NES to support Nymi Lock Control

Edit the active policy in NES to enable the use of Nymi Lock Control. Refer to [Modifying the default group policy](#) on page 34.

Users can use an authenticated Nymi Band to unlock user terminals, when Nymi Lock Control is installed on the user terminal.

Note: If you enabled Nymi Lock Control in NES *after* users already enrolled their Nymi Bands, the Nymi Band user must log into the Nymi Band Application to receive the update in the group policy. The Nymi Band Application will prompt the user to create an internal security key, which allow the Nymi Band to operate with Nymi Lock Control.

Setting the NES URL

After you install the Nymi Band Application, ensure that the enrollment process uses the correct NES URL.

1. Run *regedit.exe*
2. On the User Account Control window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.
4. Right-click **NES**, and then select **New > String value**.
5. In the **Value** field, type URL.
6. Double-click **URL** and in the **Value Data** field, type `https://nes_server/NES_service_name/` or `http://nes_server/NES_service_name` depending on the NES configuration
where:
 - *nes_server* is the FQDN of the NES host.
 - *NES_service_name* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but it is recommended that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
7. Click **OK**.

Install Nymi Runtime

Nymi Runtime facilitates communication between NES and the Nymi Bands.

Install the Nymi Runtime on each user terminal on which you will also install a Nymi-enabled Application. You can perform a customizable installation or a silent installation.

Note: Nymi Lock Control automatically installs Nymi Runtime.

Note: On the machine that runs the Nymi Band Application, do not make any modifications to Nymi Runtime. You can update Nymi Runtime by performing an installation or upgrade of the Nymi Band Application. For more information about installing the Nymi Band Application, see the *Nymi Band Application Installation* section of this guide.

Performing a customizable Nymi Runtime installation or upgrade

Perform the following steps to install or upgrade Nymi Runtime on a network device, on which you want to install a Nymi-enabled application.

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the `..\nymi-sdk\windows\setup` folder, run the *Nymi Runtime Installer version.exe* file.
4. On the Welcome page, click **Install**.

5. On the **User Account Control** page, click **Yes**.
The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the **Welcome to the Nymi Runtime Setup Wizard** page, click **Next**.
7. On the **Nymi Runtime Setup** page, click **Next**.
8. On the **Service Account** window, click **Next**.
9. On the **Ready to install** page, click **Install**.
10. Click **Finish**.
11. On the **Installation Completed Successfully** page, click **Close**.
12. In the **Windows Services** applet, confirm that you can see the *Nymi Agent* and *Nymi Bluetooth Endpoint* services, and that the status of each service is *Running*.

Performing a silent installation or upgrade of Nymi Runtime

Perform the following steps to install or upgrade the Nymi Runtime and the BLE adapter drivers silently, without user intervention.

1. Log in to the network terminal with an account that has administrator privileges.
2. Extract the Nymi API distribution package.
3. Launch the command prompt as administrator.
4. Change to the `..\nyimi-sdk\windows\runtime` folder, and then type: `"Nymi Runtime Installer version.exe" /xenoui /q`

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

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

The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, Nymi Runtime appears in the **Program and Features** applet.

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

The silent installation process creates an installation log file in the `%temp%` directory named `Nymi Runtime_version_time.log`

User terminal for NES administration

NES Administrators can use any user terminal with a web browser to access the NES Administrator Console.

An NES Administrator is not required to perform any configuration tasks on the user terminal before accessing the NES Administrator Console.

Connect to NES for the First Time

An NES Administrator uses a web browser on a network device to connect to the NES Administrator Console.

Accessing NES Administrator Console

Perform the following steps to connect to the NES Administrator Console and the System Diagnostics page.

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://server-2.nymi.lab/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.

2. Click the **Sign in** button.
The Sign in dialog opens. Enter username and password.
3. Verify the username has administrative access by observing **Policies**, and **Search** in the main menu.

The *Nymi Connected Worker Platform Troubleshooting Guide* provides information about how to resolve issues that you might encounter when you try to access the NES Administrator Console.

Configure a Group Policy

NES provides you with a default group policy.

Review the Group Policy and make any configuration changes as needed.

Modifying the default group policy

The default group policy, *Default Settings Set* is configured with the following settings:

- Authenticate identity by fingerprint only
- Save enrollment data to NES only.
- Create application certificates automatically (an OTP is not required)
- Capture the NFC UID of the Nymi Band
- Log a user out of the Nymi Band Application or the NES Administrator Console after 5 minutes of inactivity

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

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://server-2.nymi.lab/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.
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 Group Policy page appears. The following figure shows the Group Policy page.

The screenshot shows a web interface titled "Group Policy". Below the title is a table with the following columns: Policy Name, Is Active, Created, Modified, and Modifier. There is one row in the table with the following data: Policy Name: [Default settings set](#), Is Active: Active, Created: 2020-08-25, Modified: 2020-08-27, Modifier: UAT-Lab\uatadmin. Below the table is a dark button labeled "Create New Group Policy".

Policy Name	Is Active	Created	Modified	Modifier
Default settings set	Active	2020-08-25	2020-08-27	UAT-Lab\uatadmin

Create New Group Policy

Figure 7: Group Policy Page

4. Click **Default settings set**.

The Edit page appears.

5. Enable or disable **Smart Distancing and Contact Tracing**.

- Select the option to enable Smart Distancing and Contact Tracing functionality on the Nymi Band during enrollment. This includes **Smart Distancing Reminders** and contact tracing event collection.
- Leave the option cleared to disable **Smart Distancing and Contact Tracing**. **Smart Distancing Reminders** will not be available if this option is cleared.

Note: Update enrolled Nymi Bands with Smart Distancing and Contact Tracing functionality by logging into the Nymi Band Application.

6. Enable or disable **Smart Distancing Reminders**. This option is only available if **Smart Distancing and Contact Tracing** is enabled.

- Select the option to allow users to receive smart distancing reminders on their Nymi Bands. The Nymi Band will vibrate and display a reminder on the screen when Nymi Band users are in close proximity with each other for approximately 5 minutes.
- Leave the option cleared to disable smart distancing reminders on Nymi Bands.

7. From the **Enrollment Settings** section, perform the following actions:

- a) For the **Corporate Credentials Authentication** option, perform one of the following actions:
 - Select the option to allow a user to authenticate by corporate credentials. The **Nymi Band Application** creates a corporate credential authenticator during enrollment.
 - Leave the option cleared to allow users to only authenticate by fingerprint. The **Nymi Band Application** does not create a corporate credential authenticator during enrollment.
- b) For the **Enrollment Destination** option, select one of the following actions:
 - NES — **Nymi Band Application** saves enrollment data to NES only.
 - NES and Evidian — **Nymi Band Application** saves enrollment data to NES and the Evidian EAM Controller. Select this option when using Evidian in your environment.
- c) From the **NFC UID Capture** list, the following option: **Mandatory**.
- d) Optionally, to enable the enrollment process to display an identifying label on the Nymi Band, 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 user's Active Directory username 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.

Note:

- If the **Display Band Label on Nymi Bands** option was disabled and you later enable the option in the active policy, Nymi Band users can apply a Band Label by logging into the Nymi Band Application and using the Nymi Band Enrollment screens without performing the Delete User Data process.
- If the **Display Band Label on Nymi Bands** option was enabled in the active policy and you want to disable the option and remove the Band label on Nymi Bands, do the following:
 1. Delete user data on each Nymi Band that was enrolled when the active policy had the **Display Band Label on Nymi Bands** option enabled. See *Deleting User Data*.
 2. Edit the active policy in NES and clear the option **Display Band Label on Nymi Bands**.
 3. Advise the user to log in to the Nymi Band Application and re-enroll the Nymi Band.

8. From the **Lock Control** section, enable or disable **Nymi Lock Control**.

- Select the **Enable Nymi Lock Control** option to display the following features. These features cannot be enabled unless **Enable Nymi Lock Control** is selected. The **Nymi Band Application** creates security settings during enrollment.
 - **Lock When Away**
 - **Unlock When Present**
 - **Keep Unlocked when Present**
- Leave the option cleared to prevent users from unlocking their terminals with **Nymi Lock Control**.

Note: Edit the *nbe.toml* file to define close proximity for **Nymi Lock Control**. Refer to *Editing the nbe.toml File*.

The following settings are available when **Nymi Lock Control** is enabled:

- a) The **Lock When Away** option provides you with the ability to lock the terminal when the user moves away.
 - Select the option to configure **Nymi Lock Control** to lock 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 for at least 30 seconds. 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.
 - Clear the option to prevent **Nymi Lock Control** from locking the user terminal when the **Nymi Band** is not in close proximity of the user terminal.

Note: If the **Nymi Band** deauthenticates, the user terminal locks regardless of how you configure the **Lock When Away** option.
 - b) The **Unlock When Present** option provides you with the ability to define how close the **Nymi Band** must be to the terminal to allow the user to unlock the terminal with the **Nymi Band**:
 - Select the option to prevent 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.
 - Clear the option to allow a user to unlock the terminal by pressing the **Enter** key or space bar on the keyboard when the **Nymi Band** is within Bluetooth range, but not in close proximity of the user terminal.
 - c) The **Keep Unlocked when Present** option provides you with the ability to define how the **Nymi Band** interacts with operating system screen timeouts or sleep settings that lock the terminal:
 - Select the option to override any system screen timeouts or sleep settings, and keep the user terminal unlocked as long as the **Nymi Band** is present and authenticated.
 - Clear the option to prevent **Nymi Lock Control** from overriding any system screen timeouts or sleep settings.
9. (Optional - not recommended) In the **Authentication Settings** section, perform the following action.
- a) For the **Liveness Detection** setting, deselect the option to disable ECG detection during authentication. Under default settings, authentication requires fingerprint match and ECG detection to ensure the user is wearing the **Nymi Band**. Disabling **Liveness Detection** will disable the ECG detection requirement and will result in faster authentication times, however you

will have reduced security. When this option is disabled, the Nymi Band will not collect ECG during authentication.

10. In the **Active Directory** section, perform one of the following actions.

- a) Deselect the option **Check User Status**.
- b) Select the option **Cache User Status** to cache user status in NES for a specified period, which prevents NES from querying AD each time that a **lookup** call is made. When you select this option, the **Cache Expiry** field appears.
- c) From the **Cache Expiry** list, select the amount of time that NES caches the user status for a user. When NES receives a **lookup** command, it will provide the user status from cache, if the amount of time that the status has been stored in NES does not exceed the **Cache Expiry** value. The default value is 15 minutes.

11. Click **Save**.

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

The screenshot shows the 'Edit Group Policy' page with the following settings:

- Policy Name:** Default settings set
- Is Active:** Yes (to deactivate, activate another policy)
- Manual NEM OTP Mode:**
- Auto Logout Timeout:** 5 minutes
- Smart Distancing and Contact Tracing:**

Enrollment Settings:

- Enrollment Destination:** NES
- Fingerprint Required:**
- Corporate Credentials Authentication:**
- NFC UID Capture:** Mandatory
- Display Band Label on Nymi Bands:**
- Allow Band Label Customization:**

Active Directory:

- Check User Status:**

Lock Control:

- Enable Nymi Lock Control:**

Buttons: Save, Back to List, Reset to Default

© Copyright 2021 Nymi Inc.

Figure 8: Edit Group Policy page

Creating a new policy

Perform the following steps to create a new policy.

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://server-2.nymi.lab/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.

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 Policy page.



Policy Name	Is Active	Created	Modified	Modifier
Default settings set	Active	2020-08-25	2020-08-27	UAT-Lab\uatadmin

Create New Group Policy

Figure 9: 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 Administrators group.

4. Configure the options for the policy, and then click **save**. The *Modifying a group policy* provides detailed information about the configuration options for a policy.

Customizing the Nymi Band Application certificate creation

Perform the following steps to configure the Nymi Band Application to request an OTP and to generate an OTP for a user.

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://server-2.nymi.lab/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.

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 navigation bar, click **Policies**.
4. In the **Policies** window, select the active policy.
5. Select **Manual NEM OTP mode**, and then click **Save**.
6. On the navigation bar, select **Search**.
The **Search** page appears, which displays a search field on the left side of the page.
7. In the **Search** field, type the username, first name, or last name of the user that logs in to the enrollment terminal, as the value appears in AD.

8. Click **Search**.

The **Users** page displays the user or a list of users that match the search criteria. The following figure provides an example of the **Users** page when multiple users are found based on the search criteria.

