Administration Guide

Nymi Connected Worker Platform
v1.0
2022-05-16

Contents

Preface..... 7

Overview.....9
Connected Worker Platform Components in a Local Configuration..... 9
Nymi Band 3.0.....12
Nymi Lock Control.....14
NFC support.....15
Nymi-Supported NFC Readers.....15
Configuring Unverified NFC Readers.....16
Bluetooth Adapter Placement.....16
Nymi Band Enrollment Process..... 17
Authentication After Enrollment..... 17

Checklist for Nymi Band Distribution and Enrollment.....19

Connect to NES for the First Time.....21
Accessing NES Administrator Console.....21

Customizing the CWP configuration..... 22
Viewing Policies..... 22
Manage Group Policies.....24
Modifying the Default Group Policy.....24
Creating a New Group Policy..... 26
Changing the Active Group Policy.....27
Deleting Group Policies.....27
Customizing the Enrollment..... 28
Customizing the Nymi Band Authentication Method..... 29
Customizing Smart Distancing and Contact Tracing..... 33
Customizing Health Attestation.....35
Customizing Temperature Alerts.....36
Customizing the Nymi Band Label.....37
Customizing Connected Worker Platform to support NEAs that check AD status..... 39
Customizing Nymi Lock Control Support.....40
Manage Individual User Policies.....42
Creating an Individual User Policy..... 43
Creating an Individual User Policy from an Existing Individual User Policy.....44
Deleting an Individual User Policy..... 46

Adding a User to an Individual User Policy....46
Displaying Individual User Policy Membership....48

Nymi Band Enrollment....50
Assigning the Nymi Band to the Enterprise....50
Fingerprint Capture....51
Assigning the Band Label....54
Preview Band Label....54
Customize Band Label....55
Applying Policy Settings....56
Completing Enrollment....57

Using the Nymi Band....59
Authentication After Enrollment....59
Authentication by fingerprint....59
Authentication by corporate credentials....60
Authentication Failures....60
Viewing Nymi Band Text....62
Viewing Nymi Band Screens....62
Viewing the Band Label....66
Nymi Band Dashboard....67
Nymi Band Vibration....68
Tapping the Nymi Band....69
SEOS Access....70
Collecting Data From a Nymi Band....70

Using the Contact Tracing Dashboard....71
Accessing the Contact Tracing Dashboard....71
Viewing the Contact Tracing Dashboard....71
Contact Tracing Dashboard Example....71
Enrolled Employees....72
Social Distancing Compliance (%)....72
Average and Maximum Contacts (%)....72
Most Contacted Employees....72
Total Contacts by Day....73
Most Contacted Employee Details....73
Employee Contact Timeline....73

Using Health Attestation....74
Web-Based Attestation....74
Performing Web-based Attestation....74
Performing Attestation on the Nymi Band....77
Accessing Health Attestation and Secondary Screening Results....77

View Daily Attestation Summary Results....78

Using Temperature Alerts....84
Performing Secondary Screening.... 84
Modifying Secondary Screening Results....87
Viewing Daily Secondary Screening Results for the Current Day.... 88
Viewing Secondary Screening Results for a User.... 90

Using Nymi Lock Control.... 93
Initializing Nymi Lock Control.... 93
Confirming Nymi Lock Control Recognizes the Nymi Band....94
Unlocking with an NFC or BLE Tap....94
Unlocking with Nymi Credential Provider....94
Unlocking a Nymi Lock Control User Terminal Without a Nymi Band.... 95
Locking the User Terminal....96
Stopping Nymi Lock Control.... 96
Resetting an Expired Password.... 96

Nymi Band Management....98
Removing the Nymi Band....98
Storing the Nymi Band....98
Charging the Nymi Band....98
Managing Battery Life....100
Exiting Sleep Mode.... 101
Authenticating User Identity to the Nymi Band.... 101
Authentication by fingerprint....101
Authentication by corporate credentials.... 104
Cleaning the Nymi Band.... 104
Restarting the Nymi Band.... 104
Determining Nymi Band Firmware Version.... 105

Nymi Band User Management.... 106
NFC (Unique Identifier) UID Management....106
Searching for User or Nymi Bands Information....106
Searching for Users....107
Searching for Nymi Bands.... 109
Searching for Individual User Policy Membership.... 113
Issuing a temporary Nymi Band to a user.... 114
Restoring the Nymi Band.... 115
Replacing the Nymi Band for a user....115
Suspending the primary Nymi Band for a user....116
Disconnecting the Nymi Band from a user in NES....117
Deleting User Data....117

Reassigning a Nymi Band....118
Re-enrolling a User....118

Storage of Data....120
Storage of NES Data....120
Adding additional users or groups to view and query audit database....120
NES SQL Database Overview....122
Viewing and Querying Audit Schema....132
Performing More Complex Queries of the Audit Tables....132

Log Files....135
Configuring Contact Tracing Logging....135
Enrollment Terminal log files....137
Saving Nymi Band Application log files....137
Viewing Nymi Band Application log files....137
User Terminal Log Files....138
Nymi Lock Control Log Files....138
Nymi Edge Agent Log Files....139
NES log files....139
Enabling Verbose Logging....139
NES web service log file locations....140
Nymi Support Tool....141
Firmware log files....142
Firmware log retrieval....142
Submitting a support request....143

Manage the Connected Worker Platform Environment....144
Manage NES....144
NES Backup and Recovery....144
Uninstalling NES Installer....144
Adding and Removing NES Administrator Access....145
System Diagnostics....145
Accessing NES Administrator Console....145
System Diagnostics Information....146
Certificate Management....149
Check certificate expiration dates....149
Renewing the L2, L1, and Root Certificates....152
Backup and Restore the Kubernetes Environment....155
Restoring Kubernetes from a Backup....156
Restoring Kubernetes from a Disaster on the Same Kubernetes Cluster....157
Recycling the CWP Kubernetes Cluster Passwords....158
Changing Passwords in the Kubernetes Cluster....158
Changing passwords for the Nymi Edge Agent....159

Uninstalling Nymi Components.....160
Uninstalling the Nymi Band Application.....160
Uninstalling Nymi Lock Control.....160
Uninstalling the Nymi Runtime.....160
Uninstalling on Nymi Bluetooth Endpoint on HP Thin Pro.....160
Uninstalling the Nymi Edge Agent.....161

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
1.0	May 16, 2022	First release of this document for CWP 1.3. Includes the following changes: • Moved Upgrading content to the Nymi Connected Worker Platform NES Deployment Guide

Related documentation

- **Nymi Connected Worker Platform Overview Guide**

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

This document provides the steps that are required to deploy the Nymi Enterprise Server (NES). This installation uses the `Nymi Token Service` to install certificates that enable communication between components. This document also provides information about deploying the Connected Worker Platform in a Citrix or RDP environment.

- **Nymi SDK for C Developer's Guide**

  This document provides information about how to develop Nymi-enabled Applications by using the `Nymi API`(`NAPI`).
- **Nymi SDK for Linux Developer's Guide**

  This document provides information about how to develop Nymi-enabled Applications by using the `Nymi API`(`NAPI`).
- **Nymi SDK for WebSocket Developer's Guide**

  This document provides Nymi developers with an alternative way to utilize the functionality of the `Nymi SDK`, over a WebSocket connection managed by a web-based or other applications.
- **Nymi Connected Worker Platform Troubleshooting Guide**

  This document provides information about how to troubleshoot issues and the error messages that you might experience with the `NES Administrator Console`, the Nymi Enterprise Server deployment, the Nymi Band, and the `Nymi Band Application`.
- **Connected Worker Platform Release Notes**

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

How to get product help

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

How to provide documentation feedback

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

Overview

Connected Worker Platform Components in a Local Configuration

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.

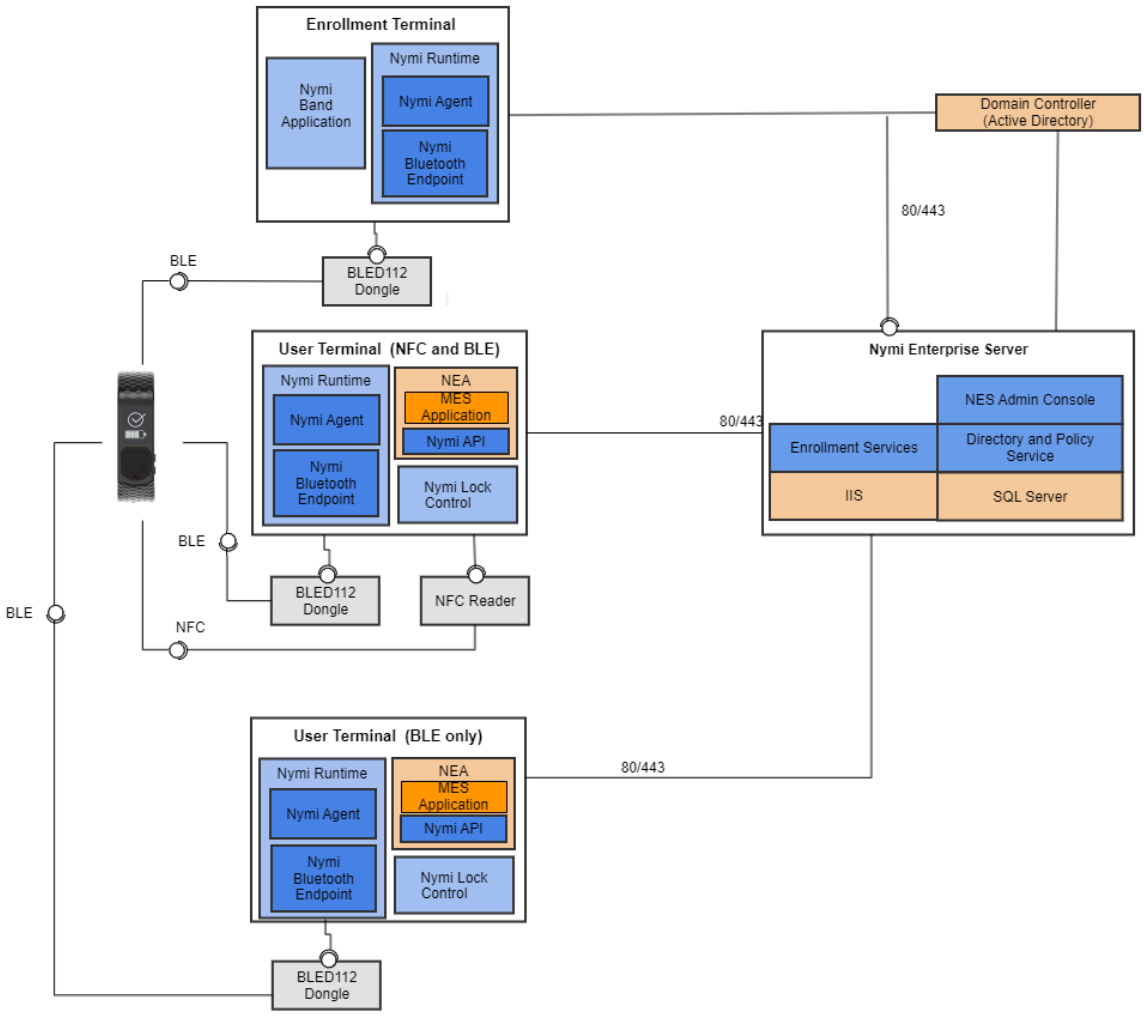


Figure 1: Connected Worker Platform components and connection ports

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, which the `Nymi Band Application` automatically installs.
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 that provides the `NES Administrator Console` and coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates. Includes the following services: • Enrollment Service (ES) - authenticates, validates, and authorizes certificate requests from requesters, such as the Nymi Band Application and NEAs. • Directory and Policy Services (DPS) - maintains the NES database, which contains a list of Active Directory (AD) users and the Nymi Bands that are associated with each user. Provides IIS web services, which allows the NES Administrator Console access to the NES database. • Authentication Service (AS) - provides authentication and authorization support for domain users and computers. AS uses adapters to interface with external directory and database systems, such as an AD adapter to interface with Active Directory.
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.

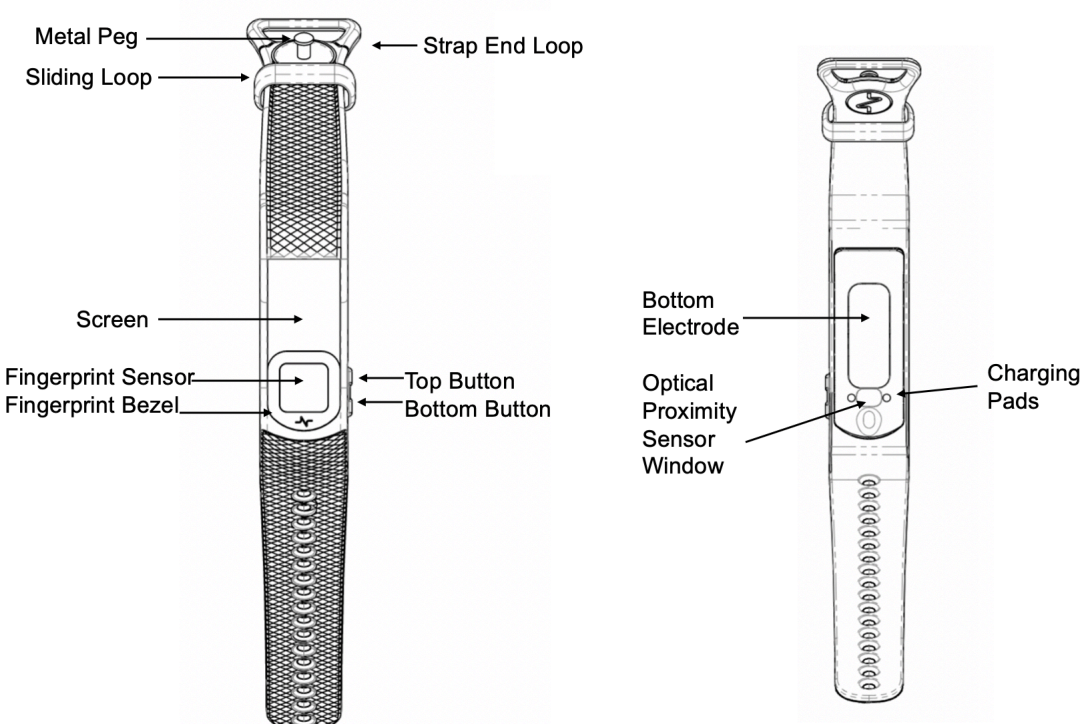


Figure 2: Nymi Band front and back

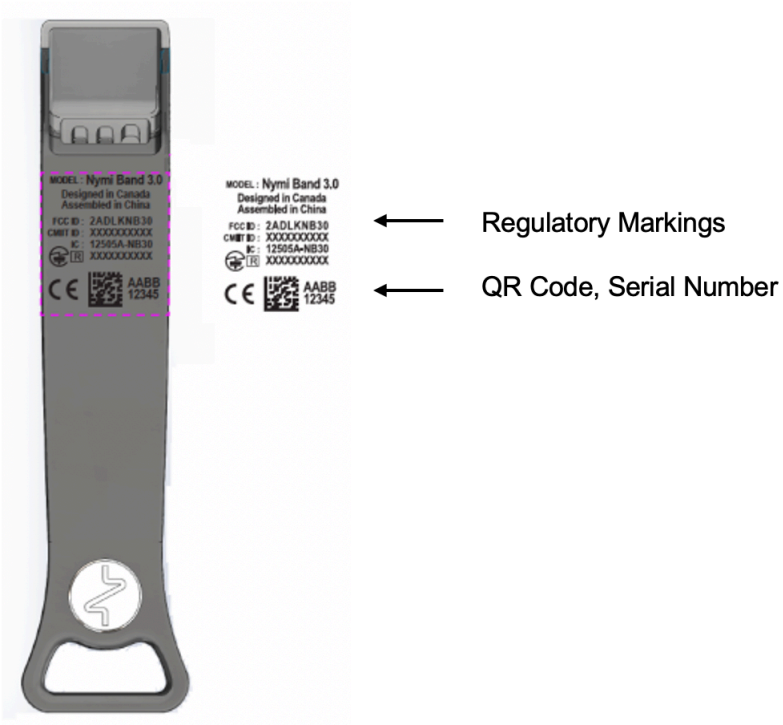


Figure 3: Nymi Band Strap

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-Supported 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.