The screenshot shows a search interface with the following elements:

- Search** header
- Radio buttons for **Users** (selected) and **Nymi Bands**
- Text: **Search by first name, last name, or username**
- Search input field containing **doe** and a **Search** button
- Text: **3 users matching 'doe' found**
- Table with 3 columns: **Domain\username**, **First Name**, and **Last Name**

Domain\username	First Name	Last Name
QA-Lab\edoelger	Evelyne	Doelger
QA-Lab\JaneDoe	Jane	Doe
QA-Lab\JohnDoe	John	Doe

Figure 10: Users page

9. If the search results returned more than one user, click the username of the correct user.

10. On the **User** page, click **OTP Generation** at the bottom of the page.

The **Generate User OTP** page appears.

11. From the **OtpSubjectID** list, select **NEM**.

12. Click `Generate`.

The `Generate User OTP` page displays summary information about the user and the OTP for the user.

Note: The OTP expires 1 hour after you generate it.

The following figure provides an example of the `Generate User OTP` page.

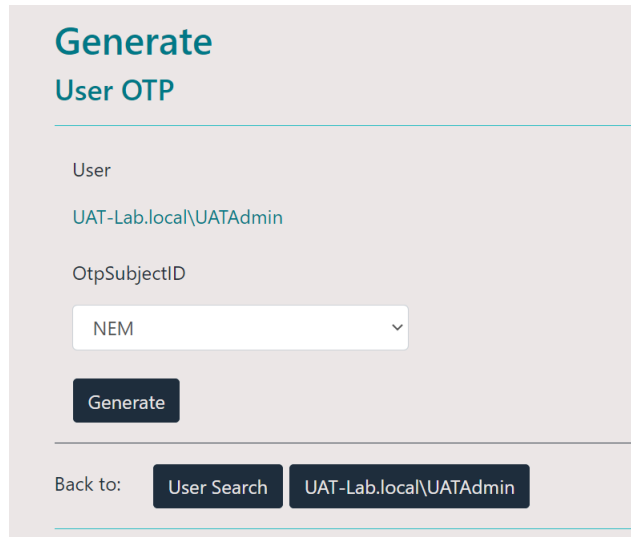


Figure 11: Generate OTP page

13. Log in to an enrollment terminal and start the `Nymi Band Application` by double-clicking the `Nymi Band Application` icon on the desktop.

14. In the `Username` and `Password` fields, type the Windows username and password of the user with the OTP, and then click `Sign In`.

The `Install application certificates` screen appears.

15. In the `One-time password` field, type the OTP value.

16. Click `Install`. When the operation completes successfully, the `Assign Nymi Band` screen appears.

17. Sign out of the `Nymi Band Application` by clicking `Sign out`.

Note: If you receive an error, refer to the *Nymi Connected Worker Platform Troubleshooting Guide*.

Updating the Nymi Band with Group Policy Changes

In situations where a group policy option, such as **Display Band Label on Nymi Bands**, **Nymi Lock Control**, **Liveness Detection**, or **Smart Distancing Reminders**, is updated in the active policy **after** Nymi Bands have been enrolled, Nymi Band users must update their Nymi Band configuration settings. Update the Nymi Band configuration settings by logging into the Nymi Band Application. Re-enrollment is not necessary.

Nymi Band Enrollment

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

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

Assigning the Nymi Band to the Enterprise

Each Nymi Band generates a unique setup code that identifies the Nymi Band to the Nymi Band Application and assigns the Nymi Band to the enterprise.

When the user wears the Nymi Band, and presses the top button, the setup code appears on the screen, as shown in the following figure.



Figure 12: Nymi Band Displaying a Sample Setup Code

The user performs the following steps to assign the Nymi Band to the enterprise environment.

1. Logs into an enrollment terminal.
2. Starts the Nymi Band Application by double-clicking the Nymi Band Application icon on the desktop.
3. Types their corporate credentials on the Sign in page, and then clicks **Sign In**. The corporate credentials of the user are verified against AD and application certificates are installed for secure communication.
4. On the Nymi Band, presses the top button to reveal the setup code.

- On the **Enter Setup Code** page, types the setup code that appears on the Nymi Band screen, and then clicks **Next**.

Note: The setup code changes if the user removes the Nymi Band from their wrist, or walks away from the enrollment terminal before completing the enrollment.

The following figure provides an example of the **Enter Setup Code** page.

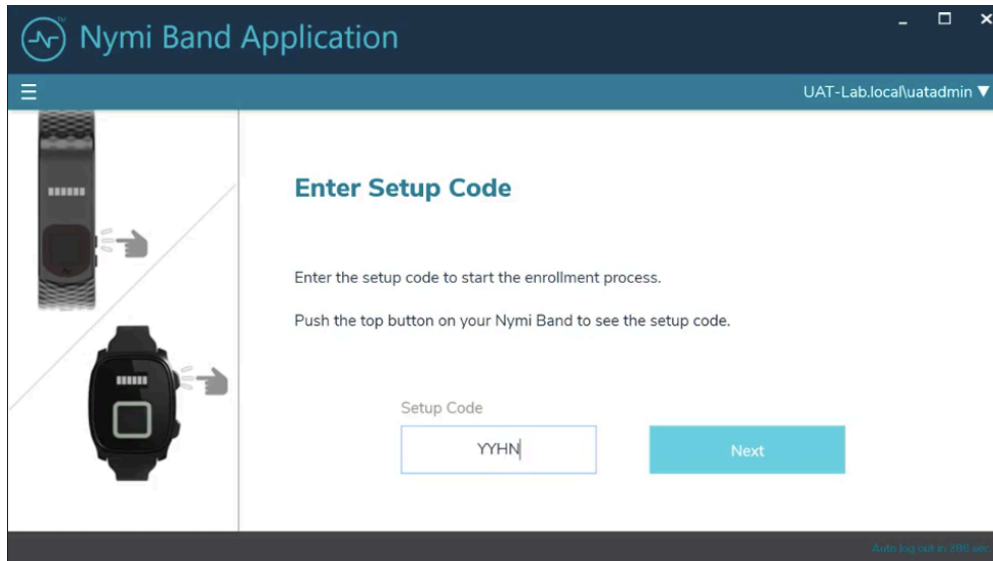


Figure 13: Enter Setup Code

After the user clicks **Next**, the **Add User** message appears on the Nymi Band screen, as shown in the following figure.



Figure 14: Nymi Band Add User Screen

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

Fingerprint Capture

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

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

- Is placed on the sensor only when prompted
- Is lifted from the sensor only when prompted

- Is placed on the middle of the sensor and covers as much of the sensor as possible
- Is motionless on the sensor, while the sensor is capturing the image

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

1. Reads the information on the **Capture Fingerprint** page, and then clicks **Start**.

The following figure provides an example of the **Capture Fingerprint** page.

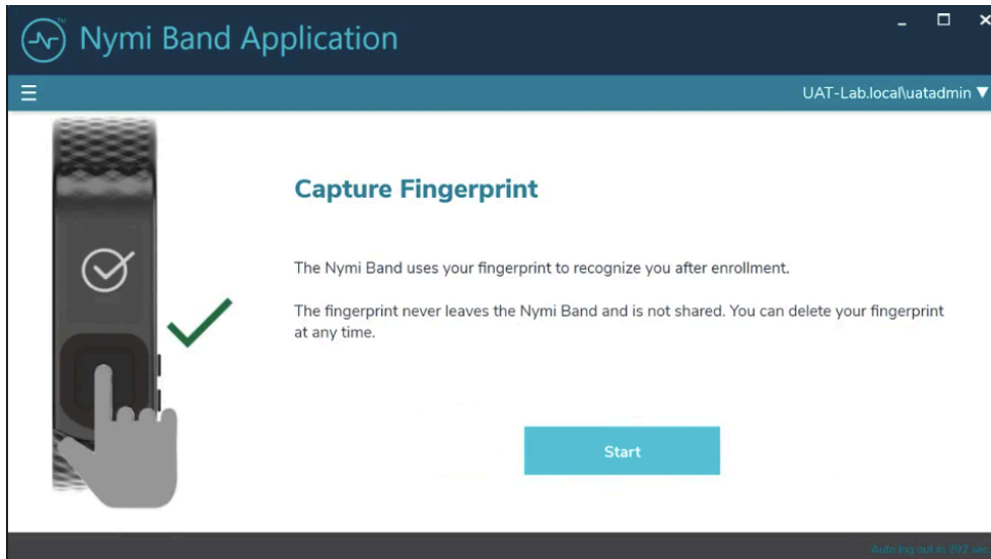


Figure 15: Capture Fingerprint

2. Waits for the **Fingerprint** icon to appear on the Nymi Band screen.
3. Places their finger on the fingerprint sensor and the fingerprint bezel that surrounds the sensor when the fingerprint icon appears, as shown in the following image.



Figure 16: FINGERPRINT

4. When the **LIFT FINGER** message appears on the screen, the user lifts their finger from the sensor and bezel.

When the **TOUCH SENSOR** message appears on the screen, the user places their finger on the sensor and bezel.

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



Figure 17: LIFT FINGER



Figure 18: TOUCH SENSOR

5. The user repeats the steps to lift their finger and touch the sensor and bezel, as prompted.



Figure 19: Success

When the Nymi Band fingerprint capture process completes, the results differ depending on the active group policy assigned through the NES Administrator Console. If the Band Label feature is enabled, users are prompted to assign the Band Label to their Nymi Band, as described in the next section.

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

Assigning the Band 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.

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

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

Note: This page appears when the NES Administrator selects the **Display of Band Label on Nymi Bands** option in the NES active group policy.

- **Customize Band Label**- Provides the user with the ability to customize a Band Label that appears on their Nymi Band when enrollment completes.

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

For more information about the Band Label policy options see, *Modifying the default policy*.

Preview Band Label

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

The following figure provides an example of the Preview Band Label page.

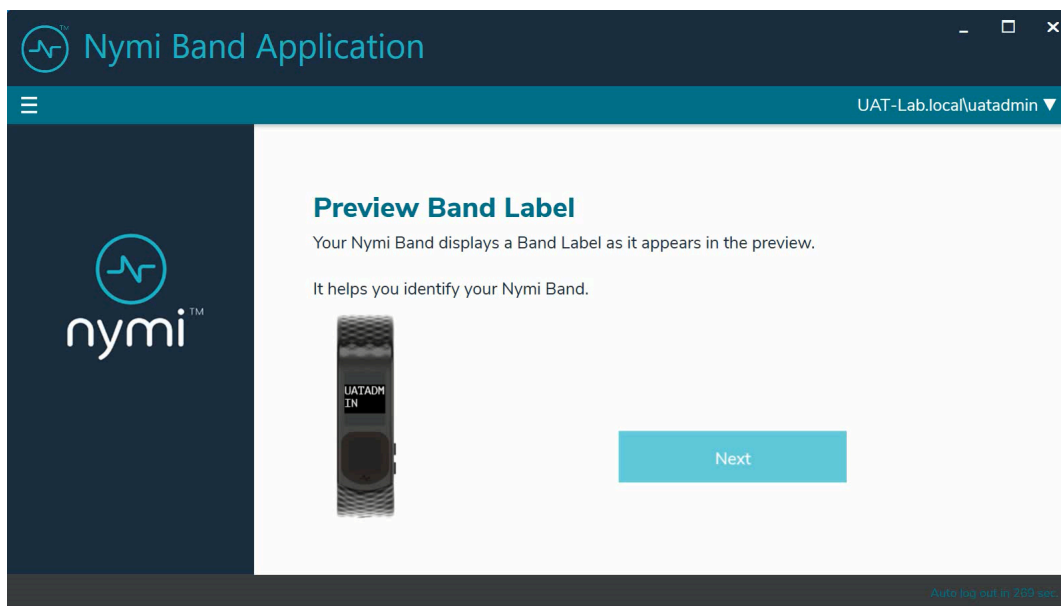


Figure 20: Preview Band Label

Click **Next** to continue the enrollment process.

Customize Band Label

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

Perform the following steps to customize the Band Label.

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

Supported Band Labels:

- Contain a maximum 12 characters
- Contain a combination of alphanumeric characters (all alpha characters display in uppercase on the Nymi Band)
- Contain a combinations of the following characters including spaces: A-Z, 0-9 and & ! " # \$ % ' () * + , . - \ / : ; < > = ? @ [] { } | ^ _ ` ~
- Do not contain leading or trailing spaces.

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

The following figure provides an example of the **Customize Band Label** page when unsupported characters are entered.