CWP supports the following NFC readers:

- HID Omnikey 5022
- ACS ACR122U
- Systec CONNECT BOX
- Elatec TWN4 LEGIC NFC USB
- HID Omnikey 5127CK Mini
- ACS ACR1252U
- Identiv CLOUD/uTrust 3700 F
- RFIdeas WAVE ID Nano SDK 13.56MHz CSN Black Vertical USB Reader

Configuring Unverified NFC Readers

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

About this task

Procedure

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

Results

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

```
}
 {

    "supportedReader" : "Omnikey 5x25"

 }
}
```

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

Note: When the **`Attestation on Nymi Band`** option is enabled in the active NES policy, after the user authenticates to the Nymi Band, the Health Check Status question appears on the Nymi Band. The *Using Heath Attestation* chapter provides more information.

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 3: Nymi Band configuration checklist for users

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

Completed?	Task
	• Verify that the firmware version on the Nymi Band matches the version on the packing slip. The firmware version is visible when the Nymi Band is plugged into a USB charger and you press the top and bottom button on the Nymi Band. • Unplug the Nymi Band and press any button to verify that the battery icon and NO USER appears on the display of the Nymi Band.
	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.

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.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing `https://nes_server/NES_service_name` or `http://nes_server/NES_service_name`

   depending on the NES configuration, where:

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

     For example, `https://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.

What to do next

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.

Customizing the CWP configuration

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

Viewing Policies

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

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing `https://nes_server/NES_service_name` or `http://nes_server/NES_service_name`

   depending on the NES configuration, where:

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

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

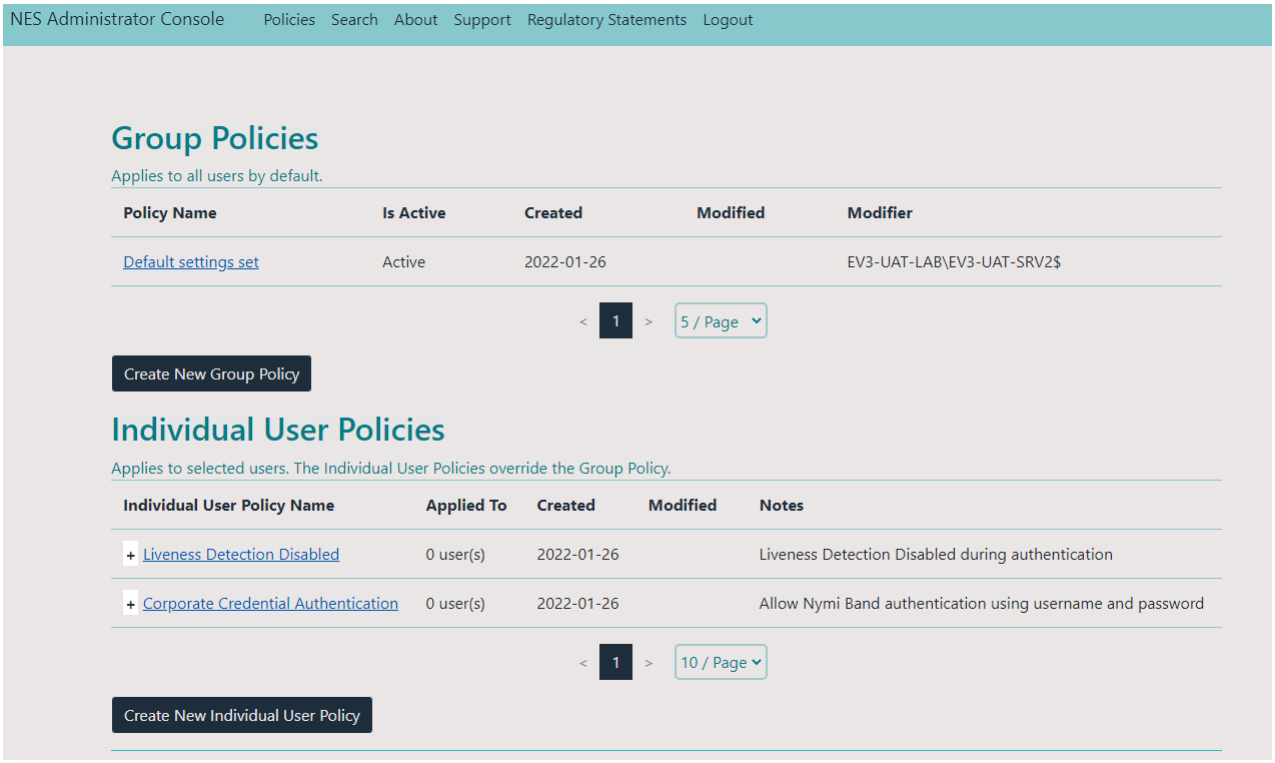


Figure 4: Policies page

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

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

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

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

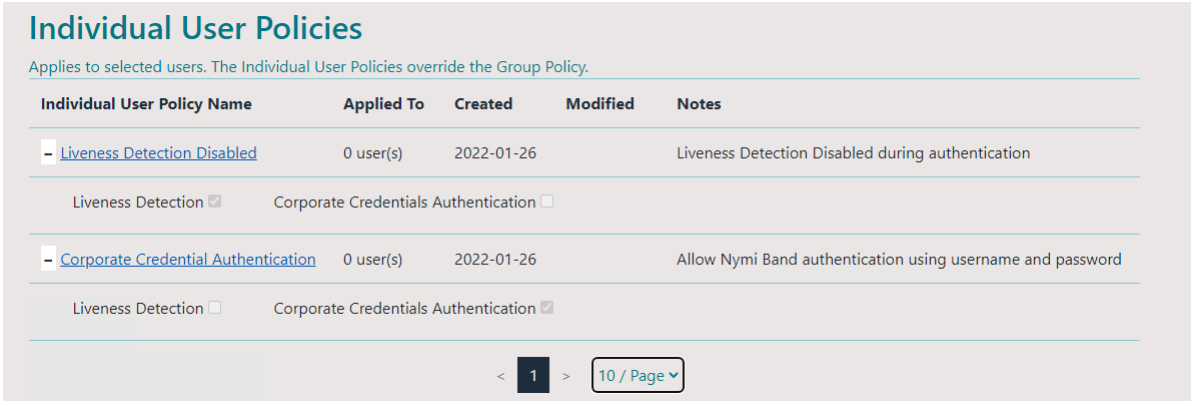


Figure 5: Individual User Policy settings view

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

Manage Group Policies

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

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

Modifying the Default Group Policy

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

About this task

- Save enrollment data to the NES database only.
- Log a user out of the Nymi Band Application or the NES Administrator Console after 5 minutes of inactivity
- Always check for liveness during authentication.
- Do not use Nymi Bands for Smart Distancing and Contact Tracing
- Do not require health attestation to enable the use of an authenticated Nymi Band to gain access to physical access to SEOS-enabled doors.
- Do not send temperature alerts to an authenticated Nymi Band.
- Do not allow users to use the Nymi Band to lock and unlock their user terminals.

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

Procedure

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

   depending on the NES configuration, where:

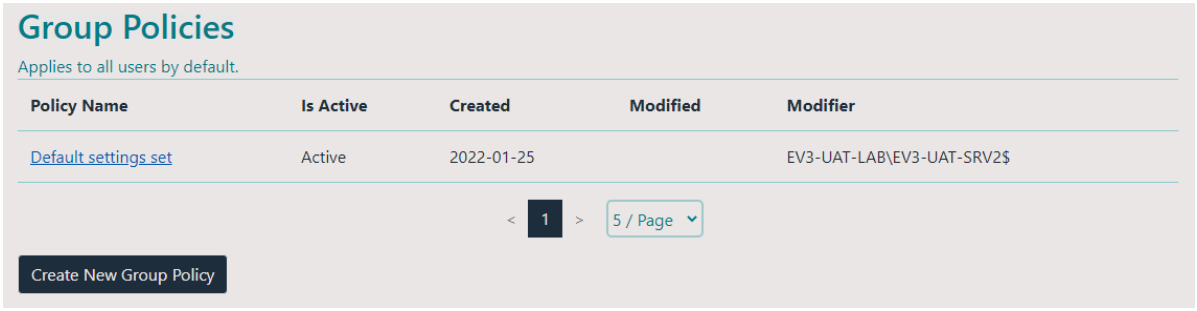
   - *`nes_server`* is the Fully Qualified Domain Name (FQDN) of the NES host.
   - *`NES_service_name`* is the service mapping name for the NES web application. The default service mapping name is *nes*.

     For example, `https://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 `Policies` page appears. The following figure shows the `Group Policy` pane on the `Policies` page.



`Figure 6: Group Policies Pane`

4. Select the policy that you want to change.

   The `Edit` page appears.

5. Modify the options, as required.

6. Click **`Save`**.

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

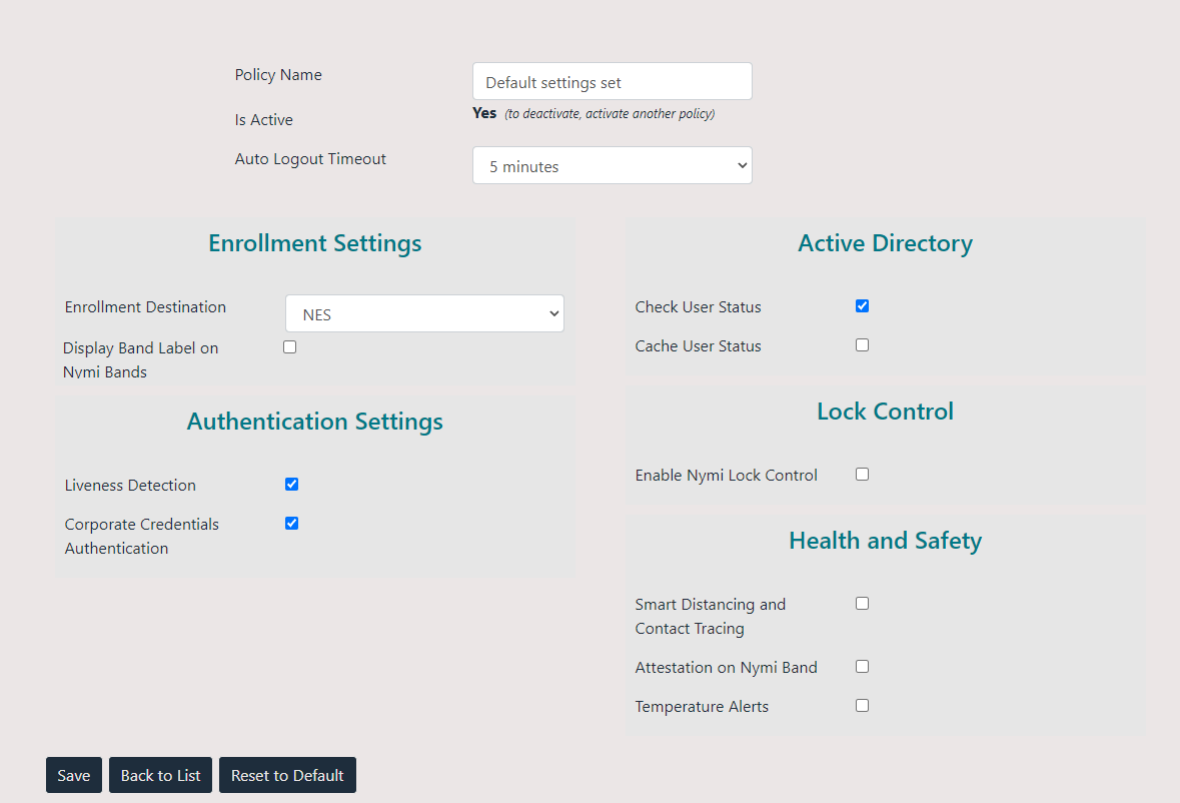


Figure 7: Edit Group Policy page

Creating a New Group Policy

Perform the following steps to create a new group policy.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing `https://nes_server/NES_service_name` or `http://nes_server/NES_service_name`

   depending on the NES configuration, where:

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

     For example, `https://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 Policies pane on the Policies page.

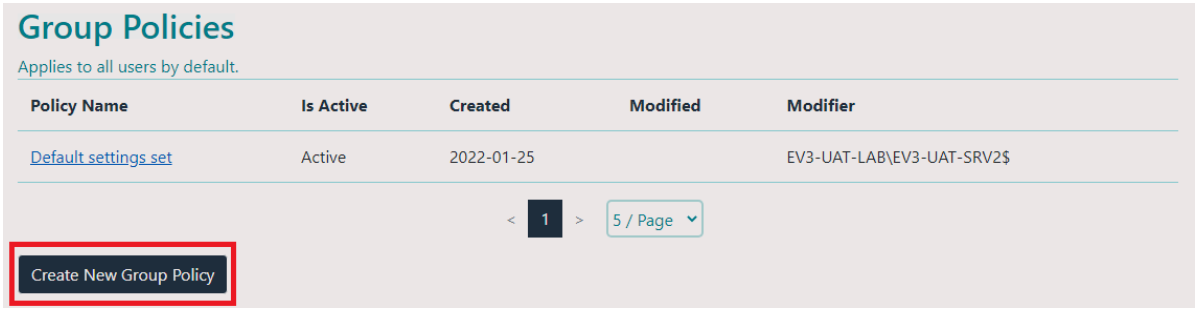


Figure 8: Group Policy page

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

   Note: If the Sign in screen appears instead of the Create Policy page, the user account that you specified is not a member of the NES Administrator group.
4. Configure the options for the group policy, and then click **Save**.

Changing the Active Group Policy

NES can only have one active policy.

About this task

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

Procedure

1. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
2. In the Group Policies pane, in the **Policy Name** column, select the policy from the list.
   The Edit Policy window appears.
3. On the Edit Group Policy page, select the **Is Active** option.
4. At the bottom of the page, click **Save**.

Deleting Group Policies

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

About this task

You cannot delete an active policy.

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Group Policies pane, select the policy from the list.
   The Edit Policy window appears.
4. If the policy that you want to delete is active, then clear the **Is Active** option.
5. Click **Delete**.
6. On the Delete Group Policy window, click **Delete**.

   Note: The **Delete** button is not enabled if the policy is the active policy, or if only one group policy exists.
7. Edit one of the remaining policies and select the **Is Active** option.

   Note: NES must always have one active policy.
8. To the right of Policy table, beside the policy that you want to delete, click **Delete**.

Customizing the Enrollment

The Connected Worker Platform provides enhancements that support coexistence of Evidian-integrated MES applications and Nymi-integrated MES applications.

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

Configuring NES and Evidian Enrollment

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

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Policies window, select the active policy.
4. From the **Enrollment Destination** list, select the **NES and Evidian** option.

5. Click **Save**.

Results

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

If you enable this option after users have enrolled their Nymi Band, the user must re-enroll the Nymi Band.

Reverting to an NES only Enrollment Configuration

Perform the following actions to modify the configuration of a policy to allow users to use the Nymi Band with Nymi-integrated MES applications only.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Policies window, select the active policy.
4. From the **Enrollment Destination** list, select the **NES only** option.
5. Click **Save**.

Results

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

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

Customizing the Nymi Band Authentication Method

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

By default,

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

Table 4: Authentication method advantages and disadvantages

Setting	Advantage	Disadvantage
Corporate Credentials = disabled Liveness Detection = disabled **Note:** This is the default configuration for new installations.	• Biometric guarantee of the identity of the user. • Authentication by fingerprint does not check for an ECG signal.	• Authentication by fingerprint does not check for an ECG signal. • User cannot authenticate by using their corporate credentials when authentication by fingerprint fails.
Corporate Credentials = disabled Liveness Detection = enabled	• Biometric guarantee of the identity of the user. • Authentication by fingerprint also checks for an ECG signal.	• Authentication might fail when the fingerprint is dirty, cut, too wet or too dry, or when the fingerprint sensor is not clean. • A small percentage of the population has difficulty providing stable ECG to the Nymi Band during authentication,which results in the liveness check and authentication to fail.