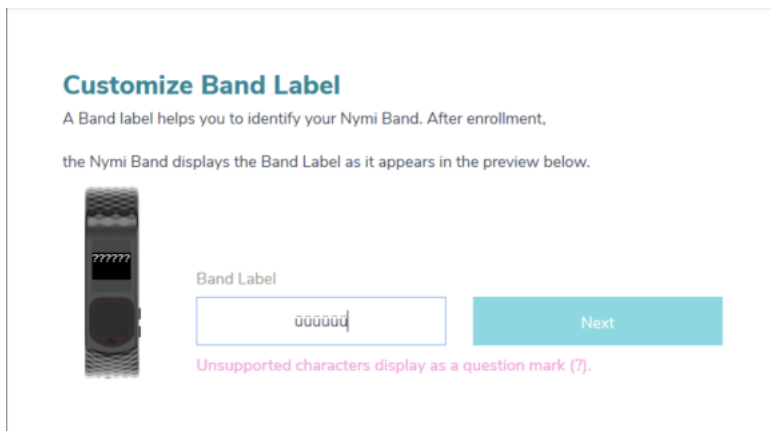


Figure 21: Custom Band Label Unsupported Characters

2. Review the Band Label in the Band Label preview.
3. Make any necessary modifications in the **Band Label** field.

4. Click **Next**, to save the Band Label and to proceed with the enrollment process.

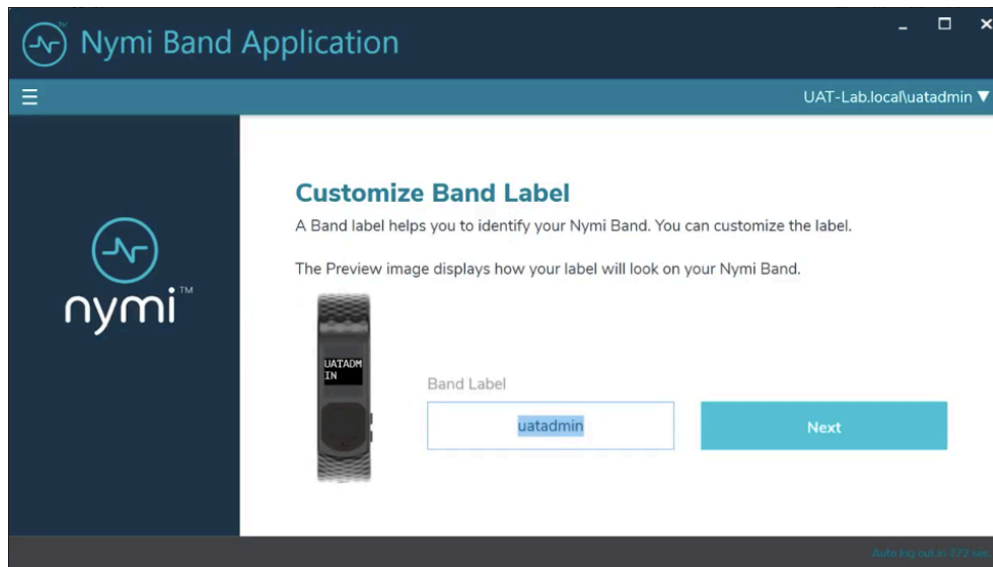


Figure 22: Custom Band Label Configuration

Applying Policy Settings

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

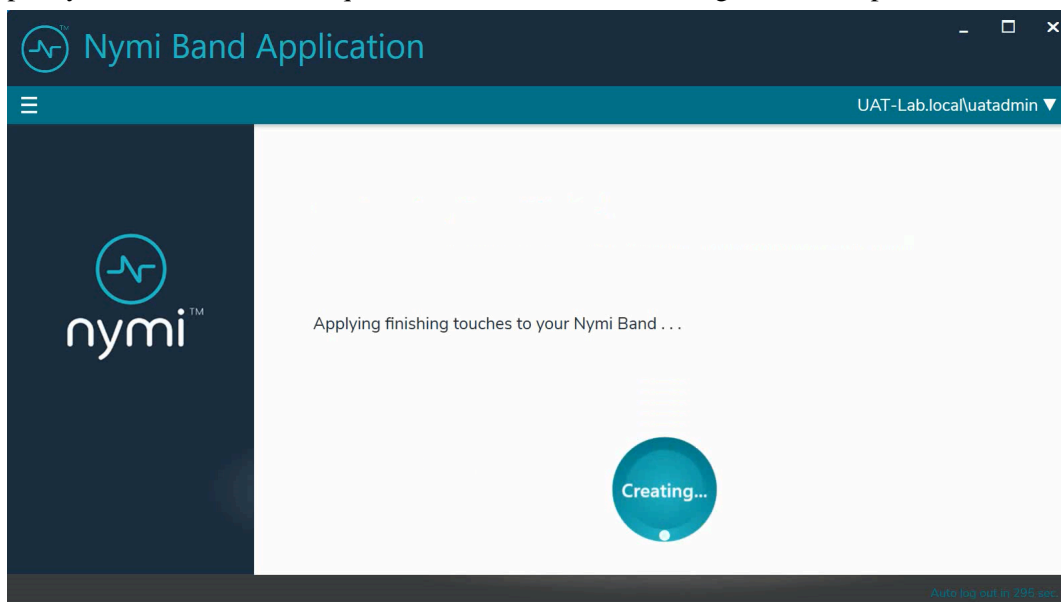


Figure 23: Applying Policy Settings

Completing Enrollment

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

The following figure provides an example of the **Success** page when enrollment completed successfully.

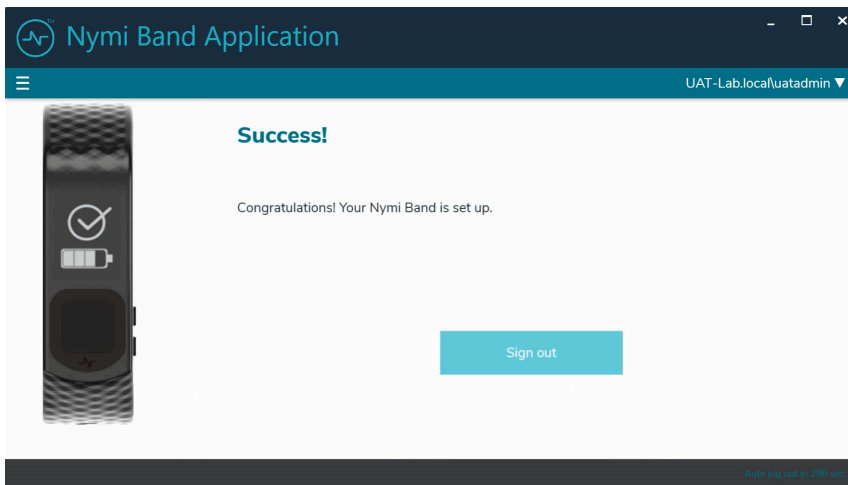


Figure 24: Success

Click **Sign out**. The Nymi Band is authenticated and ready for use by the user.

Interacting with the Nymi Band

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

Viewing Nymi Band Text

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

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



A B C D E F G H I J K L M
 N O P Q R S T U V W X Y Z
 0 1 2 3 4 5 6 7 8 9
 ! " # \$ % & ' () * + , . - \ /
 : ; < > = ? @ [] { } | ^ _ ` ~






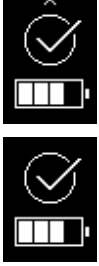

Figure 25: Nymi Band Font



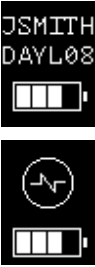


Viewing Nymi Band Screens

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

Table 7: Nymi Band Screen

Nymi Band Screen	Nymi Band Screen Name	Description
	Blank Screen	Indicates that you need to charge the battery or that the Nymi Band is in sleep mode. Press any button to wake up the Nymi Band.
	No User	Indicates that the Nymi Band is off-body and not assigned to a user and displays the battery charging level.

Nymi Band Screen	Nymi Band Screen Name	Description
	Setup code	Displays a message with letters and numbers when you wear an unenrolled Nymi Band. This is the setup code of the Nymi Band, which is used by the Nymi Band Application during the enrollment process.
	Add User	Appears after you type the setup code in the Nymi Band Application. When you see this message, follow the instructions in the Nymi Band Application to complete the enrollment process.
	Authentication Required	Indicates that you need to authenticate your identity. Hold your fingerprint on the fingerprint sensor to initiate the authentication process.
	Authentication In Progress	Indicates that the authentication process is in progress. Hold your finger on the fingerprint sensor until the screen shows the success indicator. The screen without the progress bar indicates the authentication process with Liveness Detection disabled.
	Success	Indicates a success based on user enrollment or user authentication. The top image is when Band Label is enabled and the bottom image is when the Band Label is disabled.
	Authenticated	Indicates that the Nymi Band is on-body and authenticated. The top image is when the Band Label is enabled and the bottom image is when the Band Label is disabled. The Nymi Band is ready to use.
	Authentication Lockout	Indicates that the user is locked out of the Nymi Band for the shown duration. The lockout prevents the user from authenticating with their fingerprint.

Nymi Band Screen	Nymi Band Screen Name	Description
	Keep Distance	Indicates that the user is in close proximity to another Nymi Band user. This image appears after prolonged close-proximity with another user, and if Smart Distancing and Contact Tracing is enabled.
	Deauthenticated	Indicates that the Nymi Band is deauthenticated. The top image is when Band Label is enabled, and the bottom image is when the Band Label is disabled or when authentication fails.
	Unauthenticated Band	Indicates that the Nymi Band is off-body. The top image is when Band Label is enabled and the bottom image is when the Band Label is disabled.
	Delete User Data	Indicates that the proces of deleting user data is running. Deleting user data on a Nymi Band removes all the data for the currently enrolled user from the Nymi Band.
	User Data Deleted	Indicates that the user data on a Nymi Band has been removed.

Viewing the Band Label

When the Band Label is assigned during enrollment, it displays on a Nymi Band that is:

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

On-Body and authenticated

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

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



Figure 26: Band Label on an enrolled and authenticated Nymi Band

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

Deauthenticated

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

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



Figure 27: Band Label on an unauthenticated Nymi Band

Enrolled and Charging, or on the Charger

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

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



Figure 28: Band Label on a charging Nymi Band

Nymi Band Dashboard

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

Nymi Band Vibration

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

Vibration Event	Details	When is it used
Acknowledgement	One short vibration. Used when the Nymi Band acknowledges that the user input has been received or to prompt the user to pay attention to the Nymi Band	<ul style="list-style-type: none"> Nymi Band detects user's finger at the beginning of an authentication Nymi Band starts charging
Success	Two short vibrations in quick succession. Used when the Nymi Band confirms an operation is successfully completed	<ul style="list-style-type: none"> Nymi Band's authentication success Fingerprint enrollment success Start of restart or security wipe sequence
Warning	Long vibration. Used when the Nymi Band confirms that an operation is successfully completed	<ul style="list-style-type: none"> Failed authentication Nymi Band transition from authenticated state to deauthenticated state
Smart Distancing Reminder	One short vibration. Used when the Nymi Band detects a close and persistent presence of another user wearing a Nymi Band enrolled in the contact tracing program. A reminder to keep distance is also shown on the Nymi Band.	<ul style="list-style-type: none"> Smart Distancing and Contact Tracing and Smart Distancing Reminders are enabled in the NES Two or more Nymi Band users are in close proximity to each other for at least 5 minutes

Tapping the Nymi Band

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

Note: Tapping the Nymi Band with a compatible BLE adapter requires you to first edit the Nymi Bluetooth Endpoint configuration file. Refer to *Editing the nbe.toml File* to enable BLE tap. In the *nbe.toml* file, change the value of *rssi_tap_threshold* to a non-zero, negative number to enable BLE tap. Nymi recommends -42.

Tips for tapping your Nymi Band

- For tapping to work, users must first authenticate their identity to the Nymi Band. If the screen on the Nymi Band is blank, press any button on the Nymi Band to wake it from sleep. If the screen remains blank, users need to charge the Nymi Band. If the screen displays the fingerprint image, users need to authenticate their identity.

- Users do not need to touch the face of the Nymi Band directly to the reader. Keep it just above the surface of the NFC reader (approximately 1 cm) or BLE adapter (within 10 cm).
- If tapping fails, move the Nymi Band away from the reader (30 cm or more) and then try again.
- Users may need to adjust the tapping speed. It should take approximately 1 second to move the Nymi Band towards and away from the reader.

Using Nymi Lock Control

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

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

The following image provides an example of the login screen when Nymi Lock Control is installed on the terminal.

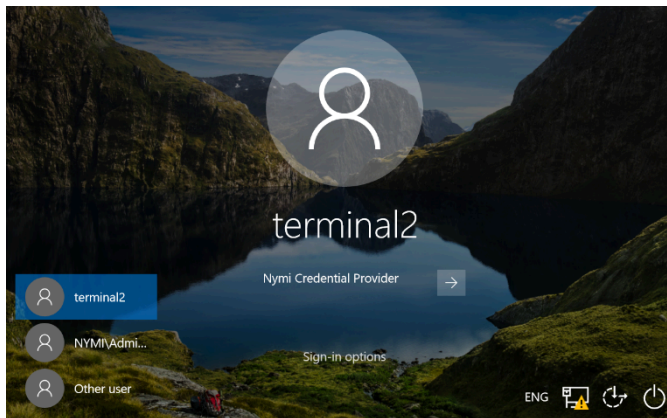


Figure 29: User Terminal Log in Screen with Nymi Lock Control

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.

To confirm Nymi Lock Control Recognizes the Nymi Band, the Nymi Band user performs the following steps:

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](#) on page 80 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.

Unlocking with an NFC or BLE Tap

Perform the following actions to unlock a user terminal by tapping the Nymi Band against an attached BLED112 adapter or an attached NFC reader.

1. Press any key to display the Windows Login screen.
2. Tap the authenticated Nymi Band against the BLED112 adapter or NFC reader.

If using a BLED112 adapter, press the Enter key or space bar on the keyboard to unlock the terminal.

Desktop unlocks.

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.

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.

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.

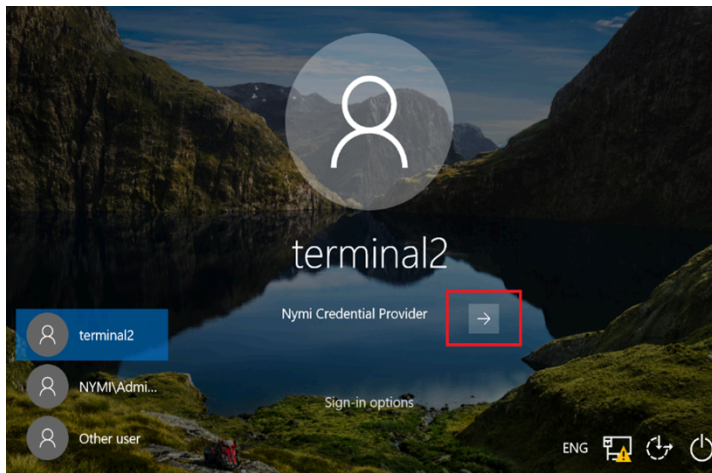


Figure 30: Nymi Credential Provider Submit button

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

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.

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.

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.

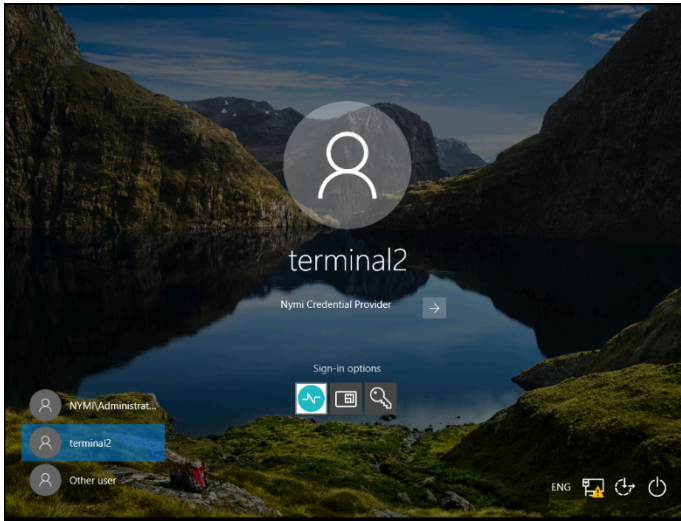


Figure 31: Sign-on Options screen

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.

Stopping Nymi Lock Control

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

Perform the following steps to stop the `Nymi Lock Control` application on the user terminal.

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

Nymi Band Management

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

Removing the Nymi Band

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

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



Figure 32: Deauthentication with Band Label enabled



Figure 33: Deauthentication with Band Label disabled

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

Storing the Nymi Band

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

- Store the Nymi Band in a dry and temperature controlled environment inside the range of 0°C to 45°C.
- Apply a label near or on the Nymi Band charger to allow users to quickly identify their Nymi Band when charging in mass charging configurations. The *Nymi Band Charging Recommendations Guide* provides information and references designs for charging station configurations.

Charging the Nymi Band

The Nymi Band is charged by placing it on a Nymi Band charger. The Nymi Band charger receives power from standard USB ports. It takes up to two hours to charge a fully depleted Nymi Band. A fully-charged Nymi Band typically has a 3-day battery life based on 300 BLE or NFC taps over 10 hours per day. Charging must occur in a temperature controlled environment inside the range of 15 to 30°C (59

to 86°F). This will ensure the Nymi Band charges in a timely manner and will maintain the longevity of the battery.

Nymi provides a custom charging cradle for charging the Nymi Band.



Figure 34: Battery Charger

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

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

To charge a Nymi Band, perform the following steps:

1. Plug the charging cradle into the USB port on your computer or a USB charging hub. A red LED indicator appears in near the top of the charging cradle indicating that it is receiving power.
2. Hold the cradle side of the Nymi Band charger close to the underside of the Nymi Band until it attaches magnetically. Make sure the pins on the charging cradle align with the port on the back of the Nymi Band. The Nymi Band vibrates indicating that it is receiving power. A blue indicator light appears on the side of the charging cradle to indicate that the user successfully connected the Nymi Band to the charging cradle and the Nymi Band is receiving power.

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



Figure 35: Charging battery indicator

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



Figure 36: Full battery indicator

Managing Battery Life

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

The Nymi Band has a typical 3-day battery life based on 300 BLE or NFC taps over 10 hours per day.

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

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

Additional icons display when the Nymi Band is:

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

Exiting Sleep Mode

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

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

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

Authenticating User Identity to the Nymi Band

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

Authentication by fingerprint

When the screen displays the fingerprint icon, the user holds their finger on the square fingerprint sensor and surrounding bezel. The Nymi Band displays the fingerprint authentication screen while fingerprint match and optional ECG liveness detection are in progress during authentication. The ECG liveness detection is automatically enabled for the default group policy. Refer to "Authentication Settings" in [Modifying the default group policy](#) on page 34 to disable ECG liveness detection.



Figure 37: Fingerprint Authentication screen

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



Figure 38: Success Screen with Band Label



Figure 39: Success Screen

Authentication Failure

Lockout policies help prevent adversarial users from gaining unauthorized access to systems through brute-force attacks. Nymi Bands will temporarily lock the wearer out after 5 consecutive, failed fingerprint match attempts. Every additional failed attempt will increase the lockout duration.

Authentication lockout is present for all Nymi Bands with the firmware released with CWP 1.1. To update the Nymi Band, refer to [Updating Nymi Band Firmware](#).

When an authentication fails, the Nymi Band vibrates and the authentication failure message appears. When the fingerprint icon appears, the user can try to authenticate again. If authentication fails 5 consecutive times (due to failed fingerprint match), the user will be temporarily locked out of their Nymi Band. During the lockout, a lock icon appears on the Nymi Band with the duration of the lockout. The first lockout persists for 1 minute and the duration will double after each failed fingerprint match,

up to a maximum of 60 minutes, as shown in the image below. The Nymi Band will return to normal behavior with a successful fingerprint match.



Figure 40: Fingerprint Authentication Lockout Screen

Note: The counts for authentication lockout only apply to failed fingerprint matches. Failures due to unrecognized ECG readings do not increase the count.

If the fingerprint authentication fails, ensure the following:

- User's finger and the sensor are clean and dry.
- User's finger is still on the sensor and bezel during the authentication period.
- User does not lift their finger off the sensor or bezel during the authentication period.

Clearing a Lockout

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

Clear the lockout by any of the following methods:

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

Note: Consider re-enrolling the user to the Nymi Band with another fingerprint if the user is repeatedly locked out with their fingerprint.

Authentication by corporate credentials

When the screen displays the fingerprint icon, the user logs into the Nymi Band Application, and clicks the **Authenticate** button.

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

Cleaning the Nymi Band

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

Restarting the Nymi Band

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

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

Perform the following steps to restart the Nymi Band.

1. Ask the user to remove the Nymi Band.
2. Plug the Nymi Band into a charger.
3. Press and hold the top button, the word **RESTART** and a countdown progress bar appears on the screen. Continue to hold the top button for 10 seconds to complete the countdown, and initiate the restart procedure. The following figure shows the **RESTART** message with countdown.



Figure 41: RESTART message

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

Nymi Band Firmware Update Utility

Nymi provides you with a utility that enables you to update the firmware on one or multiple Nymi Bands. This utility is intended to be used in an unattended or batch mode, which simplifies the process of updating a large number of Nymi Bands. During the update process, the utility provides the operator with high-level status information about the process. The upgrade process generates a log file that details the Nymi Bands that were updated, including serial numbers and firmware versions.

Firmware Update Workflow

When you run the update utility, it determines if there are any Nymi Bands in the vicinity that are on charge and require an update. The firmware update utility only updates Nymi Bands with an older firmware.

If the utility detects a Nymi Band that requires a firmware update, the utility performs the following actions:

- Prepares to install the update. The Nymi Band screen displays **STAND BY**.
- Transfers the firmware to the Nymi Band. The Nymi Band screen displays **DOWNLOAD** with a progress bar.
- Restarts the Nymi Band and applies the firmware update to the Nymi Band. The Nymi Band screen displays messages about the update progress.
- The Nymi Band displays **SUCCESS**, for a brief period of time, after it is updated.

- When the utility completes a Nymi Band update, the utility scans for other Nymi Bands in the vicinity (within Bluetooth range) that require an update. If a Nymi Band is found, the update is started on another Nymi Band.
- The utility keeps running until terminated by the user.

Note: If the Nymi Band uses recovery firmware, the messages that are displayed during a firmware update may be different than what is indicated above.

Determining Nymi Band Firmware Version

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

1. Remove the Nymi Band from the wrist of the user.
2. Put the Nymi Band on the charger.
3. Press and release the top and bottom button.

The firmware version appears on the screen, as shown in the following figure.



Figure 42: Nymi Band firmware version

Before you perform a firmware update

Firmware update recommendations

- Nymi recommends that you update the firmware on a maximum of five Nymi Bands at one time. Attempting to update more than five concurrently may require the user to stop and manually restart the utility.
- You may need to disable or extend sleep mode on the Windows computer to prevent the utility from terminating when the computer goes to sleep. When the utility terminates, Nymi Bands that were in the process of downloading software will revert back to the previous firmware version. If the firmware update terminates, restart the *fw_updater* utility, which will restart the upgrade process on Nymi Bands, that are on charge, require an update, and are within Bluetooth range.
- To display additional help information while using the firmware update utility, run the `fw_updater_gold_v<version>.exe` application with the `--help` argument.
- The `fw_updater_gold_v<version>.exe` utility requires the Nymi Band to be in close proximity of the Bluetooth adapter(s) before the firmware update transfers to the Nymi Band. The range varies with the environment, and the default range is approximately 6-18 inches. The default range is limited to avoid unintended updates of Nymi Bands. If an increased range is desired, run the `fw_updater_gold_v<version>.exe` utility with the `--rssi <value>` argument, with `<value>` having a range of -50 to -99. A lower RSSI value (closer to -99) provides longer range, while a larger value (eg. -50) will decrease it. By default a value of -60 is used.

Requirements for multiple Nymi Band update

- A Nymi Band with a charging cradle or multiple Nymi Bands to update
- A USB hub with one or more (up to a maximum of five) Bluetooth adapters plugged into it
- One charging cradle for each Nymi Band
- The executable file has the same version number as the fw_updater utility executable file (*fw_updater_gold_v<version>.exe*)
- Windows 10 computer

Updating Nymi Band Firmware Overview

During a firmware update, the utility provides you with update and status information, such as:

- Firmware version
- Number of BLE adapters that are available
- Number of Nymi Bands that are in the process of being updated
- Total number of Nymi Bands that are updated during the session

Updating Nymi Band Firmware

Perform the following steps to concurrently update the firmware on multiple Nymi Bands.

1. Download and extract the firmware package into a directory of your choice on a Windows computer. For example, *C:\Nymi_firmware*.
2. If the Windows machine has the Nymi Band Application or Nymi Runtime installed on it, stop the Nymi Bluetooth Endpoint service.
3. Plug the USB hub into an electrical outlet, and then into a USB port on the Windows machine.
4. Put up to five Nymi Bands on charge. Plug each charging cable and up to five Bluetooth adapters into the USB hub. Double-click the *fw_updater_gold_v<version>.exe* executable in the file folder.

Note: If you put a drained Nymi Band on charge, the charging icon appears, and the upgrade process starts when there is a sufficient battery charge on the Nymi Band.

On start up, the application scans the Bluetooth adapters on the USB hub for a Nymi Band that has a firmware version that is older than the version in the firmware package, or a Nymi Band with recovery firmware. A firmware transfer starts for each detected Nymi Band.

5. The Nymi Band automatically restarts when the download completes, and then completes the firmware update process. A brief SUCCESS message appears.