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

Setting	Advantage	Disadvantage

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

Configuring Corporate Credentials Authentication

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

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. From the **`Enrollment Settings`** section, select the option **`Corporate Credentials Authentication`**.
5. Click **`Save`**.

Results

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

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

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

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

Disabling Corporate Credentials Authentication

Perform the following steps to disable corporate credentials authentication in an NES policy.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. From the **`Enrollment Settings`** section, clear the option **`Corporate Credentials Authentication`**.
5. Click **`Save`**.

Results

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

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

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

Configuring Liveness Detection

Perform the following steps to disable the liveness check during authentication by fingerprint.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. In the **`Authentication Settings`** section, clear the **`Liveness Detection`** option.

5. Click **Save**.

Results

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

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

Enabling Liveness Detection

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

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Policies window, select the active policy.
4. In the **Authentication Settings** section, select the **Liveness Detection** option.
5. Click **Save**.

Results

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

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

Customizing Smart Distancing and Contact Tracing

Nymi offers a smart distancing and contact tracing solution that will allow users to accurately track contact events and encourage social distancing behavior. Smart Distancing and Contact Tracing (SDCT) functionality is enabled through the NES Administrator Console.

Smart Distancing and Contact Tracing enables the Nymi Band to scan for other authenticated Nymi Bands in vicinity. When two or more Nymi Bands remain in close proximity of each other for 5 consecutive minutes, each Nymi Band logs a proximity event. Proximity events are sent to the SDCT services for analysis. When a Nymi Band reports 3 proximity events (cumulative total of 15 minutes) with another Nymi Band over a 24-hour period, a contact event is recorded in a CWP Database. Optionally, you can configure the Nymi Band to generate smart distancing reminders. When users are in close proximity of each other for 5 minutes, a smart distancing reminder causes the Nymi Band to vibrate and display a message to the users advising them to maintain social distancing.

Configuring SDCT

Perform the following steps to enable the Smart Distancing and Contact Tracing functionality on the Nymi Band during enrollment. This includes **Smart Distancing Reminders** and contact tracing event collection.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Policies window, select the active policy.
4. Select the **Smart Distancing and Contact Tracing** option.
   The **Smart Distancing Reminders** option appears.
5. Select **Smart Distancing Reminders**, to allow users to receive smart distancing reminders on their Nymi Bands.
6. Click **Save**.

Results

During enrollment the Nymi Band Application updates the Nymi Band to enable SDCT support.

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

Disabling SDCT options

Perform the following steps to disable contact tracing and smart distancing reminders.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Policies window, select the active policy.
4. Perform one of the following actions:

   - To disable the smart distancing reminders that a user receives when a Nymi Band detects that it is in close proximity of another Nymi Band for 5 consecutive minutes, clear the **Smart Distancing Reminders** option.

     Note: TheNymi Band continues to record proximity events.

- To prevent the solution from recording proximity and contact tracing events, and providing users with smart distancing reminders, clear the **Smart Distancing and Contact Tracing** option

5. Click **Save**.

Results

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

Customizing Health Attestation

The Connected Worker Platform provides organizations with the ability to manage access into the workplace based on the results of an individual's self assessment.

Nymi provides a solution that requires individuals to perform health attestation, which restricts or allows physical access by using the Nymi Band dependent upon on the attestation responses of the user. By default, the health attestion functionality is disabled and a user can use an authenticated Nymi Band to gain access to a SEOS-enabled door. When you configure the NES active policy to enable heath attestation, an authenticated Nymi Band cannot unlock a SEOS-enabled door until the wearer answers an attestation question on the Nymi Band. A positive attestation allows the wearer to use their Nymi Band to unlock a locked SEOS-enabled door. A negative attestation prevents the wearer from using the Nymi Band to unlock a SEOS-enabled door. For more information about how Health Attestation affects SEOS access, see the section *SEOS Access*.

Configuring Health Attestation

Perform the following steps to enable the Health Attestation functionality on all Nymi Bands during enrollment.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Policies window, select the active policy.
4. Select the **Attestation on Nymi Band** option.
5. Click **Save**.

Results

During enrollment the Nymi Band Application updates the Nymi Band to allow the wearer to specify the status of their health attestation results.

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

Disabling Health Attestation

Perform the following steps to disable the health check question that appears on the Nymi Band after successful authentication.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. Clear the **`Attestation on Nymi Band`** option.
5. Click **`Save`**.

Results

After a user authenticates to their Nymi Band, the Nymi Band does not show the user the health attestation confirmation question, and the user can use a SEOS-enabled Nymi Band to gain physical access, where applicable.

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

Customizing Temperature Alerts

The Connected Worker Platform provides organizations with the ability to monitor elevations in the skin temperature of a Nymi Band user without the need to manually take a temperature reading of the employee by screeners.

Configuring Temperature Alerts

Perform the following steps to enable the temperature alerting functionality on all Nymi Bands during enrollment.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. Select the **`Temperature Alerts`** option.
5. Click **`Save`**.

Results

During enrollment the `Nymi Band Application` updates the Nymi Band to allow the Nymi Band to collect wrist temperature readings, create a temperature profile, and provide the wearer with alerts when their wrist temperature is elevated.

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

Disabling Temperature Alerts

Perform the following steps to disable the temperature alerting functionality on a Nymi Band.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. Clear the **`Temperature Alerts`** option.
5. Click **`Save`**.

Results

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

Customizing the Nymi Band Label

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

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

Nymi supports two types of band labels:

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

Configuring a Band Label on the Nymi Band

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

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Policies window, select the active policy.
4. In the **Enrollment Settings** section, select **Display Band Label on Nymi Bands**
   The **Allow Band Label Customization** option appears.

   Perform one of the following actions:

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

Results

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

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

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

Disabling Band Label

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

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
3. In the Policies window, select the active policy.
4. In the **Enrollment Settings** section, perform one of the following actions:

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

5. Click **Save**.

Results

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

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

Customizing Connected Worker Platform to support NEAs that check AD status

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

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

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

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

Configuring Check User Status

Perform the following steps to configure NES to provide the status of a user in active directory to a NEA.

About this task

Procedure

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

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

Customizing Nymi Lock Control Support

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

Configuring Nymi Lock Control

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

About this task

Procedure

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

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

5. Click **`Save`**.

Results

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

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

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

Disabling Nymi Lock Control

Perform the following steps to disable `Nymi Lock Control`.

About this task

Procedure

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
3. In the `Policies` window, select the active policy.
4. In the **`Lock Control`** section, clear the **`Enable Nymi Lock Control`** option.
5. Click **`Save`**.

Results

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

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

Manage Individual User Policies

After deploying NES, two individual user policies are available.

When you add users to these policies the user experiences the following behaviour:

- Liveness Detection Disabled - Biometric authentication of the Nymi Band only validates that there is a fingerprint match and does not perform a liveness check.
- Corporate Credentials Authentication - Biometric authentication and corporate credential authentication is supported authentication. To authenticate a Nymi Band by corporate credentials, the user logs into the `Nymi Band Application` with their username and password, while wearing their unauthenticated Nymi Band. *Customizing the Nymi Band Authentication Method* provide more information about using Corporate Credentials Authentication.

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

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

Creating an Individual User Policy

Perform the following steps to create a new individual user policy.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing `https://nes_server/NES_service_name` or `http://nes_server/NES_service_name`
   depending on the NES configuration, where:
   - *`nes_server`* is the Fully Qualified Domain Name (FQDN) of the NES host.
   - *`NES_service_name`* is the service mapping name for the NES web application. The default service mapping name is *nes*.

     For example, `https://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. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
4. On the **`Individual User Policies`** pane, click **`Create New Individual User Policy`**.
   The **`Create New Individual User Policy`** page appears.
5. In the **`Individual User Policy Name`** field, type a name for the policy.
6. Select the required policy options.
7. Optionally, in the **`Notes`** field, provide some descriptive text.
   The following figure provides an example of a new individual user policy with both the **`Liveness Detection Disabled`** and **`Corporate Credentials Authentication`** options enabled.

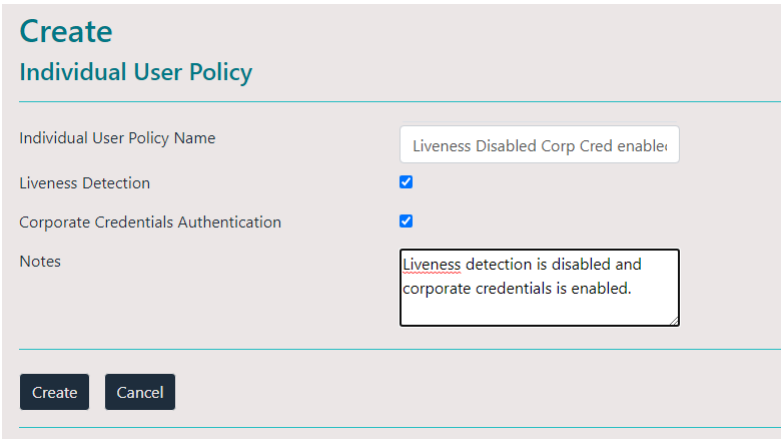


Figure 9: Create Individual Policy page

8. Click **Create**.
   The new policy appears in the **Individual User Policies** pane of the Policies page.

What to do next

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

Creating an Individual User Policy from an Existing Individual User Policy

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

About this task

Procedure

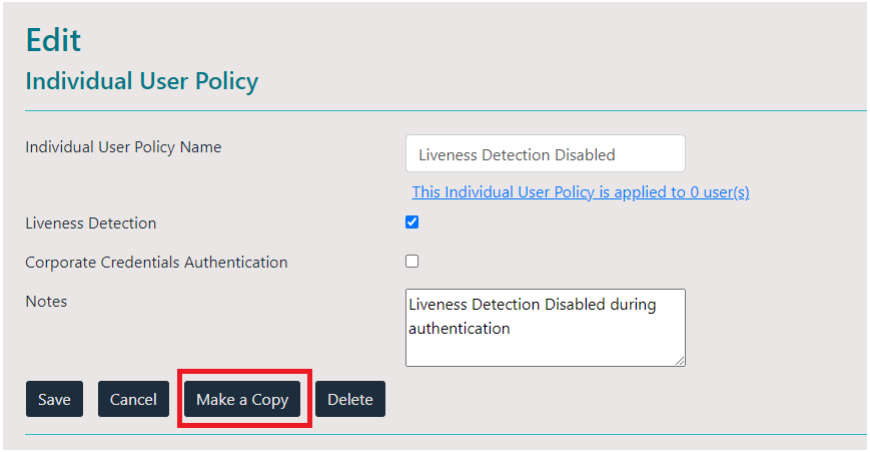
1. Connect to the NES Administrator Console in a browser by typing `https://nes_server/NES_service_name` or `http://nes_server/NES_service_name`
   depending on the NES configuration, where:
   - *nes_server* is the Fully Qualified Domain Name (FQDN) of the NES host.
   - *NES_service_name* is the service mapping name for the NES web application. The default service mapping name is *nes*.

     For example, `https://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. From the navigation bar, select **Policies**.
   The Policies page appears with a table that displays a list of existing group and individual policies.
4. On the **Individual User Policies** pane, select an existing policy.

The `Edit Individual User Policy` window appears.

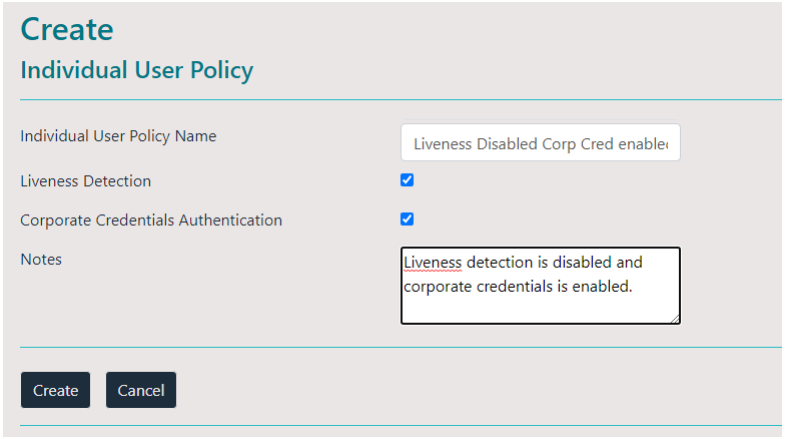
5. Click **`Make a Copy`**, as shown in the following figure.



`Figure 10: Make a Copy button`

The `Create Individual User Policy` window appears.

6. In the **`Individual User Policy Name`** field, type a name for the policy.
7. Select the required policy options.
8. Optionally, in the **`Notes`** field, provide some descriptive text.
   The following figure provides an example of a new individual user policy with both the **`Liveness Detection Disabled`** and **`Corporate Credentials Authentication`** options enabled.



`Figure 11: Create Individual Policy page`

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

What to do next

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

Deleting an Individual User Policy

Perform the following steps to delete an individual user policy.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing `https://nes_server/NES_service_name` or `http://nes_server/NES_service_name`

   depending on the NES configuration, where:

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

     For example, `https://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. From the navigation bar, select **`Policies`**.
   The `Policies` page appears with a table that displays a list of existing group and individual policies.
4. On the **`Individual User Policies`** pane, in the **`Individual User Policy Name`** column, select the policy.
5. Click **`Delete`**.
6. On the `Delete Individual User Policy` window, click **`Delete`**.

Results

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

Adding a User to an Individual User Policy

About this task

To add users to individual policy, perform the following steps.

Procedure

1. Connect to the NES Administrator Console in a browser by typing `https://nes_server/NES_service_name` or `http://nes_server/NES_service_name`

   depending on the NES configuration, where:

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

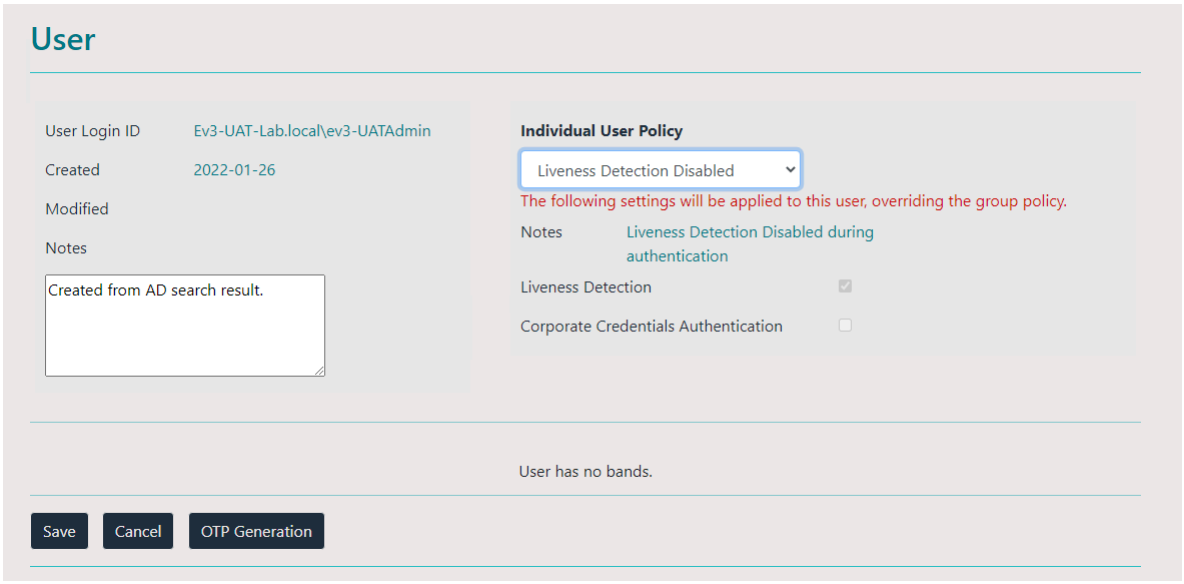
  For example, `https://server-2.nymi.lab/nes`.