As each Nymi Band firmware update completes, take the completed Nymi Band off charge and plug in another Nymi Band that requires updating. The firmware update utility continues to scan for Nymi Bands that require an update.

6. To stop the application, press **Ctrl+C**.
7. If required, restart the Nymi Bluetooth Endpoint service before using the Nymi Band Application or an application that uses Nymi Runtime.

Firmware updater log files

At any time during the firmware update process, you can view firmware log file information. The *result_log.csv* is available in the same directory where the *fw_updater_gold_v<version>.exe* file is executed. You can provide this file to Nymi Support when troubleshooting is required. Alternatively, if a *--log* argument was provided using a command line, then the log is available in the directory determined by the user.

The *fw_updater.log* file contains system diagnostic information about actions that are run during Nymi Band firmware upgrades. This file is required by Nymi Support to help resolve Nymi firmware issues regarding upgrades.

Nymi creates a maximum of 5 rotating log files. Each of these log files cannot exceed 10MB.

Administrative Actions

This section provides information about tasks that you might perform in the NES Administrator Console while managing the Connected Worker Platform.

Policy Management

This section describes how to perform common policy tasks such as editing policies, changing the active policy, and deleting policies.

Editing policies

Perform the following steps in the NES Administrator Console to modify the attribute values of an existing group policy.

For example, to change the enrollment URL.

1. From the navigation bar, select **Policies**.
2. On the `Group Policy` page, to the right of the configuration that you want to edit, click the policy description. See the section *Creating a new policy* for information about each policy option.
3. On the `Edit Group Policy` page, update the values for any attributes that you want to change.
4. Click **Save**.

Changing the active policy

NES can only have one active policy.

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

1. From the navigation bar, select **Policies**.
2. On the `Group Policy` page, click the description of the policy that you want to set as the active policy.
3. On the `Edit Group Policy` page, select the **Is Active** checkbox.
4. At the bottom of the page, click **Save**.

Deleting policies

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

1. From the navigation bar, select **Policies**.
The `Group Policy` page appears with a table that displays a list of existing policies.
2. If the policy that you want to delete is active, edit the policy, and then clear the **Is Active** option.
3. Edit one of the remaining policies and select the **Is Active** option.
Note: NES must always have one active policy.
4. To the right of `Policy` table, beside the policy that you want to delete, click **Delete**.

Nymi Band User Management

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

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

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

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

NFC (Unique Identifier) UID Management

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

Searching for User or Nymi Band Information

The **Search** page enables Administrators to search the NES database for information about users 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 using the Nymi Band serial number

Searching for Users

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

1. From the NES Administrator Console, select **Search**.
The **Search** page appears.
2. In the **Search** page, select the **Users** option.

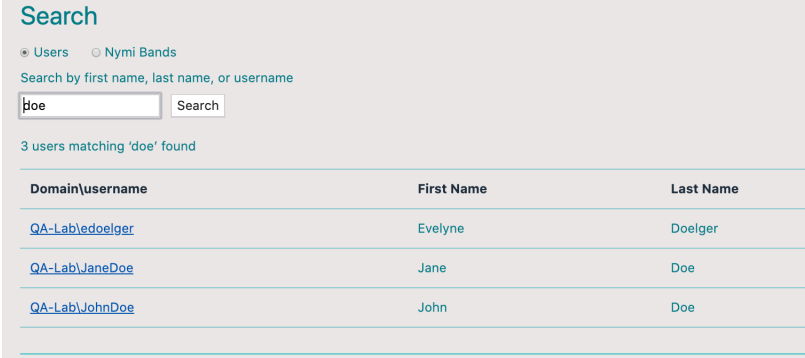
3. In the **Search** field, type the full or partial criteria for the following:

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

Note: If more than 12 results are returned, the following warning message appears, **Too many matches were found. The first 12 matches appear below. Repeat the search by entering a more specific search string.**



The screenshot shows a search interface with the following elements:

- Search bar with the text "doe" and a "Search" button.
- Radio buttons for "Users" (selected) and "Nymi Bands".
- Text: "Search by first name, last name, or username".
- Text: "3 users matching 'doe' found".
- Table with 3 columns: Domain\username, First Name, and Last Name.

Domain\username	First Name	Last Name
QA-Lab\doelger	Evelyne	Doelger
QA-Lab\JaneDoe	Jane	Doe
QA-Lab\JohnDoe	John	Doe

Figure 43: Users Search Results Page

The `Search` page displays the following information:

- the user or a list of up-to 12 users that match the search criteria
- a summary message with the number of search results matching

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

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.

The screenshot shows the 'User' details page in the NES Administrator Console. The user's login ID is 'QA-Lab.local\uat1', created on '2020-04-28'. A 'Notes' field contains the text 'Created from AD search result.' Below the notes is a 'Save' button. Underneath is a section for 'Nymi Bands' with a table containing one entry: 'Y99D100U1', which is 'Active' and 'Primary', with a note 'Load test band' and a creation date of '2020-04-28'. A 'Disconnect' link is provided for this band.

Figure 44: User Details Page

Table 8: User Details Summary

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

Searching for Nymi Bands

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

1. From the NES Administrator Console, select **Search**.
The Search page appears.
2. In the Search page, select the **Nymi Bands** option.

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

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

Note: If more than 12 results are returned, the following warning message appears, **Too many matches were found. The first 12 matches appear below. Repeat the search by entering a more specific search string.**

Figure 45: Nymi Band Search Results Page

The Search page displays the following information:

- returns a list that matches the serial number. The list contains the serial number, the Domain\username, first name and last name of the user
 - a summary message with the number of search results matching
- 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.

Nymi Band Details Page

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

Table 9: 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.

Field	Description
Security App Key	Displays the status of the symmetric key ID of the Nymi Band. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> If a policy enables the use of External Authenticator, the field displays Created If a policy is not configured to enable the use of an External Authenticator, the field displays Not Created
Serial Number	Displays the unique value that is located on the back of the Nymi Band.
Encrypted Password	Indicates if the user's password was encrypted and saved in NES database. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> If the fingerprint step was performed, the field displays Yes If the fingerprint step was not performed, the field displays No
Band Label	Displays the Band Label assigned to the Nymi Band. Band Labels can only be assigned to Nymi Band 3.0, when the active policy is configured to support the option.
Firmware Version	Displays the version of the Nymi Band firmware at the time of enrollment.
Created	Displays the date that the Nymi Band was registered to the user or the first time that an NES Administrator searched for the user.
Modified	Displays the date that the Nymi Band assignment was modified.
Is Active	Displays Active when the Nymi Band is active and is empty when the Nymi Band is disabled.
Is Primary	Displays Primary when the user has at least one Nymi Band assigned, and the Nymi Band is the primary Nymi Band. Appears empty when the Nymi Band is a temporary Nymi Band.
Notes	Displays an informative message about the Nymi Band that was supplied by the administrator.

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

The screenshot shows the 'Nymi Band' details page in the NES Administrator Console. The page has a teal header with the Nymi logo and navigation links: NES Administrator Console, Policies, Search, About, Support, Regulatory Statements, and Logout. The main content area is light gray and contains the following details:

- Domain \ Username:** QA-Lab.local \ JaneDoe
- Band ID:** DF:A7:07:7D:42:F9
- NFC UID:** 5F6977841C41EE
- Security App Key:** Created (with a checked checkbox)
- Corp. Credentials Auth.:** Created (with a checked checkbox)
- Serial Number:** NAHAVCPEGEDG (with a checked checkbox)
- Encrypted Password:** Missing (with a text input field)
- Has Fingerprint:** Yes (with a text input field)
- Band Label:** JANE DOE
- Firmware Version:** 4.0.2
- Created:** 2020-03-31
- Modified:** 2020-03-31

A 'Save' button is located below the 'Encrypted Password' field. At the bottom left, there is a link 'Back to Owner'.

Figure 46: Nymi Band Details page

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.

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

This process involves two main steps:

- suspending the user's existing Nymi Band
 - enrolling the temporary Nymi Band to the user
1. In the NES Administrator Console, select **Search**.
 2. In the **Search** page, select the **Users** Option.
 3. In the **Search** field, type the full or partial username, first name, or last name of the user.
 4. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
 5. Select the Domain\username link of the user. to open the **User Details** page.
 6. Click the Serial Number of the original Nymi Band. The Nymi Band page appears.

7. Clear the **Is Active** box.
8. Select the **Is Primary** box.
9. 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.

10. Contact the user to enroll the temporary Nymi Band.
11. 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.

Restoring the Nymi Band

Perform the following steps in the NES Administrator Console to restore the Nymi Band configuration for a user who was issued a temporary Nymi Band.

1. In the NES Administrator Console, select **Search**.
2. In the **Search** page, select the **Users** Option.
3. In the **Search** field, type the full or partial username, first name, or last name of the user.
4. Click **Search**. The **Search** page displays the user, or a list of users that match the search criteria.
5. Select the **Domain\username** link of the user. to open the **User Details** page.
6. On the **Users** page, click the Serial Number for the primary Nymi Band. The **Edit Nymi Band** page appears.
7. Select the **Is Active** box and (if necessary) the **Is Primary** box.
8. 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.

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

This process involves two main steps:

- suspending or deleting the user's existing Nymi Band.
- enrolling the Nymi Band to the user.

Note: In this release, if you delete the existing Nymi Band, you will lose the ability to track historical data.

Perform the following steps to suspend the original Nymi Band and then enroll the new Nymi Band to the user.

1. In the NES Administrator Console, select **Search**.
2. In the **Search** page, select the **Users** Option.
3. In the **Search** field, type the full or partial username, first name, or last name of the user.
4. Click **Search**. The **Search** page displays the user, or a list of users that match the search criteria.
5. Select the Domain\username link of the user. to open the **User Details** page.
6. Click the Serial Number of the original Nymi Band. The **Nymi Band** page appears.
7. Clear the **Is Active** box.
8. In the **Notes** field, add descriptive information, such as **Lost Band**.
9. Click **Save**.
The original Nymi Band is disabled.
10. Contact the user to enroll the new Nymi Band by using the Nymi Band Application.
11. When the enrollment succeeds, 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**.
12. If the original Nymi Band is found, perform a Delete User Data process of the original Nymi Band.

Suspending the primary Nymi Band for a user

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

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

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

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 process on the Nymi Band.

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

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

1. In the NES Administrator Console, select **Search**.
2. In the **Search** page, select the **Users** Option.
3. In the **Search** field, type the full or partial username, first name, or last name of the user.
4. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
5. Select the Domain\username link of the user. to open the **User Details** page.
6. 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**.
7. On the Disconnect screen, scroll to the bottom and select **Disconnect**.

Deleting User Data

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

1. Remove the Nymi Band from the wrist of the user, and then attach the Nymi Band to a charger.
2. On the Nymi Band, hold the bottom button. The Delete User Data message displays on the screen, as shown in the following figure.



Figure 47: Delete User Data

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



Figure 48: User Data Deleted

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.

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

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

1. Perform a delete user data process of the Nymi Band. See section *Deleting User Data* for more information.
2. In the NES Administrator Console, select **Search**.
3. In the **Search** page, select the **Users** Option.
4. In the **Search** field, type the full or partial username, first name, or last name of the user.
5. Click **Search**. The *Search* page displays the user, or a list of users that match the search criteria.
6. Select the Domain\username link of the user. to open the **User Details** page.
7. 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**.
8. Provide the user with the new Nymi Band and ask the user to enroll the Nymi Band.
9. In the **Search** field, type the full or partial username, first name, or last name of the user.
10. Select the Domain\username link of the user. to open the **User Details** page.
11. In the Nymi Band table, confirm that the Nymi Band is **Active**.

Resetting an Expired Password

1. (Optional) If you have Nymi Lock Control, ensure that it is enabled in the group policy (refer to [Modifying the default group policy](#) on page 34). If you enable Nymi Lock Control after changing the password, you will have to re-log into the Nymi Band Application to apply changes to the Nymi Band.

2. If your password is expired, you will be prompted to change your password. Perform the following steps:

- a. Click **OK**.

The `Nymi Credential Provider` window appears prompting the user for their password.

- b. Click the **Sign-in** option.
- c. Select the Key icon.
- d. Enter the current password for the user and then click **OK**.

A message appears and states that the password has expired.

- e. Click **OK**. A window appears to update the password.
- f. In the **Password** field, type the current password.
- g. In the **New password** field, type a new password.
- h. In the **Confirm password** field, type the new password again.
- i. Press **Enter**.

A message appears advising that the password has changed. Desktop appears.

- j. Log into the Nymi Band Application with your new credentials while wearing your authenticated Nymi Band.

NES Audit Logging

Nymi stores information related to specific NES events 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.

Accessing this data enables users to gather useful information for audit and compliance purposes.

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`.

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 audit tables. By default, the account that installs the SQL server software has read access to the NES database. In addition Auditor account configured during installation has 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.

Viewing all Audit Log data using SQL Queries

Audit information can be viewed in SQL database tables.

Changes are entered into the database when changes are made to NES objects, such as configuration settings and data. When changes are made to these objects (such as creating, updating, deleting) the system saves them into the appropriate SQL tables.

- `audit.UserCore`: This table contains audit log data pertaining to NES users. The table contains data including, but not limited to, user name, event time, event type, domain data.
- `audit.NymiBand`: This table contains audit log data pertaining to Nymi Band events. The table contains data including but not limited to, users, user ID, event type, Nymi Band ID, serial number, and additional information.
- `audit.ApplicationSetting`: This table contains audit log data pertaining to NES application settings. The table contains data including but not limited to, identity, event time, ID, `AutoLogoutTimeoutSeconds`, `FingerprintRequirement`.
- `audit.ExternalAuthenticator`: This table contains audit log data pertaining to external user authentication events. The table contains data including but not limited to, username, event time, event type, public key, band external authenticator ID and additional information.

Review audit log information in the tables, by running SQL queries with a user account that has read access to the target NES database. By default, the account that installs the SQL server software has read access to the NES database. To perform queries, install a SQL querying tool such as SSMS or a custom-built application that is capable of running T-SQL queries.

Note: Ensure that the SQL Server querying tool or custom-built application is installed prior to running database commands.

Viewing audit tables

Use an SQL Management application such as SSMS to view the audit tables:

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)Tables*.
4. Select the audit table that you want to view.

Querying 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. Use a SQL Management application such as SSMS to query the audit tables from the GUI or command line.

To query for all values in an audit table by using the SSMS GUI, perform the following actions:

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

For example, to retrieve the data for an audit table type the following command: **SELECT * FROM [audit].[table_type]**

where *table_type* is one of the following values: *ApplicationSetting*, *Certificate*, *ExternalAuthenticator*, *NymiBand*, *UserCore*

The following figure provides an example of a query for all entries in the *audit.UserCore* table and the corresponding results

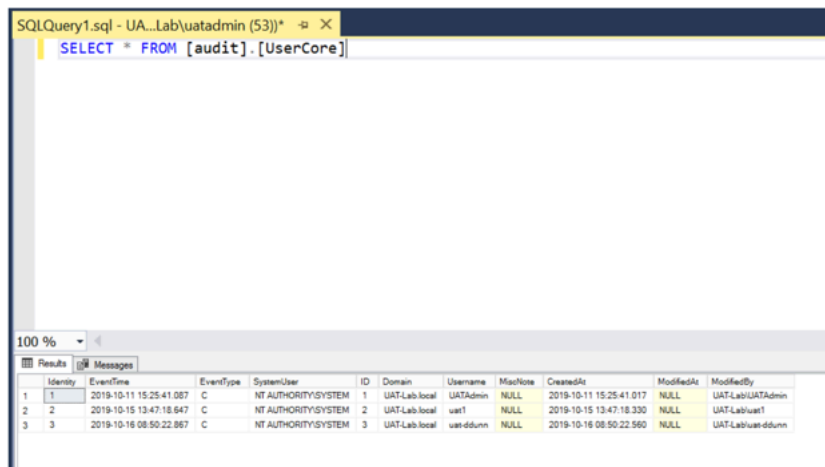


Figure 49: Querying *audit.UserCore* table

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.

Nymi Band Application log files

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

Saving Nymi Band Application log files

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

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**.

Viewing Nymi Band Application log files

Perform the following actions to view the log files.

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.

NES log files

The NES host has separate log files for each web service. When you encounter an issue, enable verbose mode for each web service, retry the operation, and then review the messages that appear in each log file.

Enabling debug mode

By default, NES does not provide detailed logging.

To enable debug mode, perform the following steps.

1. Edit the `C:\inetpub\wwwroot\nes_service_name\nes\web.config` file and in the `<system.diagnostics>` section, change the value for each `add name` parameter from **Information** to **Verbose**.

For example:

```
<system.diagnostics>
<switches>
  <add name="Global" value="Verbose" />
  <add name="Authentication" value="Verbose" />
</switches>
</system.diagnostics>
```

2. Edit the `C:\inetpub\wwwroot\nes_service_name\nenrollment\web.config` file, and in the `<system.diagnostics>` section, change the value for each `add name` parameter from **Information** to **Verbose**.

For example:

```
<system.diagnostics>
  <switches>
    <add name="Global" value="Verbose" />
    <add name="Authentication" value="Verbose" />
    <add name="CertificateEnrollment" value="Verbose" />
  </switches>
</system.diagnostics>
```

3. Edit the `C:\inetpub\wwwroot\nes_service_name\authenticationservice\web.config` file, and in the `<system.diagnostics>` section, change the value for each `add name` parameter from **Information** to **Verbose**.

For example:

```
<system.diagnostics>
<switches>
  <add name="Global" value="Verbose" />
  <add name="Authentication" value="Verbose" />
</switches>
</system.diagnostics>
```

4. Restart the IIS.

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`

Submitting a support request

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

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.

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.

Follow these steps to generate a log zip file.

1. On the computer running NES, open Windows Explore and navigate to the directory that contains the NES Installation package folder in the *NesSystemInfo* subfolder.
2. Double-click *NymiSupportTool.exe*
The User Account Control dialog box appears.

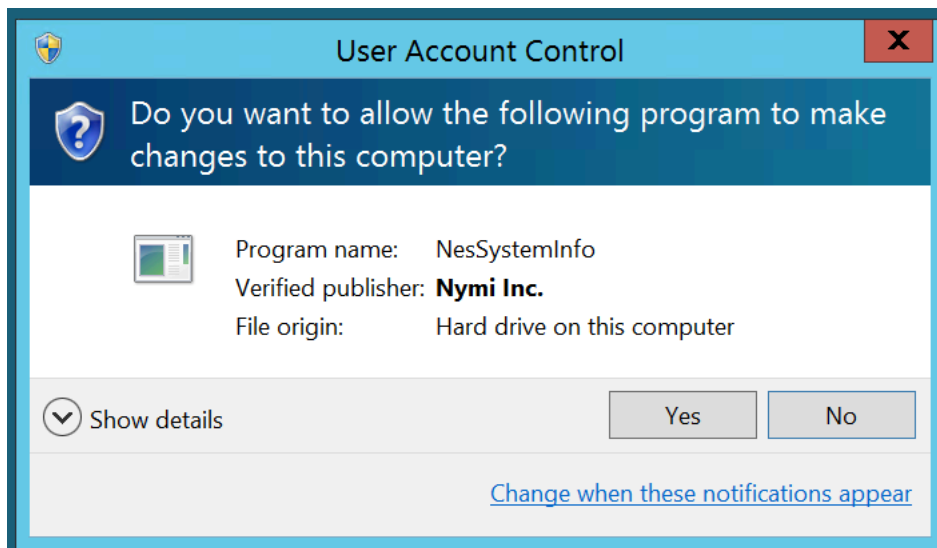


Figure 50: The User Account Control

3. Click **Yes** to start the script.

The script collects log information. A window appears that contains a folder with a zip file.

4. 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.

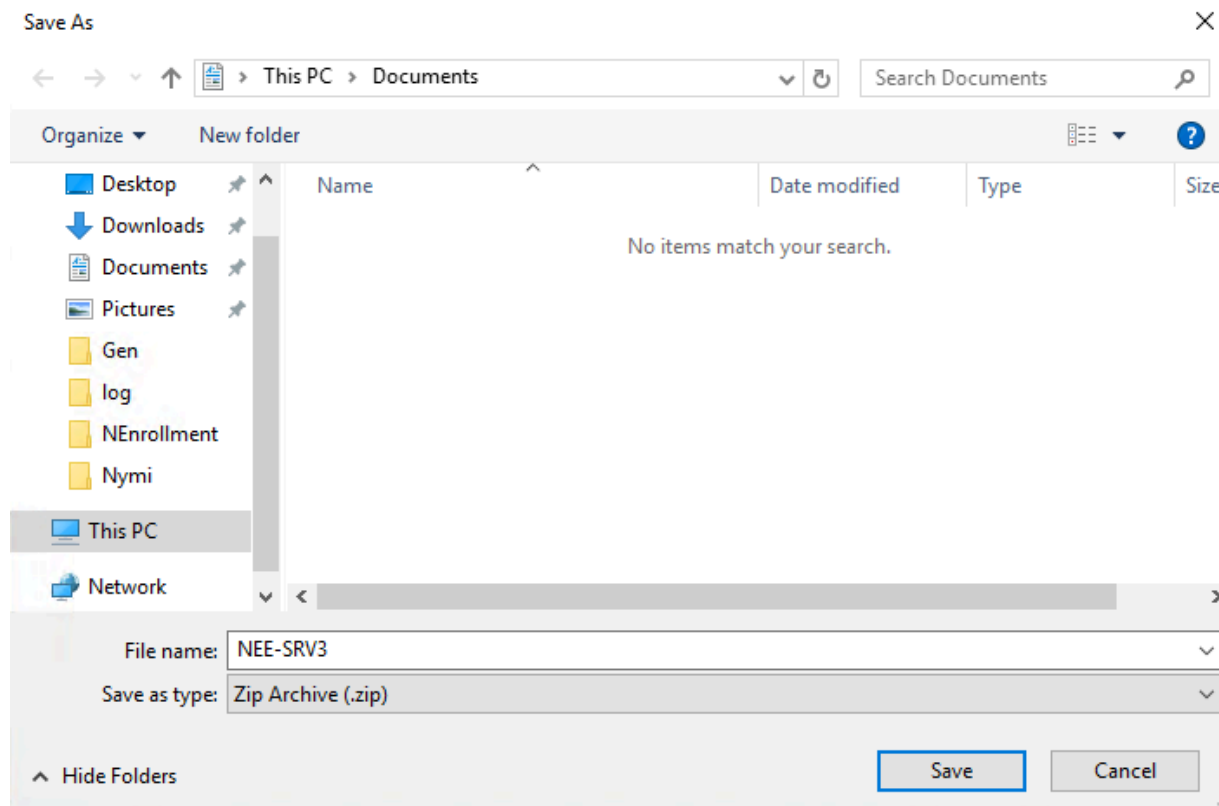


Figure 51: Saving Nymi Support Tool zip

Manage the Connected Worker Platform Environment

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

Manage NES

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

NES Backup and Recovery

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

NES backups

To protect the Connected Worker Platform and certificate data on the NES host, perform a backup of the SQL databases.

If the NES host is a virtual machine (VM), you can use VMware vMotion or recovery snapshots to protect the VM.

Administrators also need to store the `fullchain.p12` file and the accompanying password in a secure location for recovery purposes.

Performing SQL database backups

NES stores Nymi Band information and usernames 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 software to back up the SQL database.

See [Microsoft](#) for more information about how to protect the SQL server.

Note: A SQL backup does not back up any assigned one-time passwords (OTPs). After you complete a SQL recovery, you will need to assign OTPs to users, as required.

NES recoveries

This section describes how to restore NES data on the original NES host, when you were not required to install a new operating system.

Recovering NES-specific configuration

To recover the NES configuration, do the following:

- install NES, which includes certificate installation using the `fullchain.p12` file
- recover the SQL database and re-run the NES Setup wizard to configure NES

Upgrading NES

You can upgrade earlier versions of NES to the current version of NES. To upgrade a NES implementation that uses ADCS/NDES to manage certificates, you must refer to the Nymi Connected

Worker Platform Migration Guide for detailed information on migrating to the Nymi Token Service (NTS) for NES certificate issuance method.

Nymi Token Service (NTS) issues authentication tokens to NEAs that allow the NEAs, including the Nymi Band Application, to authenticate to Nymi Bands that are enrolled in the enterprise. NTS provides you with a simplified, secure deployment that does not require ADCS/NDES user accounts and reliance on specific user account permission requirements in AD security policies.

To upgrade a previous version of NES that uses NTS, perform the following steps:

Note: For upgrades from NES 2.X, Microsoft .NET framework will be upgraded to Microsoft .NET Framework 4.8.

1. Extract the NES installation package to a local directory on the NES host.
2. From the directory that contains the extracted NES installation package, run `..\NesInstaller\install.exe`.
3. On the User Access Control window, click **Yes**.
4. On the Open File - Security warning window, click **Run**.
5. 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.
6. On the Application Install Security Warning window, click **Install**.
7. On the Open File - Security warning window, click **Run**.
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 NES 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.