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

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

   The following figure provides an example of the `User` properties page with the Liveness Detection Disabled policy selected.



`Figure 12: User Properties page`

7. Click **`Save`**.

Results

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

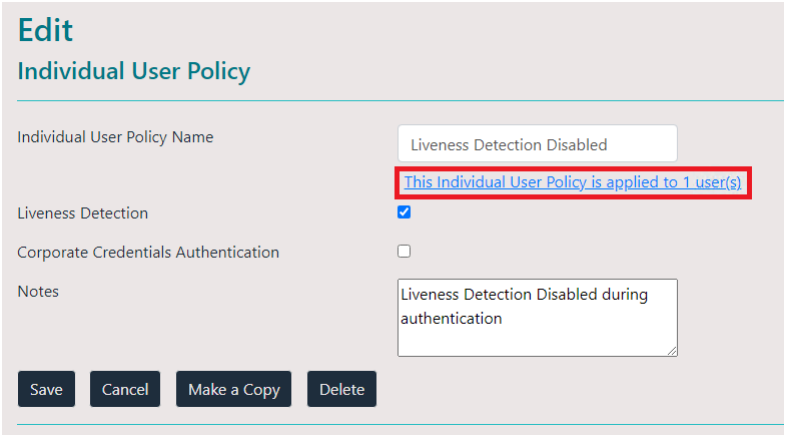
Displaying Individual User Policy Membership

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

About this task

Procedure

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



`Figure 13: Edit Individual User Policy page`

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

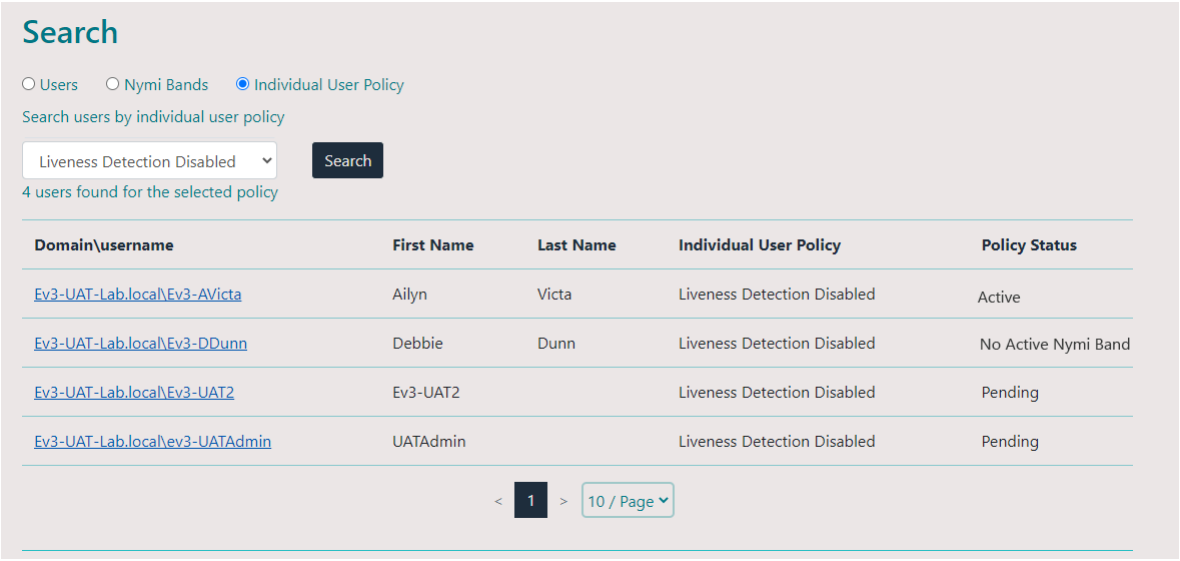
The search results include information about the status of the application of a policy to a user. There are four status types:

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

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

- Information unavailable - Enrollment occurred on an earlier version of `Nymi Band Application` that does not support the policy status features. Individual policy support starts with the CWP 1.3 `Nymi Band Application`.

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



`Figure 14: Individual User Policy Search Results`

Nymi Band Enrollment

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

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

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.

About this task

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 15: Nymi Band Displaying a Sample Setup Code`

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

Procedure

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.
5. 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.

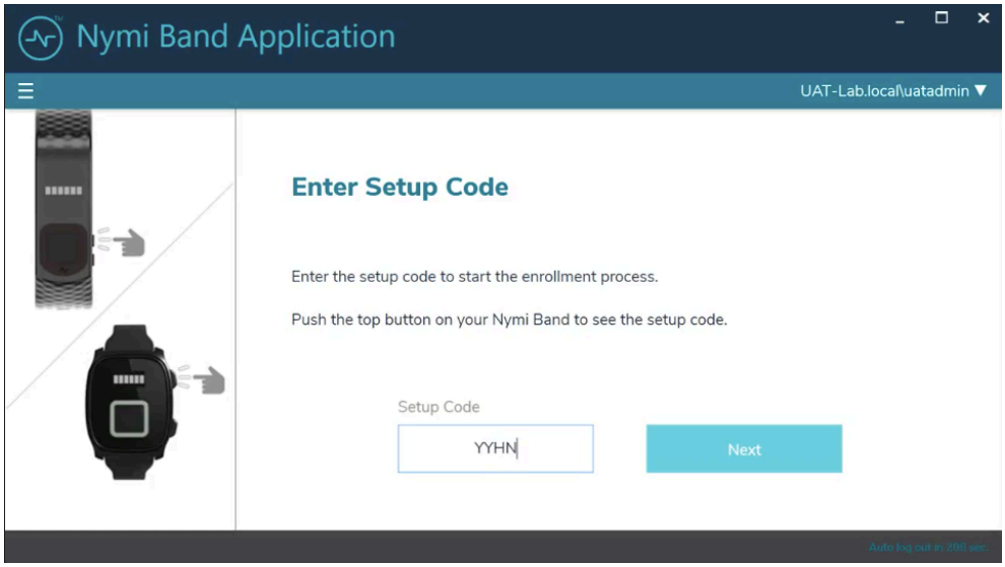


Figure 16: Enter Setup Code

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

Figure 17: Nymi Band Add User Screen

Results

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.

About this task

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

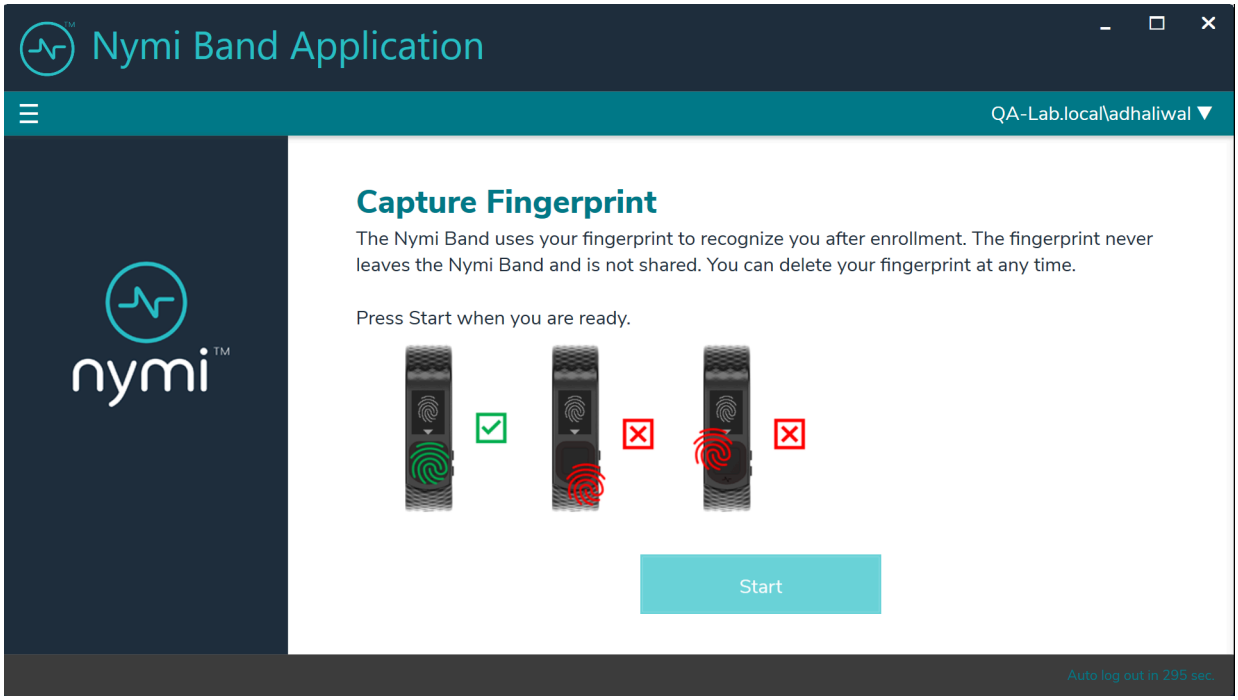
- Is placed on the sensor only when prompted
- Is lifted from the sensor only when prompted
- Is placed on the middle of the sensor and covers as much of the sensor as possible

- Is motionless on the sensor, while the sensor is capturing the image

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

Procedure

1. Reads the information on the `Capture Fingerprint` page.
   The following figure provides an example of the `Capture Fingerprint` page.



`Figure 18: Capture Fingerprint`

2. Clicks **`Start`**.
   The following figure provides an example of the `Capture Fingerprint` page after the user clicks **`Start`**.

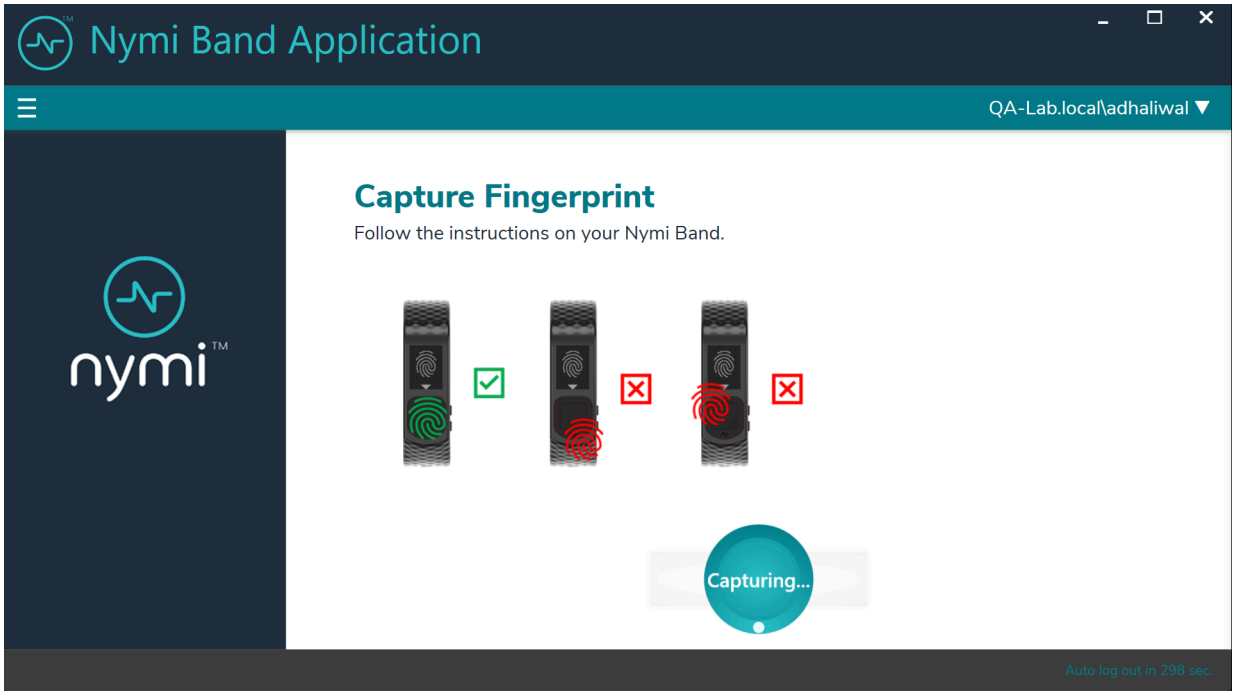


Figure 19: Capture Fingerprint In Progress

3. Waits for the **Fingerprint** icon to appear on the Nymi Band screen.
4. 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 20: FINGERPRINT

5. 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 21: LIFT FINGER

Figure 22: TOUCH SENSOR

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

Figure 23: 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

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

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

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

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

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

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.

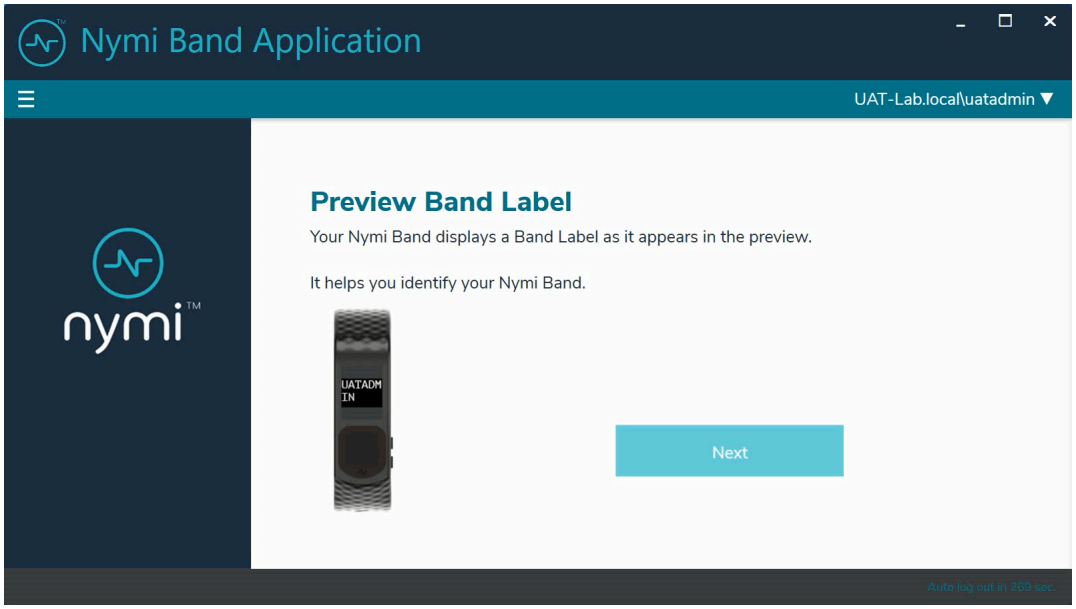


Figure 24: Preview Band Label

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.

About this task

Perform the following steps to customize the Band Label.

Procedure

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

   Supported Band Labels:

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

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

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

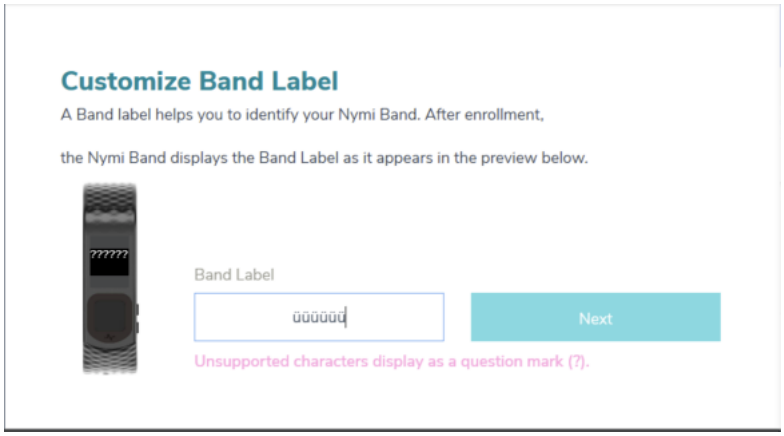


Figure 25: Custom Band Label Unsupported Characters

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.

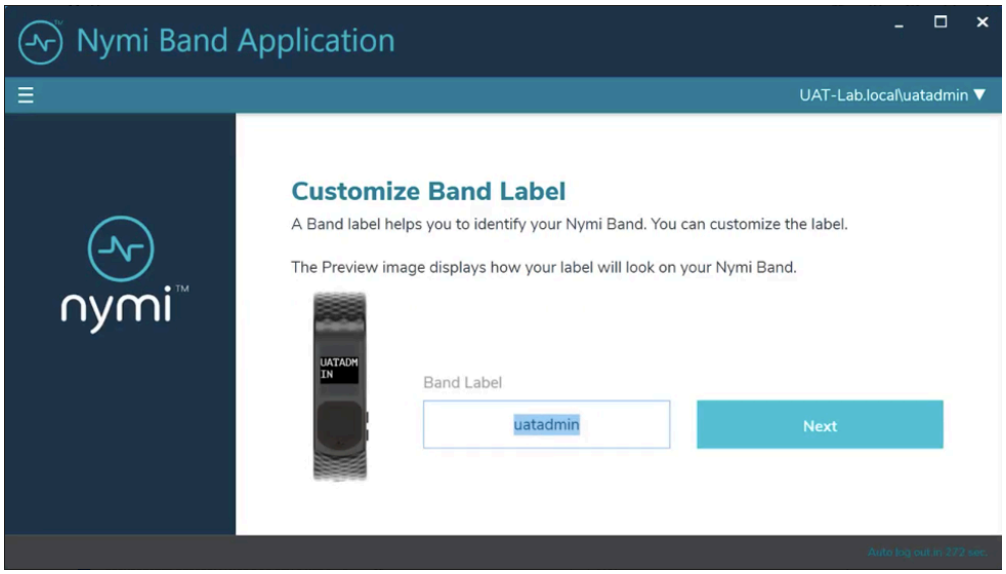


Figure 26: Custom Band Label Configuration

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.

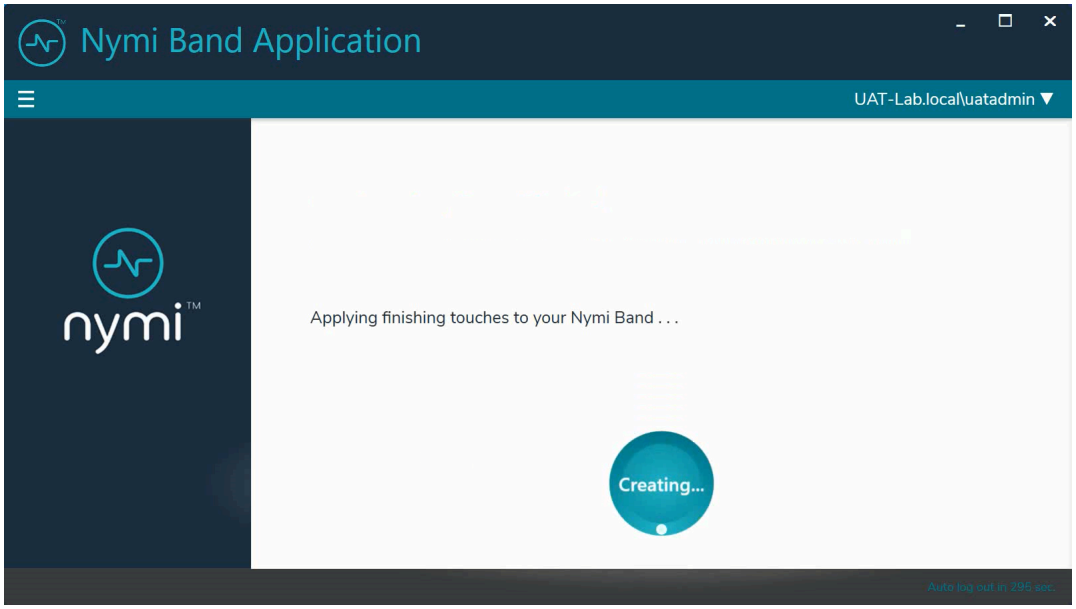


Figure 27: Applying Policy Settings

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.

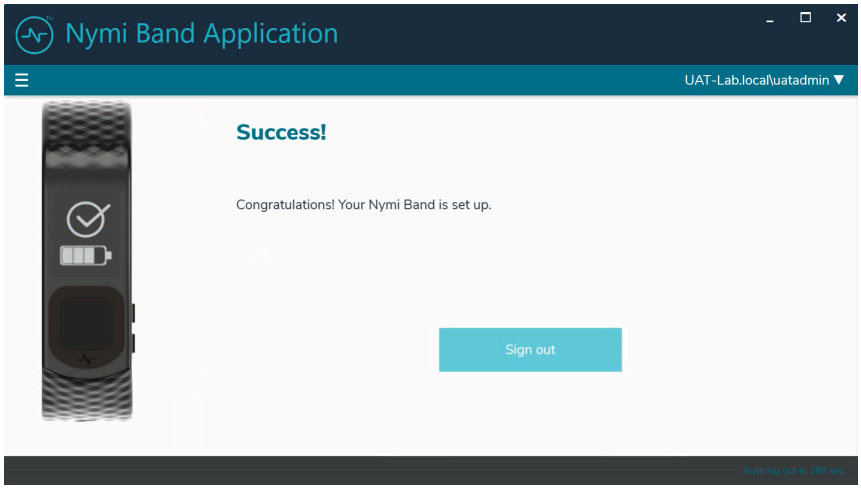


Figure 28: Success

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

Note: For environments that use the on-band attestation feature, after enrollment, the Nymi Band does not display the Health Check Status question and SEOS access is disabled. Instruct the user to remove the Nymi Band, and then authenticate to the Nymi Band again. The Health Check Status question appears and the user can perform their web-based attestation. The *Using Heath Attestation* chapter provides more information.

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

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

Using the Nymi Band

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

Authentication After Enrollment

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

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

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

Note: When the **`Attestation on Nymi Band`** option is enabled in the active NES policy, after the user authenticates to the Nymi Band, the Health Check Status question appears on the Nymi Band. The *Using Heath Attestation* chapter provides more information.

Authentication by fingerprint

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

Figure 29: 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 30: Authentication Success Screen with Band Label

Figure 31: Authentication Success Screen without Band Label

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.

Authentication Failures

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

Figure 32: Authentication Failure Screen with Retry message

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

- Fingerprint matching failure - when the authentication fails as a result of a fingerprint mismatch, the Nymi Band vibrates and displays the Retry message about 1 second after the user places their finger on the fingerprint sensor and bezel.
- Liveness failure - when the authentication fails due to the inability to detect a consistent ECG signal on the wrist, the Nymi Band vibrates and displays the Retry message about 13 seconds after the user places their finger on the fingerprint sensor and bezel.

Troubleshooting Fingerprint Mismatch Failures

If the fingerprint authentication fails, ensure the following:

- Fingerprint sensor is clean and dry.
  - If the fingerprint sensor is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
  - If the fingerprint sensor is wet, dry completely with a lint-free towel, and then retry authentication.

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

Troubleshooting Liveness Detection Failures

If the liveness detection fails, ensure the following:

- Bottom sensor is clean and dry.
  - If the bottom electrode is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
  - If the bottom electrode is wet, dry completely with a lint-free towel, and then retry authentication.
- User's finger is clean and dry.
  - If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication
  - If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
  - If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication
- User keeps their finger still on the sensor and bezel during the authentication period.
- User's wrist is not too dry. Before authentication, wash and completely dry the wrist before putting on the Nymi Band, or rub some lotion well into the wrist, and then retry authentication.
- Nymi Band bottom electrode remains in contact with the wrist during the authentication period. If the position of bottom electrode prevents contact, remove the Nymi Band, reposition the Nymi Band on the wrist, and then try authentication again.
- User does not lift their finger off the sensor or bezel until the authentication process completes.
- Ensure that the Nymi Band fits snugly on the wrist and does not move around during the authentication process.

Note: The SQL database contains a record of the failed authentication attempt. The section *Collecting Data From a Nymi Band* provides more information.

Authentication Lockout

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

After 50 consecutive failures due to a fingerprint mismatch, the Nymi Band displays the See Admin icon and prevent the user from performing additional authentication attempts.

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

Clear the lockout by one of the following methods:

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

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

Viewing Nymi Band Text

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

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

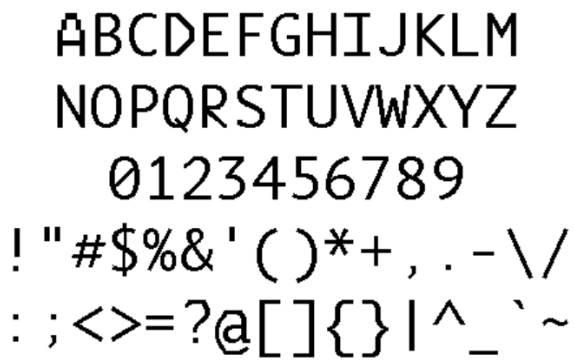


Figure 33: Nymi Band Font

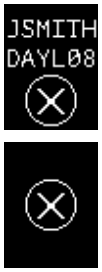
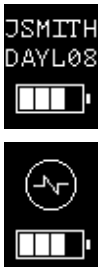
Viewing Nymi Band Screens

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 5: Nymi Band Screen

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

Nymi Band Screen	Nymi Band Screen Name	Description
 	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. The lockout prevents the user from authenticating with their fingerprint.
	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.
	Heath Check Status Required	Indicates that the Nymi Band is awaiting input from the user to provide the status of their web-based attestation results.
	Health Check/Secondary Screening Success	Appears when the user provides the Nymi Band with a positive attestation result, by holding down the top button on the Nymi Band.
	Health Check Failure	Appears when the user provides the Nymi Band with a negative attestation result, by holding down the bottom button on the Nymi Band.
	SEOS Disabled	Indicates that SEOS is not enabled. Appears in the following scenarios: • After the user sees the health check failure icon, which indicates that the user failed the web-based attestation. User can also see the icon in the Nymi Band Dashboard. • After a user wears a SEOS-enabled authenticated Nymi Band for 18 consecutive hours, the Nymi Band disables SEOS. **Note:** SEOS remains disabled until the the user authenticates to the Nymi Band again and provides a positive positive attestation result

Nymi Band Screen	Nymi Band Screen Name	Description
	SEOS Enabled	Indicates that SEOS is enabled. Appears after the user sees the health check success icon, which indicates that the user passed web-based attestation. User can also see the icon in the Nymi Band Dashboard.
	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.
	High Temperature Alert	Indicates that an authenticated Nymi Band has detected a wrist temperature that exceeds the normal range. This image remains on screen until the user presss any button on the Nymi Band to dismiss the alert.
	Secondary Screening Required	Indicates that the Nymi Band is awaiting the user to proceed to the secondary screening area for additional health evaluation, and provide the results. Appears after the user clears the High Temperature Alert screen. This image remains on screen until the user registers the results of their secondary screening on the Nymi Band.
	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 process of deleting user data is running. Deleting user data on a Nymi Band removes all the data for the currently enrolled user from the Nymi Band.
	User Data Deleted	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 34: 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 35: 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 36: Band Label on a charging Nymi Band

Nymi Band Dashboard

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

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

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

When on band attestation is enabled, a bottom arrow appears on the dashboard and you can press the bottom button to display the SEOS status. At the top of the SESO status screen, an arrow appears and you can press the top button to return to the dashboard screen.

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

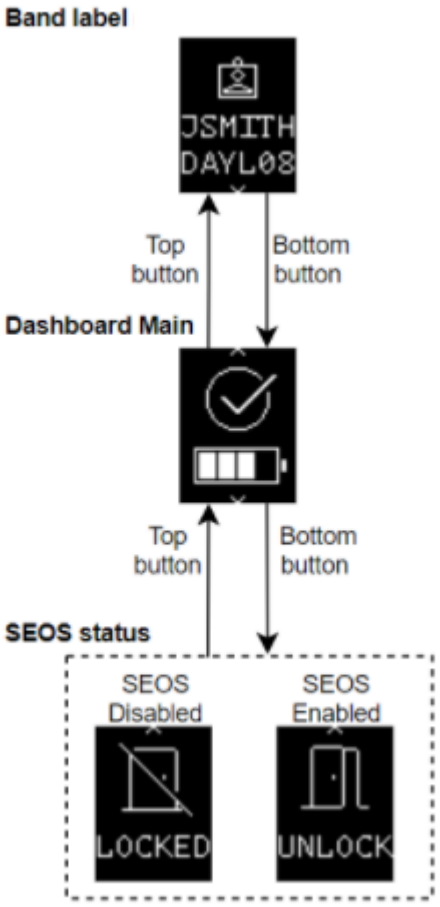


Figure 37: Nymi Band Dashboard carousel

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	• Nymi Band detects user's finger at the beginning of an authentication • Nymi Band starts charging

Vibration Event	Details	When is it used
Success	Two short vibrations in quick succession. Used when the Nymi Band confirms an operation is successfully completed	• Nymi Band's authentication success • Fingerprint enrollment success • Start of restart or security wipe sequence
Warning	Long vibration. Used when the Nymi Band confirms that an operation is successfully completed	• Failed authentication • Nymi Band transition from authenticated state to deauthenticated state • High temperature alert
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.	• 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.

SEOS Access

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

However, when you enable the **`Attestation on Nymi Band`** option in the active NES policy, the Nymi Band behaviour is as follows:

- After a user authenticates to their Nymi Band, SEOS access is disabled until the user records a postive attestation result on the Nymi Band.
- After a user authenticates to their Nymi Band and provides a postive attestation result, SEOS access remains enabled for up to 18 consecutive hours, at which time SEOS access is disabled and the 

icon appears. To enable SEOS access again, the user must remove the Nymi Band, authenticate to the Nymi Band, and then be able to provide a postive attestation status.
- When the user removes their authenticated SEOS-enabled Nymi Band, the Nymi Band deauthenticates and SEOS is disabled.
- After a user authenticates to their Nymi Band, SEOS access is disabled if the user provides a negative attestation, and remains disabled until the user re-authenticates to the Nymi Band and is able to provide a postive attestation status.

The chapter *Using Health Attestation* provides more information about how to use the Nymi Band when the **`Attestation on Nymi Band`** option is enabled in the NES active policy.

Collecting Data From a Nymi Band

Each environment has one or more user terminals on which the `Nymi Edge Agent` is installed.

When a user who is wearing an authenticated Nymi Band is within range of an `Nymi Edge Agent` user terminal or is placed on a charger near an `Nymi Edge Agent` terminal, the `Nymi Edge Agent` collects the following information on the Nymi Band:

- Authentication attempts, including Nymi Band ID, the reasons for the failure (fingerprint or ECG) and time of the attempt.
- Temperature Alerts (when the Temperature Alert feature is enabled), including the Nymi Band ID, time and a record that an alert was generated.
- On-band Attestation response (when the Health Attestation feature is enabled), including user information, time that the response was recorded, and the response result.
- Contact Tracing Events (when SDCT feature is enabled), including the Nymi Band IDs of the Nymi Band and the time of the event

The `Nymi Edge Agent` application sends the information to the Data Exchange Service, which resides in the Kubernetes cluster. The data is stored in tables in the `CWP Database`.

Using the Contact Tracing Dashboard

Access the Contact Tracing Dashboard to visualize and analyze contact tracing data for employees that are enrolled in the Contact Tracing program.

Proximity events that are logged in each employee's Nymi Band are uploaded to the Contact Tracing Dashboard via the `Nymi Edge Agent` that is installed on a user terminal. These contact events are viewed on the Contact Tracing Dashboard, where they can be analyzed to provide:

- Timely and targeted response for positive diagnosis.
- Timely and reliable contact tracing history.
- Coverage information and trends on social distancing performance.
- Targeted intervention to modify behavior and prevent an outbreak.

Accessing the Contact Tracing Dashboard

Connect to the Contact Tracing server in a web browser.