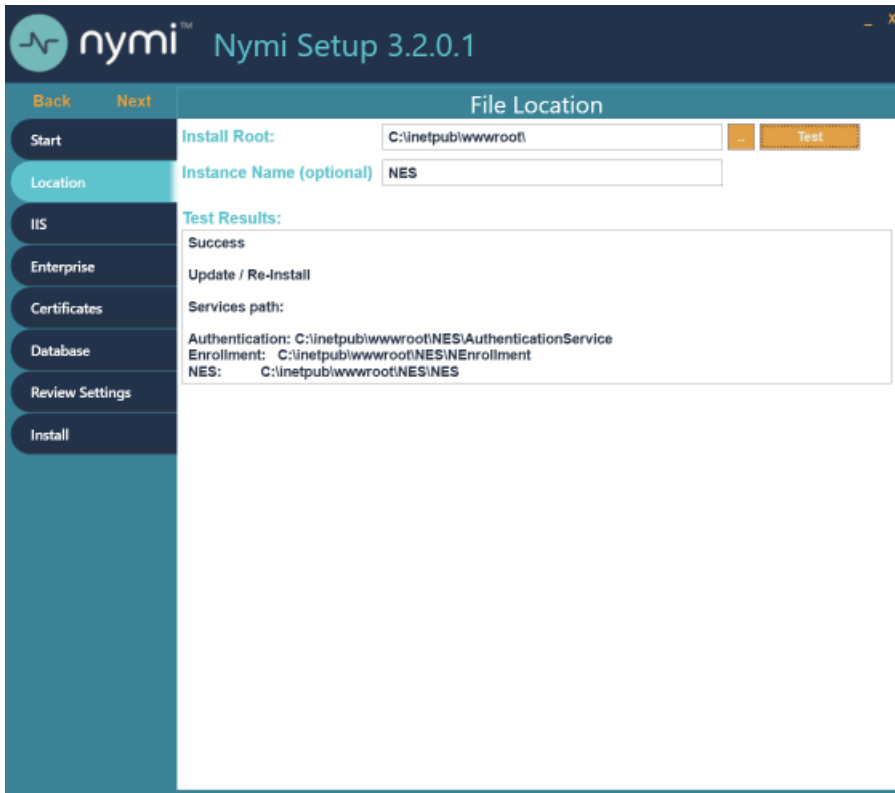


Figure 52: Update / Reinstall installation type

9. On the left navigation pane, click **Install**.

10. Click **Update**.

Note: If the update option is not available, the **Install Root** or **Instance Name** fields on the **Location** tab are not the same values that were specified when you deployed the previous NES version.

11. On the Level Two certificate warning window, click **OK**.

12. On the Update NES window, click **Yes** to reapply the configuration.

The Install window display the status of the upgrade process.

13. When the Install window displays the Installation Complete message, close the Nymi Setup window.

Uninstalling NES Installer

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

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**.

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.

Accessing NES Administrator Console

Perform the following steps to connect to the NES Administrator Console and the System Diagnostics page.

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://server-2.nymi.lab/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.
2. Click the **Sign in** button.
The Sign in dialog opens. Enter username and password.
3. Verify the username has administrative access by observing **Policies**, and **Search** in the main menu.

The *Nymi Connected Worker Platform Troubleshooting Guide* provides information about how to resolve issues that you might encounter when you try to access the NES Administrator Console.

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 10: 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 11: 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 12: 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 13: 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 14: 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.
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 15: 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.
OTP	Provides details about acquiring OTP from Enrollment Service. Indicates a Pass or Fail. See the Nymi Connected Worker Platform Troubleshooting Guide for more information.
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.

Service	Description
L2 Cert Validity	Indicates if the certificate is valid. Provides the expiry date (m,d,y) of the NES L2 certificate.

Table 16: 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.

Certificate Management

This section provides information about managing L2 and TLS certificates, including how to determine the expiration date of the certificates and how to renew the L2 certificate..

The NES L2 certificate needs to be renewed before expiration. If the L2 certificate has expired, NEA certificate renewal is not possible and results in service disruption.

The NES TLS server certificate also needs to be renewed before expiration. If this certificate has expired, most Nymi services cease to operate. Customers are responsible for renewing the NES TLS server certificate.

During NES installation, the expiration date of all of these certificates is recorded. The certificates should be renewed before their expiration date (e.g., 2-4 weeks) to ensure continuity of service.

Note: The certificates mentioned above do not all expire on the same date. Therefore, it is the customer's responsibility to keep track of expiration dates for all certificates.

Typical certificate expiration dates are:

- L2 certificate: varies
- NES TLS certificate: varies

Check certificate expiration dates

Check the expiration date of the TLS and L2 certificates.

Determining L2 certificate expiration date

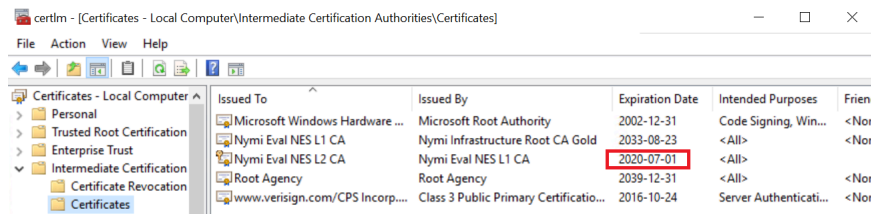
The NES L2 certificate needs to be renewed before expiration. If the L2 certificate has expired, NEA certificate renewal is not possible and results in service disruption.

Perform the following steps to determine the date of the L2 certificate expiration.

Note: The NES Administrator Console reports the L2 expiration date 3 months before the expiry date, as described in the next section.

1. Connect to the NES server.
2. Start Manage Computer Certificates.
3. Expand **Certificates > Intermediate Certification > Certificates**.

The expiration date appear for the L2 certificate, as shown in the following figure.



Certificate Renewal

Three months prior to L2 certificate renewal, when you log into the NES Administrator Console, you will receive the following notification:*The NES L2 certificate will expire on (date). Contact your Nymi Solution Consultant to renew the certificate.*

Three months prior to TLS certificate renewal, when you log into the NES Administrator Console, you will receive the following notification:*The TLS certificate will expire on (date). Contact your Nymi Solution Consultant to renew the certificate.*



Figure 53: L2 Certificate Expiration Example

Additionally, to view certificate expiration information, navigate to the **NES Administrator Console Diagnostic** page by clicking the **About** menu and then click **View Full Diagnostics**.

Under **Enrollment Service**, review the information in the **L2 Cert Validity** section.

Under **Directory and Policy Service**, review the information in the **TLS Certificate** section.

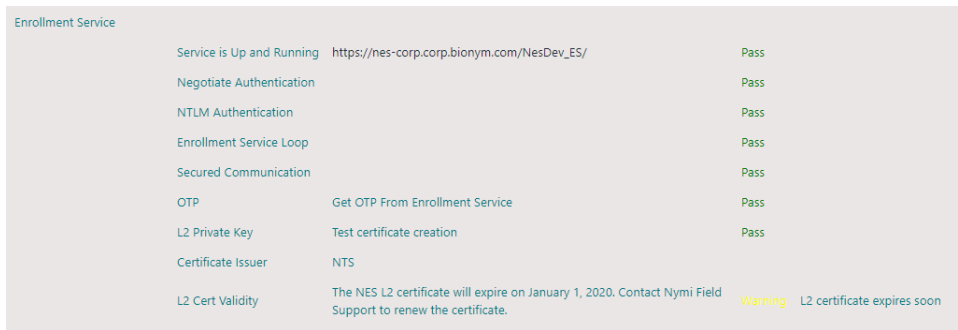


Figure 54: NES Administrator Console Enrollment Service

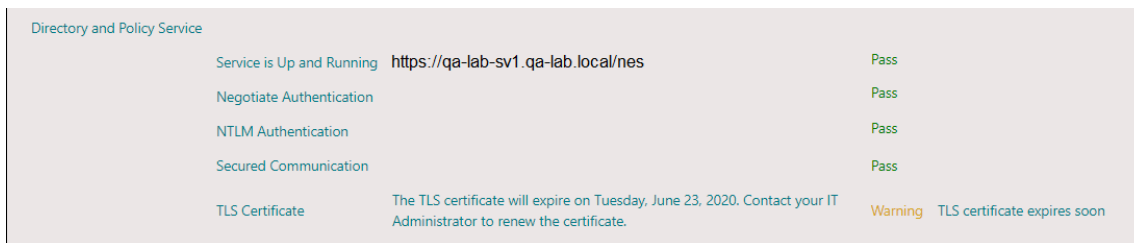


Figure 55: NES Administrator Console Directory and Policy Service

If the NES L2 certificate has expired and you log into NES, the following message appears: *The NES L2 certificate has expired. Contact your Nymi Solution Consultant to renew.* See *Renewing NTS Certificates* section in this guide for more information.

If the TLS certificate has expired and you log into NES, the following message appears: *The TLS certificate has expired. Contact your IT Administrator to renew the certificate.*

Determining TLS expiration date

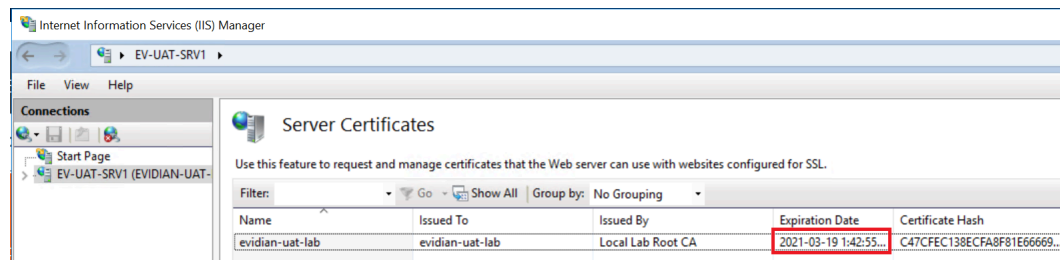
For NES servers that are configured to use https, the NES TLS server certificate also needs to be renewed before expiration. If this certificate has expired, most CWP services cease to operate. Customers are responsible for renewing the NES TLS server certificate.

Perform the following steps to determine the TLS expiration date.

1. Connect to the NES server.
2. Open IIS Manager.
3. In the left navigation pane select **server_name**.

4. On the **Features View** tab, open **Server Certificates**

The expiration date appear for the TLS certificate, as shown in the following figure.



Renewing the L2, L1, and Root Certificates

Renew your certificates before their expiration date.

Perform the following steps to renew certificates used with the NTS deployment:

- delete the existing Root CA, L1 and L2 certificates
- re-importing the CRL files
- renewing certificates
- restart the IIS

Deleting expired certificates

Perform the following steps to delete the Root, L1, and L2 certificates.

1. Right-click **Start**, select **Run**, and then type `Manage Computer Certificates`.
2. In the **Console** window, in the left navigation pane, expand **Certificates > Intermediate Certificates Authorities > Certificates**.
3. Delete the L1 and L2 certificates.
4. Expand the **Trusted Root Certification Authority > Certificates**
5. Delete `Nymi Infrastructure Root CA Gold`.

Renewing the Root, L2, and L1 Certificates

Nymi provides you with a zipped certificate file package that contains a PKCS12 file and 2 Certificate Revocation List (CRL) files. The password for the PKCS12 file will be provided to you separately.

The PKCS12 file (`fullchain.p12`) contains the following key and certificates, and is protected by the provided password:

- Root certificate
- L1 certificate
- L2 certificate
- L2 private key

Importing certificates

Perform the following steps to import the certificates on the NES host.

1. Extract the certificate zip file to a directory.

2. Right-click the *fullchain.p12* certificate file and then select **Install PFX**.
3. In the Open File - Security Warning dialog, click **Open**.
The Certificate Import Wizard dialog box opens.
4. On the Welcome to the Certificate Import Wizard screen, in the **Store Location** page, select **Local Machine**.
5. Click **Next**.
6. On the User Account Control window, click **Yes**.
7. On the Files to import page, perform the following actions ensure that the fullchain.p12 file appears in the *File* name field, and then click **Next**.
8. On the Private Key Protection page, in the Password field, type the Nymi-provided private key password, and then click **Next**.
9. On the Files to import page, ensure that the *fullchain.p12* file appears in the File name field, and then click **Next**.
10. On the Certificate Store page, leave the default option Automatically select the certificate store based on the type of certificate, and then click **Next**.
This options ensures all the certificates in the certification path (Root, Intermediate) are placed in the correct store.
11. On the Completing the Certificate Import Wizard page, click **Finish**.
12. On the Certificate Import Wizard dialog, click **OK**.
13. Copy the CRL files to the *C:\inetpub\wwwroot\crl*.
If you copied the CRL files to the path listed above and receive a message to replace the files, click **Yes**.

Managing Private Keys

If the account used for the NES Application Pool is not LocalSystem, perform the following procedure to grant NES access to the L2 private key.