About this task

Procedure

1. From web browser, navigate to `https://FQDN_CTAPI/dashboard`.
   where *`FQDN_CTAPI`* is the FQDN of the virtual server on which `CTAPI` resides.
2. Log in using the Contact Tracing Dashboard username and password. Alternatively, you can log in with the credentials of an NES Administrator.
   The format of the username is *`username@domain`*. For example, for user dredmond in domain qa-lab.local, specify the username as `dredmond@qa-lab.local`.

Viewing the Contact Tracing Dashboard

The Contact Tracing Dashboard is used to visualize and analyze contact tracing data for employees enrolled in the Contact Tracing program. This section provides detailed information on viewing the Contact Tracing Dashboard and analyzing the contact tracing data.

Contact Tracing Dashboard Example

The following figure shows the Contact Tracing Dashboard

Figure 38: Example of the Contact Tracing Dashboard

Enrolled Employees

Identifies the number of employees that are enrolled in the Smart Distancing and Contact Tracing program.

Social Distancing Compliance (%)

Identifies the percentage of employees who have had no contact with other employees for a given day.

The higher the score, the more compliant employees are in maintaining distancing. This report is based on data from the last 30 days.

For example, with a program population of 100 employees, if 2 people are in contact with each other, the compliance score drops to 98%.

Average and Maximum Contacts (%)

The average identifies the percentage of protected employees that are contacted by an individual expressed as an average across all employees registered in the program. The maximum identifies the highest percentage of employees contacted by any single individual.

For example, with a program population of 100 employees, if on a given day, only one employee came in contact with 10 people (i.e., 10% of the enrolled employee population), the average contact percentage would be 0.1% and maximum contact % would be 10% for that day.

Most Contacted Employees

Identifies the employees who have the most contact events in the program. This report is based on data from the last 30 days.

Total Contacts by Day

Identifies The total number of contact events within the program per day.

A contact event is recorded when a Nymi Band user is closer than ~2 meters from another Nymi Band for approximately 15 or more cumulatative minutes over a 24-hour period.

Most Contacted Employee Details

Identifies the number of contact event and the employees contacted for the employee with the most contact events.

This report is based on data from the last 30 days.

Employee Contact Timeline

Provides adminstrators with a timeline of all contact events for a specific employee within a date range.

You can search by username or date. Consider the following:

- Default date range is last 30 days.
- Search terms are case sensitive.
- Timestamp for a contact event is date and time of the last proximity event.
- Timestamps appear in the timezone that is defined on the browser that you use to access the Contact Tracing Dashboard

Using Health Attestation

Connected Worker Platform(CWP) provides organizations with the ability to manage access into the workplace based on the results of an individual's self assessment.

When a CWP Administrator enables the **`Attestation on Nymi Band`** option in the active NES policy, the health attestation feature on the Nymi Band is enabled. After a user successfully authenticates to their Nymi Band, the Nymi Band displays a Health Check Status question. If the user provides a positive answer on the Nymi Band, the Nymi Band grants users with the ability to use the Nymi Band to gain physical access to a SEOS-enabled door. If the user provides a negative answer on the Nymi Band, the ability to use Nymi Band to the gain physical access to a SEOS-enabled door remains disabled.

Optionally, corporate policy might require that users complete an independent health attestation prior to answering the health status question on the Nymi Band. Nymi provides an optional web-based attestation application that allows administrators to display a set of pre-defined health check questions, which the user answers and submits. The application provides the user with the results of the attestation (pass or fail), and the user can then indicate the result on the Nymi Band. The web application also provides Health and Safety personnel with a web-based Health Dashboard to view historical information about attestation results for users and allows personnel to record the outcome of subsequent secondary screening, if required.

Note: The health check questions provided in the application are fixed and a record of each attestation result is stored for 30 days. If you require changes, contact your Nymi Solution Consultant.

Web-Based Attestation

Nymi provides a web-based attestion application with pre-defined health check questions, which allows users to answer the health check questions on a web-based form from their smartphone, computers, and tablets. When the user submits their answers, the web-based attestation application provides the user with their results.

Supported browsers

The web-based attestation application supports the following browsers:

- Google Chrome on Windows terminals and Android devices
- Microsoft Edge on Windows terminals
- Safari on OSX and iOS devices.

Performing Web-based Attestation

The user performs web-based attestation to self-evaluate the state of their health.

Before you begin

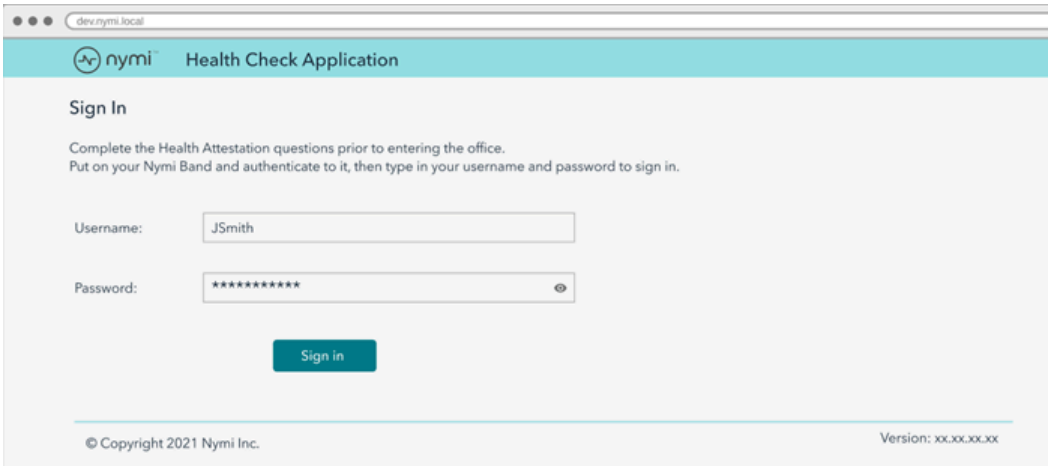
Access to web-based attestation requires the Active Directory (AD) credentials of the user, but does not require the user to connect to the corporate network.

About this task

After successful authentication, the Nymi Band screen prompts the user for the results of their web-based attestation. Perform the following steps to complete web-based attestation.

Procedure

1. From a web browser, connect to the `Health Check Application` website.
   The login page appears, as shown in the following figure.



   `Figure 39: Web-based Attestation Login Page`

2. In the **`Username`** field, type the AD username for the user account.
3. In the **`Password`** field, type the password for the user account.
4. Click **`Sign in`**.
   The `Health Attestation question` page, which displays a list of mandatory questions, and the date and time of the last attestation completed by the user.
5. On the `Health Attestation question` page, select the appropriate radio button to answer each question.

   A red asterix appears at the end of each mandatory question.

   After the user selects an answer for all the mandatory questions, the application enables the **`Submit`** button.
6. Click **`Submit`**.
   The application analyzes the responses to each question and displays the health check status of the user in `Assessment Results` page.

Results

The `Assessment Results` page displays a positive or negative status depending on a pre-defined scoring of the answer to each question.

- When the health check status is positive, the application instructs the user that they are approved to go to work and displays the following screen:

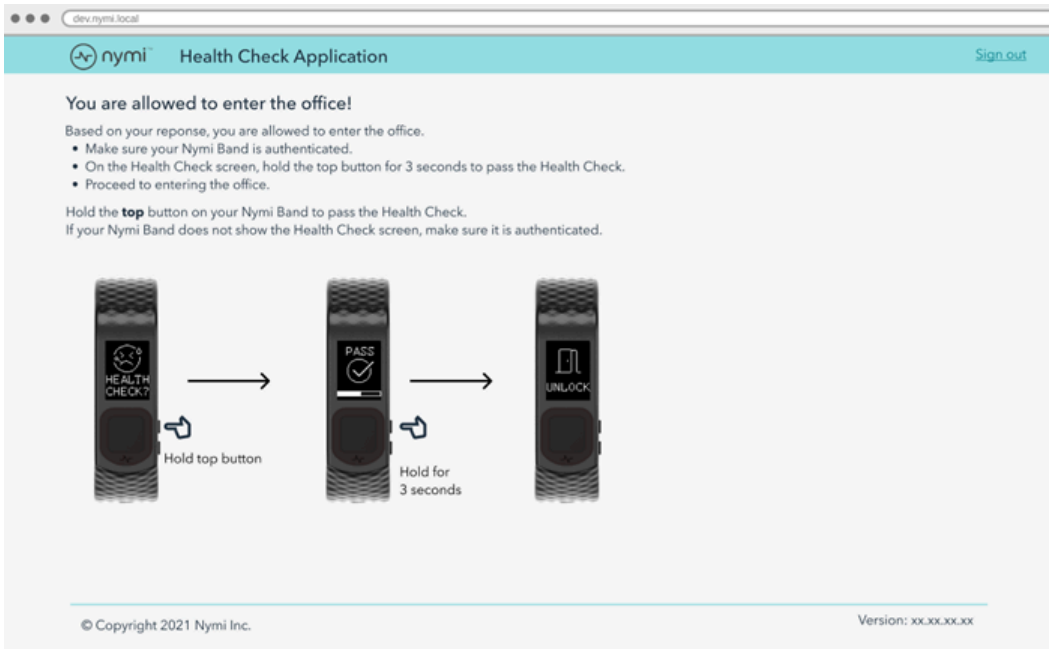


Figure 40: Positive Assessment Results page

- When the health check status is negative, the application instructs the user that they are not approved to go to work and displays the following screen:

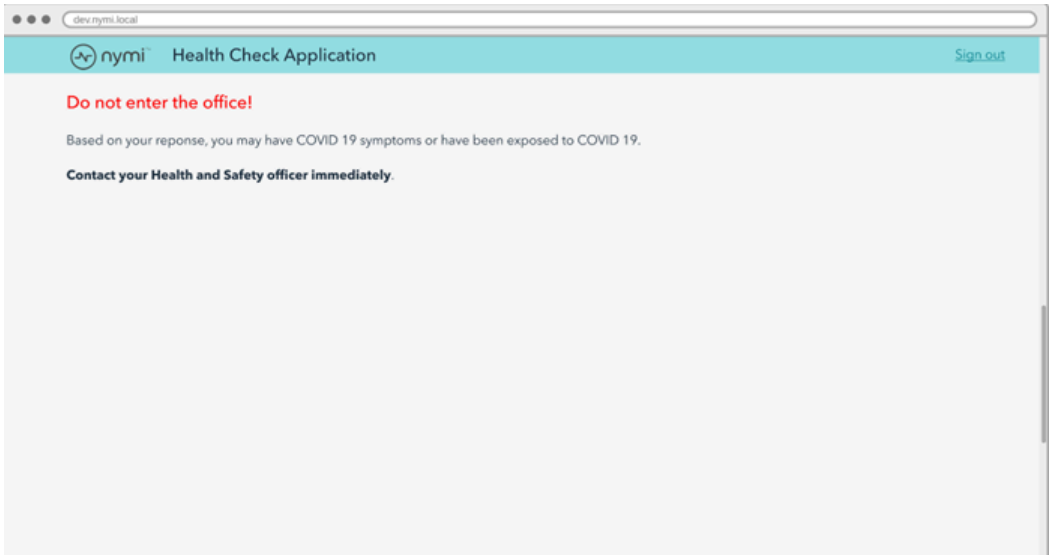


Figure 41: Negative Assessment Results page

Performing Attestation on the Nymi Band

After the user authenticates to their Nymi Band and completes their web-based attestation, the user provides their attestation results to the Nymi Band.

About this task

Perform the following steps on the Nymi Band.

Procedure

1. If the Nymi Band screen is blank, press any button to wake up the Nymi Band.

   The Health Check Status question 

appears.
2. Perform one of the following actions:
   - To record a positive attestation result, hold the top button for at least 3 seconds.

     The Heath Check Success status icon 

appears with a progress bar, and then disappears when the Nymi Band records an attestation success.

     The SEOS enabled icon 

appears and the and the Nymi Band vibrates. The user can use the Nymi Band for physical access on SEOS-enabled doors.
   - To record a negative attestation result, hold the bottom button for at least 3 seconds.

     The Heath Check Failure status icon 

appears with a progress bar, and then disappears when the Nymi Band records an attestation failure. The SEOS disabled icon 

appears and the Nymi Band vibrates.

     The user cannot use the Nymi Band for physical access on SEOS-enabled doors.

   The user can later view the SEOS status in the Nymi Band Dashboard, by using the buttons on the Nymi Band to navigate to the SEOS status screen.

Accessing Health Attestation and Secondary Screening Results

Authorized Health and Safety personnel use the `Health Check Application` to view health attestation and secondary screening results for employees.

You can review the results in the following formats:

- Daily attestation and secdonary screening result totals.

- Detailed daily attestation results for all employees filtered by event type. Event types include:
  - Passed attestations
  - Failed attestations
  - Completed attestations
- Detailed attestation results for individual employees filtered by day and event type. Event types include:
  - Passed attestations
  - Failed attestations
  - Completed attestations
- Secondary screening results filtered by day for all employees or individual employees.

Note: You can view attestion and secondary screening results that have been recorded in the last 30 days.

View Daily Attestation Summary Results

The `Health Check Application` provides Health and Safety personnel with the ability to review summary and drill-down information for daily attestation results on the current day or a previous day.

Viewing Daily Health Attestation Results for the Current Day

The `Health Check Application` main page provides Health and Safety personnel with the ability to review summary and drill-down information for daily attestation results on the current day.

About this task

Perform the following steps to view the health attestation results for all employees on the current day.

Procedure

1. Log in to the `Health Check Application` as a user with administrator access.

   The `Health Check Application` main page appears with the health attestation daily summary results for the total number of employees that passed, failed, and completed a web-based attestation on the current day. The following figure provides an example of the `Health Check Application` main page with the `Health Attestation Daily Summary` pane highlighted.

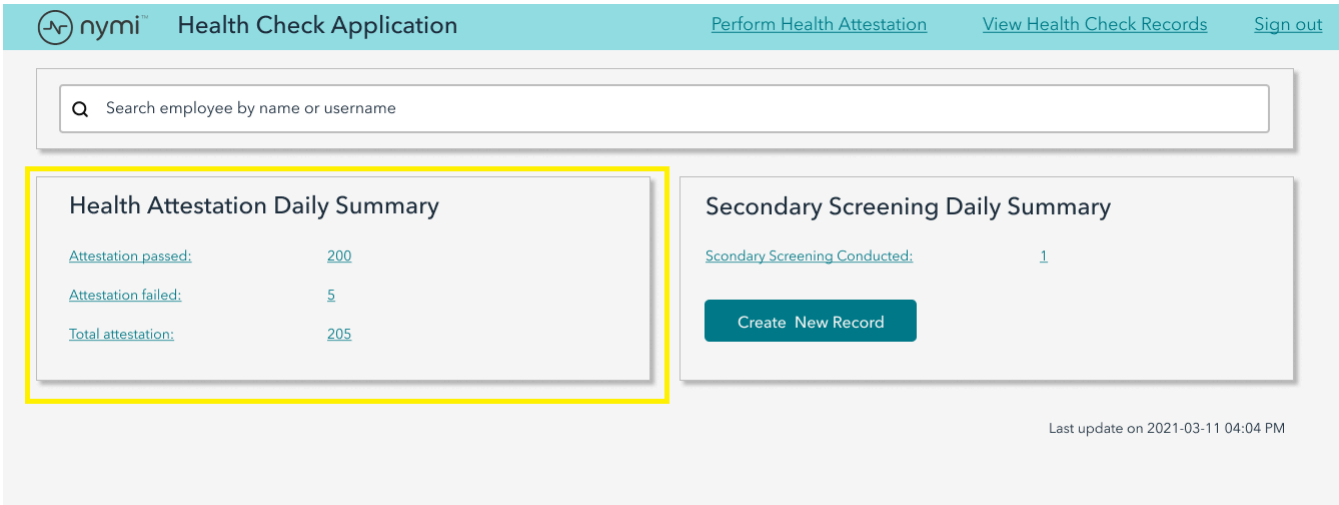


Figure 42: Health Attestation Daily Summary

2. Perform one of the following actions to drill-down into the daily summary results:

   - To view a list of all employees that passed a health check attestation, click the **Attestations Passed** label or value.
   - To view a list of all employees that failed a health check attestation, click the **Attestations Failed** label or value.
   - To view a list of all employees that completed a health check attestation, click the **Attestations Completed** label or value.