1. From the Windows Start Menu, type Manage Computer, and then select Manage Computer Certificates.
The certlm window appears.
2. Navigate to **Personal > Certificates** folder.
A list of certificates displays.
3. Right-click the NES L2 CA and select **All Tasks** and then select **Manage Private Key...**
4. On the User Account Control dialog, click Yes.
5. Select the **Security** tab and then click the **Add** button.
6. In the new window, click **Add**, which opens the **Select Users, Computers, Service Accounts, or Groups** window.
7. Type the account that was selected to be used with the NES Application Pool and then click **OK**.

8. In the **Permissions** area, assign the following permissions under **Allow**:

- Full control
- Read

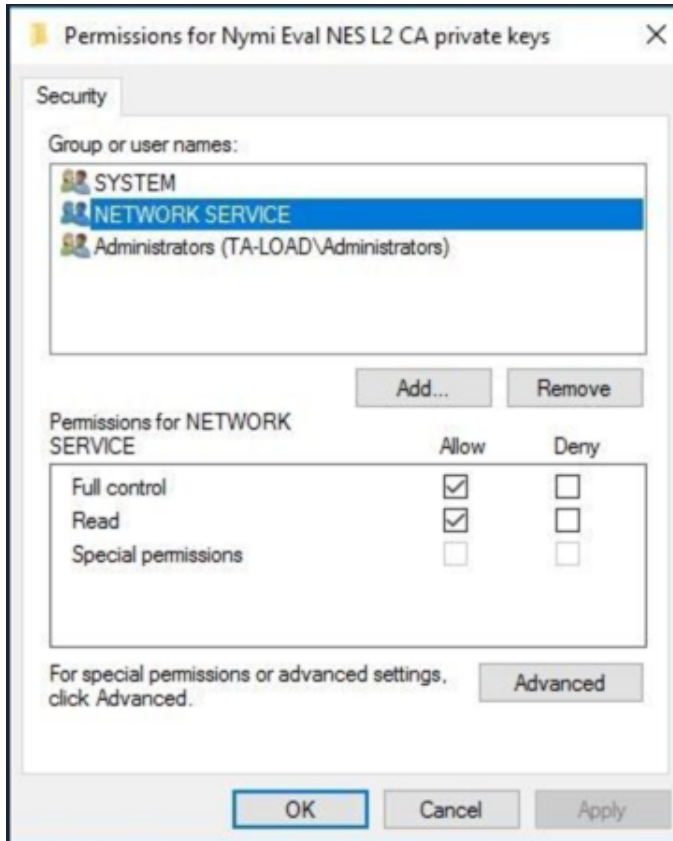


Figure 56: Setting Private Key Permissions

9. Click **OK**.

Moving the L2 certificate

Perform the following steps to move the L2 certificate from the Personal store to the Intermediate Certification store.

1. Expand **Intermediate Certification > Certificates** and then move the NES L2 CA certificate from **Personal > Certificates** to the **Intermediate Certification > Certificates**

You can move the file by dragging and dropping it from one folder to the other folder.

2. In **Intermediate Certification > Certificates**, verify that the NES L2 CA certificate has a key.

When the L2 certificate has a key, a key symbol displays in the upper-left corner of the L2 certificate icon.

3. Record the expiration date of the NES L2 CA certificate (shown in the Expiration Date column) in the Certificate Expiration Dates table, that was provided in the Nymi Connected Worker Platform NES Deployment Guide.

4. Close the `certlm` window.

Restarting IIS

After replacing the CRL file and importing the L2 certificate, restart the IIS. Administrative privileges are needed to perform this procedure.

1. From the Start menu, click Run.
2. In the Open box, type `cmd`, and click OK.
3. At the command prompt type, `iisreset/noforce`.
IIS attempts to stop all services before restarting. The `IISReset` command-line utility waits up to one minute for all services to stop.

Manage Nymi Band Application and Nymi Runtime

This section provide information about how to manage the Nymi Band Application and Nymi Runtime applications in the environment, including removing the software and upgrading the software.

Upgrading the Nymi Band application

Upgrades from a previous version are supported.

You are not required to remove the previous version before installing the newer version. You can upgrade the Nymi Band Application by using the installation wizard or silently from a command prompt.

Note: Before performing an upgrade of the Nymi Band Application, kill all user sessions for logged in users who are not performing the upgrade.

Performing a silent Nymi Band application installation or upgrade

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

1. Download the Nymi Band Application package.
2. Launch the command prompt as administrator.
3. From the folder that contains the Nymi Band Application, type *Nymi-Band-App-installer-v_version.exe /xenui /q*

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

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

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

Performing a Nymi Band application upgrade by using the installation wizard

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

1. Download the Nymi Band Application software to a directory on the network terminal. For example, *C:\Downloads*
2. Double-click the installation file *Nymi-Band-App-installer-v_version*, and then follow the prompts to update the software.

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.

Uninstalling Nymi Lock Control

Perform the following steps to uninstall Nymi Lock Control.

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**.

Upgrading the Nymi Runtime

Upgrades from a previous version are supported.

You are not required to remove the previous version before installing the newer version. You can upgrade the Nymi Runtime by using the installation wizard or silently from a command prompt.

Performing a customizable Nymi Runtime installation or upgrade

Perform the following steps to install or upgrade Nymi Runtime on a network device, on which you want to install a Nymi-enabled application.

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the `..\nymi-sdk\windows\setup` folder, run the *Nymi Runtime Installer version.exe* file.
4. On the Welcome page, click **Install**.
5. On the User Account Control page, click **Yes**.
The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the Welcome to the Nymi Runtime Setup Wizard page, click **Next**.
7. On the Nymi Runtime Setup page, click **Next**.
8. On the Service Account window, click **Next**.
9. On the Ready to install page, click **Install**.
10. Click **Finish**.
11. On the Installation Completed Successfully page, click **Close**.

12. In the Windows Services applet, confirm that you can see the *Nymi Agent* and *Nymi Bluetooth Endpoint* services, and that the status of each service is *Running*.

Performing a silent installation or upgrade of Nymi Runtime

Perform the following steps to install or upgrade the Nymi Runtime and the BLE adapter drivers silently, without user intervention.

1. Log in to the network terminal with an account that has administrator privileges.
2. Extract the Nymi API distribution package.
3. Launch the command prompt as administrator.
4. Change to the `..\nymi-sdk\windows\runtime` folder, and then type: `"Nymi Runtime Installer version.exe" /xenoui /q`

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

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

The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, Nymi Runtime appears in the Program and Features applet.

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

The silent installation process creates an installation log file in the `%temp%` directory named `Nymi Runtime_version_time.log`

Uninstalling the Nymi Runtime

To remove the Nymi Runtime, in **Add or Remove programs**, select **Nymi Runtime**, and then click **Uninstall**.

Audit Log Appendix

The section provides information about the Audit Log SQL Tables.

audit.UserCore SQL Table

Each column is prefaced with Identity

Column Name	Description
EventTime	The time when a user was changed (C (create), U (update), D (delete)).
EventType	Single character denoting C (create), U (update), D (delete).
SystemUser	The user connected to the database.
ID	The database ID of the user in the audit.UserCore table.
Domain	The domain of the user.
Username	Login name of the user.
MiscNote	Explanation about the user.
CreatedAt	Date and time that the object created.
ModifiedAt	Date and time when the object was modified.
ModifiedBy	Person who modified the object.

audit.NymiBand SQL Table

Each column is prefaced with Identity

Column Name	Description
EventTime	Time of entry.
EventType	Single character denoting C (create), U (update), D (delete).
SystemUser	The user connected to the database.
ID	The object in the UserCore table.
UserCoreId	The ID of the user who owns the Nymi Band.
NymiBandID	The DB ID of the Nymi Band (MAC address) in the audit.NymiBand table.
NfcUID	Nymi Band's NFC address.
AuthorisationID	N/A.
SymmetricKeyID	The symmetricKey ID that was created on the Nymi Band.

Column Name	Description
EncryptionIV	Encryption Initialization Vector.
EncryptedPassword	User's login encrypted password.
IsActive	0=non-active, 1=active
IsPrimary	0=non-primary, 1=primary
HasFingerprint	Fingerprint for enrollment. 0=finished, 1=not finished
EnrollmentStatus	N/A
MiscNote	Additional information about one Nymi Band (appears empty).
BandSubordinateCaCert	N/A
BandCert	N/A
UserCert	N/A
BandLabel	The Band Label name given to the Nymi Band during enrollment. This field is empty by default.
FirmwareVersion	Firmware version for the Nymi Band at time of enrollment.
CreatedAt	Date and time that the object created.
ModifiedAt	Date and time when the object was modified.
ModifiedBy	Person who modified the object.
EvidianEnrollmentCompleted	Enrollment in Evidian completed. 0=not completed, 1= completed

audit.ApplicationsSetting SQL Table

Each column is prefaced with Identity

Column Name	Description
EventTime	The time when a new application setting was (C (created), U (updated), D (deleted)).
EventType	Single character denoting C (create), U (update), D (delete).
SystemUser	The user connected to the database.
ID	The database ID of application settings on audit.ApplicationSettings table.
IsActive	0=non-active, 1=active
Description	Additional information.
AutoLogoutTimeoutSeconds	NEM application automatic log out time - no actions from the user.
NfcUIDCaptureRequirement	M Mandatory, 0=Option, 1=Not required.
FingerprintRequirement	M Mandatory, 0=Option, 1=Not required.

Column Name	Description
PassworthAuthOption	Corporate credential authentication, 0=disable, 1=enable
FingerprintOption	M Mandatory, 0=Option, 1=Not required.
LockControlSupportOption	Enable Password Encryption. 0=disable, 1=enable
DoorSecurityOption	N/A.
AdCheckUserStatus	0=does not validate user status on NES, 1=validates user status on NES
AdCacheUserStatus	Caching user status on NES, 0=disable, 1=enable
AdCacheExpiryTimeSeconds	Expiry time of user status cache in seconds.
ManualOtpOption	Manual one time password (OTP) on NEM application, 0=disable, 1=enable
ManualNeaOtpOption	Manual one time password on other applications, 0=disable, 1=enable
LockWhenAway	0=disable, 1=enable
MonitorProximity	0=do not lock machine, 1=lock machine
KeepUnlockedWhenPresent	0=do not lock machine, 1=lock machine
CheckProximityForUnlock	0=disable, 1=enable
LockProximitySphera	Checks the length of space around lock control, 0=disable, 1=enable
UnlockProximitySphera	Checks the length of space around lock control, 0=disable, 1=enable.
ProximityLockCountdown	N/A.
BandLabelOnBandEnabled	Enables setting the Band Label during enrollment. The default setting is set to false.
BandLabelOnBandCustomizationEnabled	Enables customizing Band Label by the user during enrollment. This field is used only if the BandLabelOnBandEnabled field is set to true (1). The default setting is set to false.
CreatedAt	Date and time that the object created.
ModifiedAt	Date and time when the object was modified.
ModifiedBy	Person who modified the object.
EnrollmentDestination	Specifies where the NBA saved enrollment data, 1=NES, 2=NES and Evidian.
SDCTEnabled	0=SDCT disable, 1=SDCT enable
SDRemindersEnabled	0=disable smart distancing reminders, 1=enable smart distancing reminders

audit.ExternalAuthenticator SQL Table

Each column is prefaced with Identity

Column Name	Description
EventTime	The time when a new role is inserted.
EventType	Single character denoting C (create), U (update), D (delete).
SystemUser	The user connected to the database.
ID	The object in the UserCore table.
PublicKey	Base-64 pem encoded.
BandExternalAuthenticatorid	The ID for that external authentication.
NymiBandId	ID for the Nymi Band.
Name	The name of the application that created the External Authenticator.
MiscNote	Additional information.
CreateddAt	Date and time that the object created.
PrivateKeyWO	N/A.
PrivateKeyStoreID	The location where the key is stored.
ModifiedAt	Date and time when the object was modified.
ModifiedBy	Person who modified the object.

audit.Certificate SQL Table

Each column is prefaced with Identity

Column Name	Description
NotBefore	The start date of the certificate.
NotAfter	The end date of the certificate.
SerialNumber	Serial number of the certificate.
RequesterTime	When the certificate was requested.
RequesterDomain	Domain of the user that requested the certificate.
RequesterUserName	The user name of the user that requested the certificate.
RequesterIp	The IP of the requester of the certificate.

Copyright ©2021
Nymi Inc. All rights reserved.

Nymi Inc. (Nymi) believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

The information in this document is provided as-is and Nymi makes no representations or warranties of any kind. This document does not provide you with any legal rights to any intellectual property in any Nymi product. You may copy and use this document for your referential purposes.

This software or hardware is developed for general use in a variety of industries and Nymi assumes no liability as a result of their use or application. Nymi, Nymi Band, and other trademarks are the property of Nymi Inc. Other trademarks may be the property of their respective owners.

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