   Note: If an employee submits more than one attestation a day, only the results of most recent attestation of the day appears in the results.

   The Daily Summary window appears with the results. The following figure provides an example of the results window.

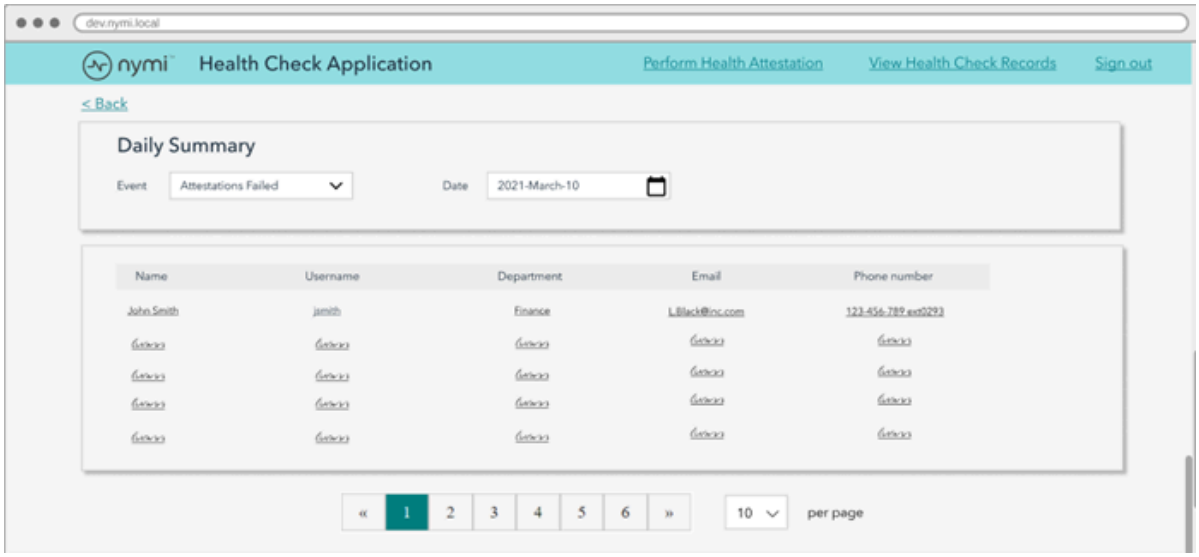


Figure 43: Attestation Daily Summary windows

Viewing Daily Health Attestation Results for a Previous Day

The **Health Check Application** main page provides Health and Safety personnel with the ability to review summary and drill-down information for daily attestation results on previous days, within the last 30 days.

About this task

Perform the following steps to view the health attestation results for all employees on a previous day.

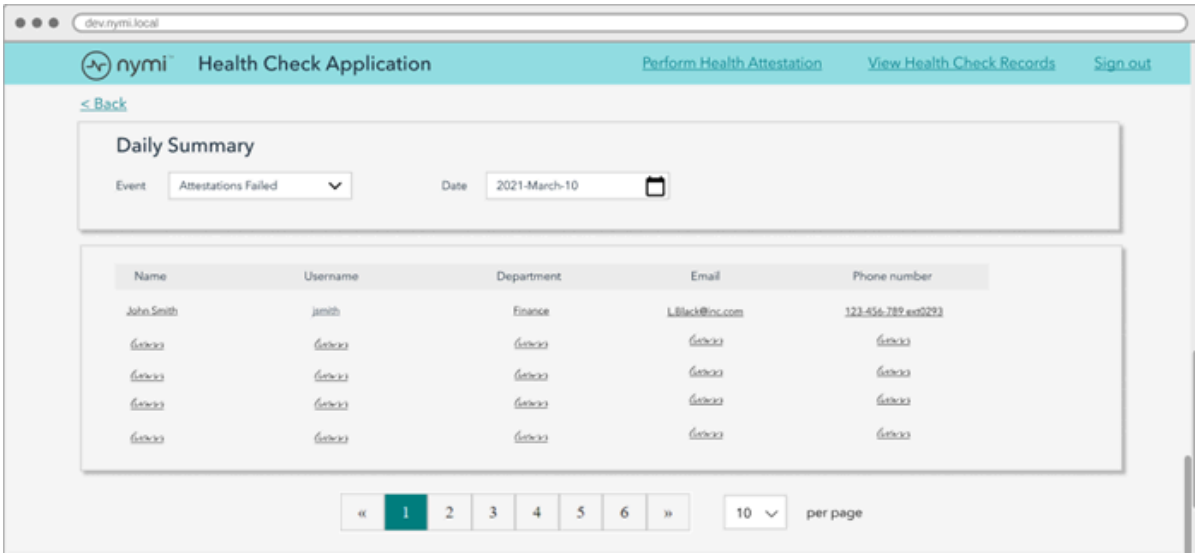
Procedure

1. Log in to the **Health Check Application** as a user with administrator access.
   The **Health Check Application** main page appears.
2. From the menu, click **View Health Check Records**.
3. On the **Event** list, perform one of the following actions:
   - To view a list of all employees that passed a health check attestation, select **Attestations Passed**.
   - To view a list of all employees that failed a health check attestation, click the **Attestations Failed**.
   - To view a list of all employees that completed a health check attestation, click the **Attestations Completed**.

   The results appear for the day that appears in the **Date** field.

   Note: If an employee submits more than one attestation a day, only the results of most recent attestation of the day appears in the results.
4. Click in the **Date** field, and then in calendar, select the appropriate date.

The `Daily Summary` results window appears with the results. The following figure provides an example of the `Daily Summary` results window.



`Figure 44: Attestation Daily Summary windows`

Viewing User Attestation and Secondary Screening Results

The `Health Check Application` main page provides Health and Safety personnel with the ability to search for users to view information about their attestation results from the last 30 days.

About this task

Perform the following steps to view the health attestation results for an employee.

Procedure

1. Log in to the `Health Check Application` as a user with administrator access.
   The `Health Check Application` main page appears with the **`User Search`** field. The following figure provides an example of the `Health Check Application` main page with the `User Search` field highlighted.

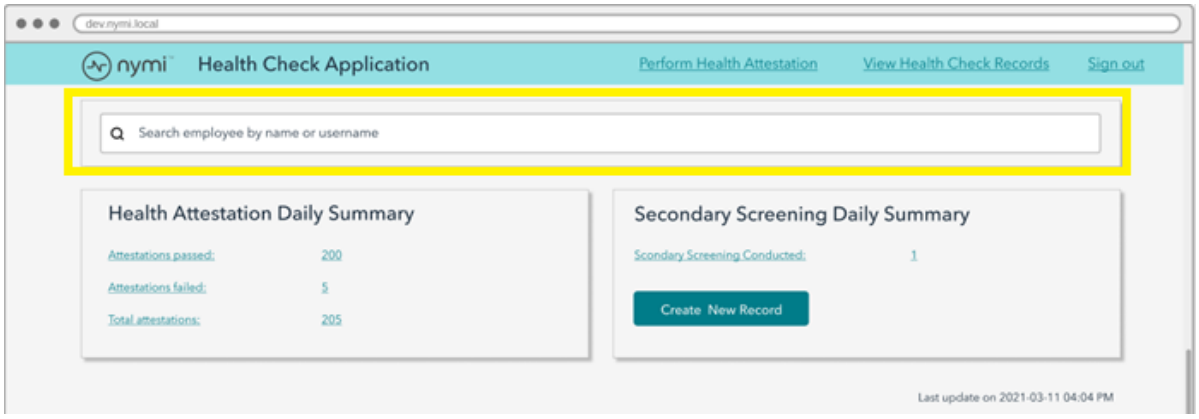


Figure 45: Health Attestation Daily Summary

2. In the **User Search** field, type the first name, last name, or username of the employee.

   A search results list appears with user matches as you type characters, as shown in the following figure.

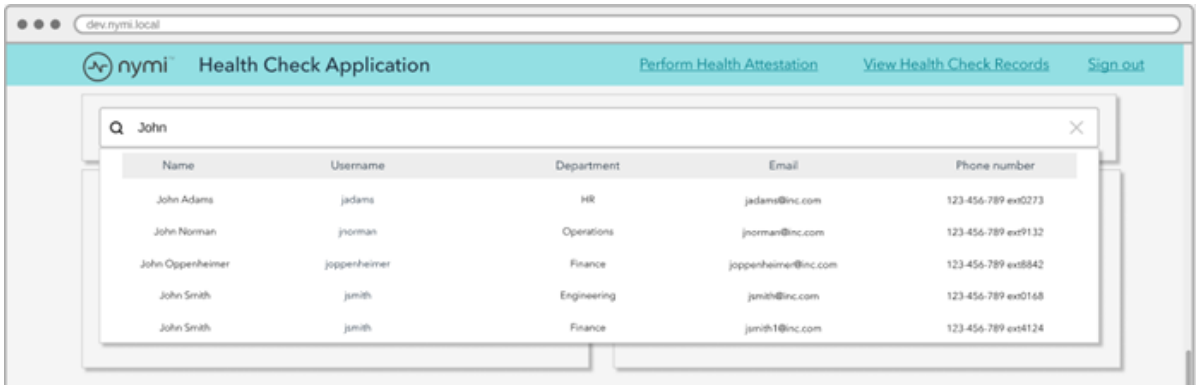


Figure 46: Employee search field

3. Select the appropriate user from the search results list.

   The `Employee Details` page appears and displays the `Employee Profile` pane, `Attestation Records` pane, `Secondary Screening Result` and `Secondary Screening Records` pane. The following figure provides an example of the `Employee Details` page.

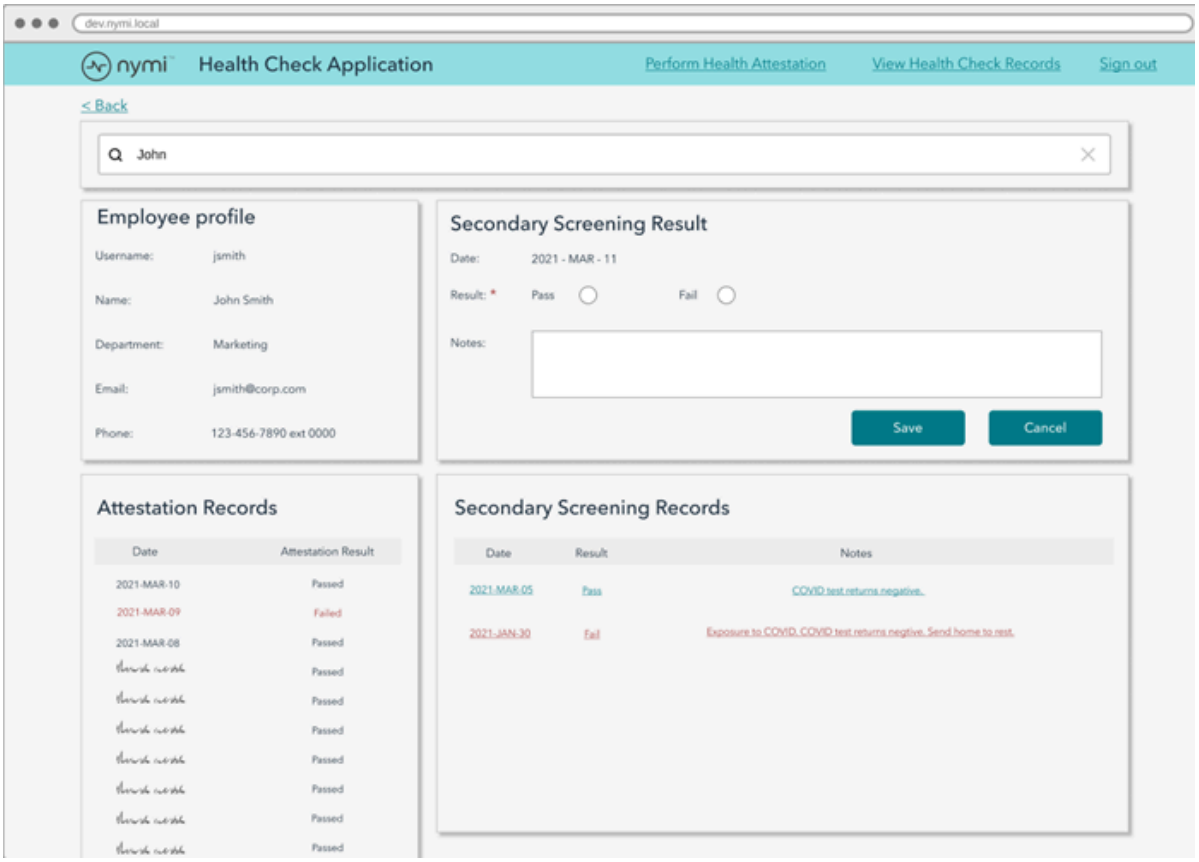


Figure 47: Employee Details page

Using Temperature Alerts

The CWP solution offers organizations the ability to alert Nymi Band users to elevations in skin temperature, and to prompt the user to perform secondary screening.

When you enable the **`Temperature Alerts`** option in the active NES policy, an authenticated Nymi Band monitors fluctuations in the skin temperature of the wrist over time, and creates a baseline skin temperature profile. When the Nymi Band detects an elevation that deviates from the temperature profile of the Nymi Band user, the Nymi Band displays an alert, and then prompts the user to proceed to a secondary screening station for an additional health assessment. The secondary screening prompt remains on the screen until cleared by an administrator during secondary screening. The Health and Safety personnel access the `Health Check Application` to record secondary screening information for a user when the user receives an alert for an elevated temperature.

You can use temperature alerts in conjunction with health attestation; however, you can use both features independently.

Consider the following information about temperature alerts:

- The Nymi Band does not display an absolute temperature reading for the user and only provides the user with an alert when their wrist temperature is higher than their usual wrist temperature.
- After the Nymi Band creates a temperature profile, an authenticated Nymi Band assesses temperature data for the user hourly. When the Nymi Band detects an elevated temperature for a period of time, the Nymi Band displays an alert to the user.
- A SQL database contains a record of the temperature alerts. The section *Collecting Data From a Nymi Band* provides more information.

Note: The Nymi Band is not a medical device and looks for deviations in skin temperature over time, which is not equivalent to a core body temperature measurement.

Performing Secondary Screening

When the Nymi Band displays the secondary screening prompt , the Nymi Band user should proceed to the secondary screening area as directed by corporate policies. Health and Safety personnel use the `Health Check Application` to register a the arrival and diagnosis of the user at a secondary screening station.

About this task

Perform the following actions to complete secondary screening of a Nymi Band user.

The data collected should be kept to a minimum to protect user privacy.

Procedure

1. Log in to the `Health Check Application` as a user with administrator access.
2. In the **`User Search`** field, type the first name, last name, or username of the employee.

A search results list appears with user matches as you type characters, as shown in the following figure.

Figure 48: Employee search field

3. Select the appropriate user from the search results list.

   The `Employee Details` page appears and displays the `Employee Profile` pane, `Attestation Records` pane, `Secondary Screening Result` and `Secondary Screening Records` pane. The following figure provides an example of the `Employee Details` page.

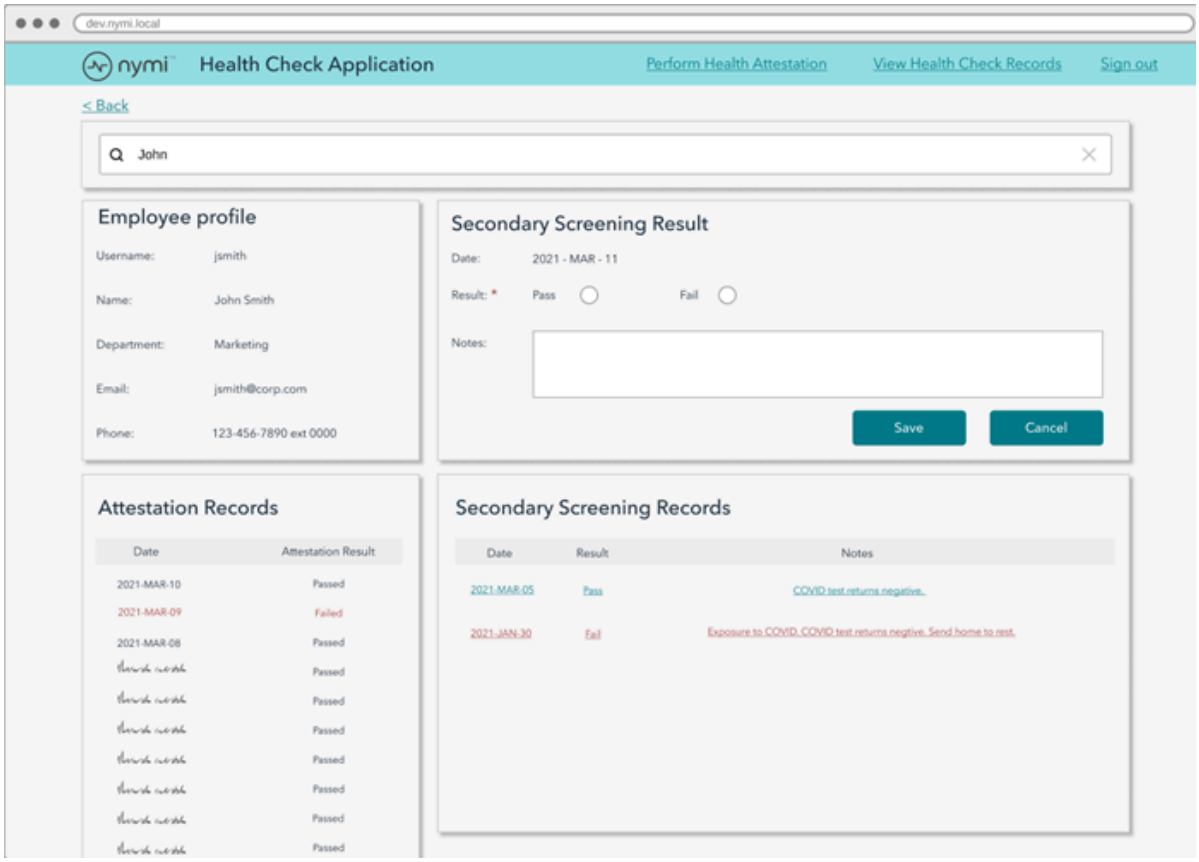


Figure 49: Employee Details page

4. In the Secondary Screening Result pane, perform the following actions:
   a) After taking the temperature of the employee, select **Pass** if the employees does not have a fever, or **Fail** if their temperature is over the value defined by your corporate policies.
   b) Optionally, in the **Notes** field, provide details about the screening, ensuring that you include the details that are required by your corporate policies.
   c) Click **Save**.
   The secondary screening result appears in the Secondary Screening Records pane.
5. Perform one of the following actions on the Nymi Band:

- If the secondary screening result determines that the user can remain in the workplace, instruct the user to press the top button of the Nymi Band for about three seconds.
- Optionally, if the secondary screening result determines that the user cannot remain in the workplace, instruct the user to press the bottom button of the Nymi Band for about three seconds.

Modifying Secondary Screening Results

`Connected Worker Platform` tracks one secondary screening result per day. Health and Safety personnel can modify secondary screening results, as required.

About this task

Perform the following actions to modify and existing secondary screening record for a Nymi Band user.

Procedure

1. Log in to the `Health Check Application` as a user with administrator access.
2. In the **`User Search`** field, type the first name, last name, or username of the employee.

   A search results list appears with user matches as you type characters, as shown in the following figure.

   `Figure 50: Employee search field`

3. Select the appropriate user from the search results list.

   The `Employee Details` page appears and displays the `Employee Profile` pane, `Attestation Records` pane, `Secondary Screening Result` and `Secondary Screening Records` pane. The following figure provides an example of the `Employee Details` page.

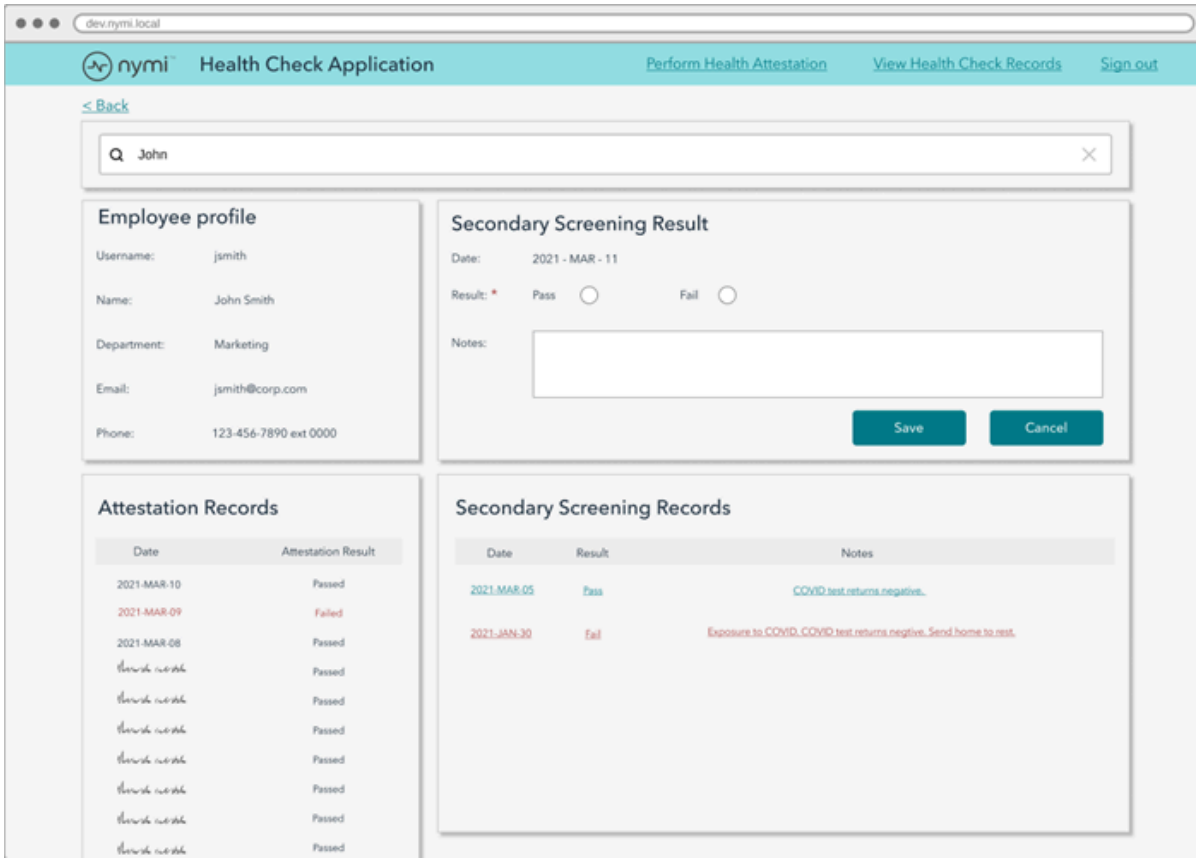


Figure 51: Employee Details page

4. In the Secondary Screening Records pane, click the **Date**, **Result**, or **Notes** hypertext link.
   The secondary screening record appears in Secondary Screening Result pane.
5. In the Secondary Screening Result pane, edit the record, as required, and then click **Save**.
   The Secondary Screening Records displays the updated record.

Viewing Daily Secondary Screening Results for the Current Day

The Health Check Application main page provides Health and Safety personnel with the ability to review summary and drill-down information for daily attestation results on the current day.

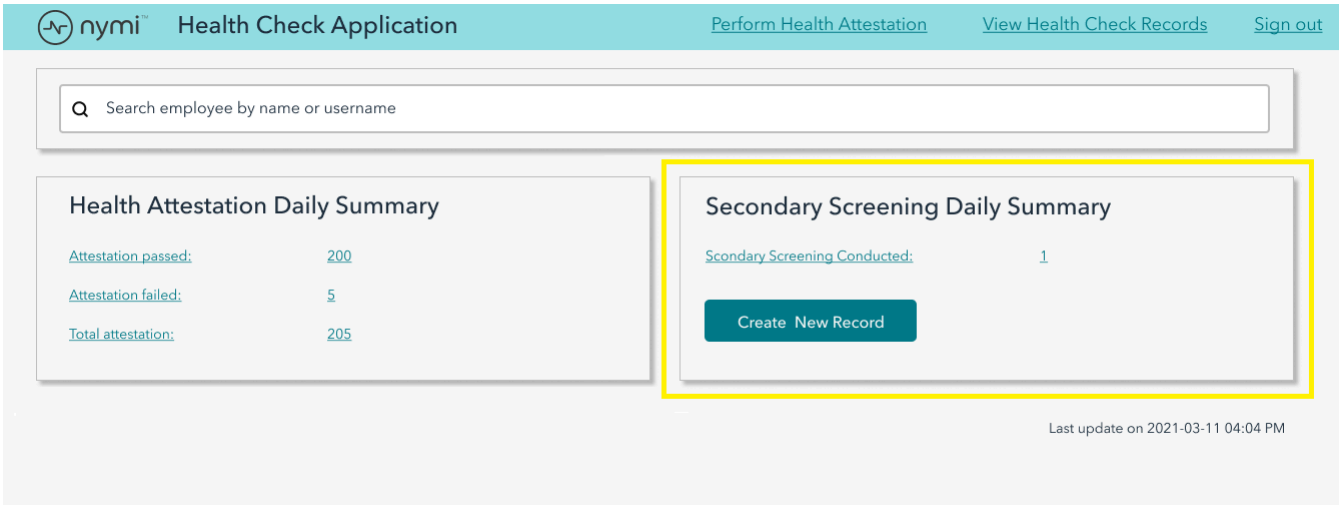
About this task

Perform the following steps to view the health attestation results for all employees on the current day.

Procedure

1. Log in to the `Health Check Application` as a user with administrator access.

   The `Health Check Application` main page appears with the health attestation daily summary results for the total number of employees that passed, failed, and completed a web-based attestation on the current day. The following figure provides an example of the `Health Check Application` main page with the `Secondary Screening Daily Summary` pane highlighted.



   `Figure 52: Secondary Screening Daily Summary`

2. To view a list of all employees that performed secondary screening, click the **`Secondary Screening Conducted`** label or value.

   Note: If an employee performs more than one attestation a day, only the results of most recent screening of the day appears in the results.

   The `Daily Summary` window appears with the results. The following figure provides an example of the results window.

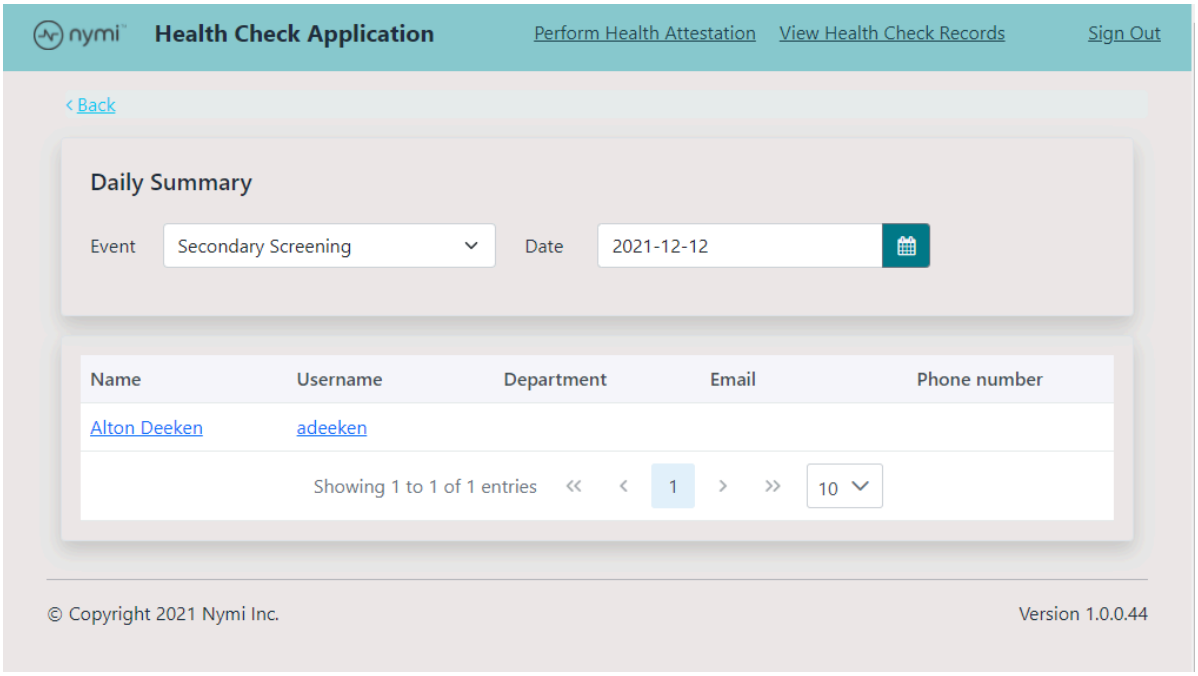


Figure 53: Secondary Screening Daily Summary window

3. To view secondary screening information for an employee, click the **Name** or **Username** label.

Viewing Secondary Screening Results for a User

The Health Check Application main page provides Health and Safety personnel with the ability to search for users to view and export information about their secondary screening results from the last 90 days.

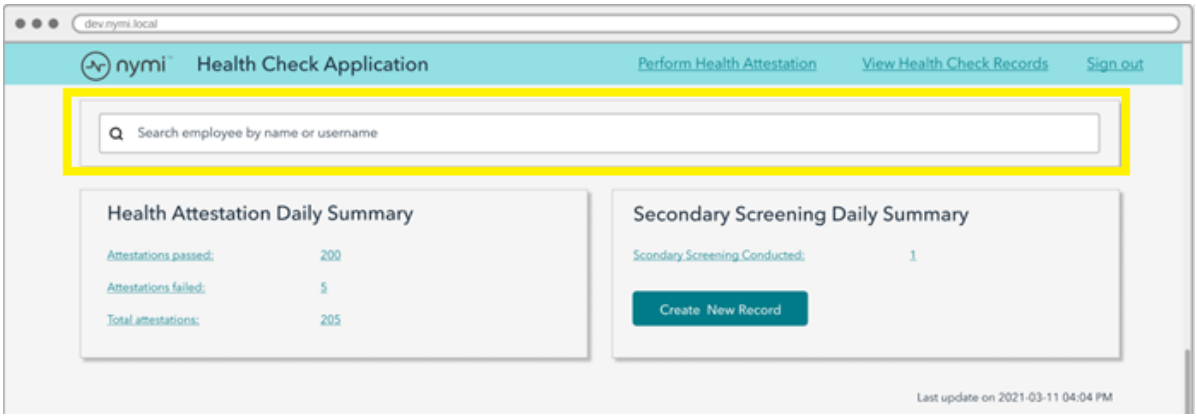
About this task

Perform the following steps to view the secondary screening results for an employee.

Procedure

1. Log in to the `Health Check Application` as a user with administrator access.

   The `Health Check Application` main page appears with the **`User Search`** field. The following figure provides an example of the `Health Check Application` main page with the `User Search` field highlighted.



`Figure 54: Health Check Application Main Page`

2. In the **`User Search`** field, type the first name, last name, or username of the employee.

   A search results list appears with user matches as you type characters, as shown in the following figure.

`Figure 55: Employee search field`

3. Select the appropriate user from the search results list.

   The `Employee Details` page appears and displays the `Employee Profile` pane, `Attestation Records` pane, `Secondary Screening Result` and `Secondary Screening Records` pane. The following figure provides an example of the `Employee Details` page.

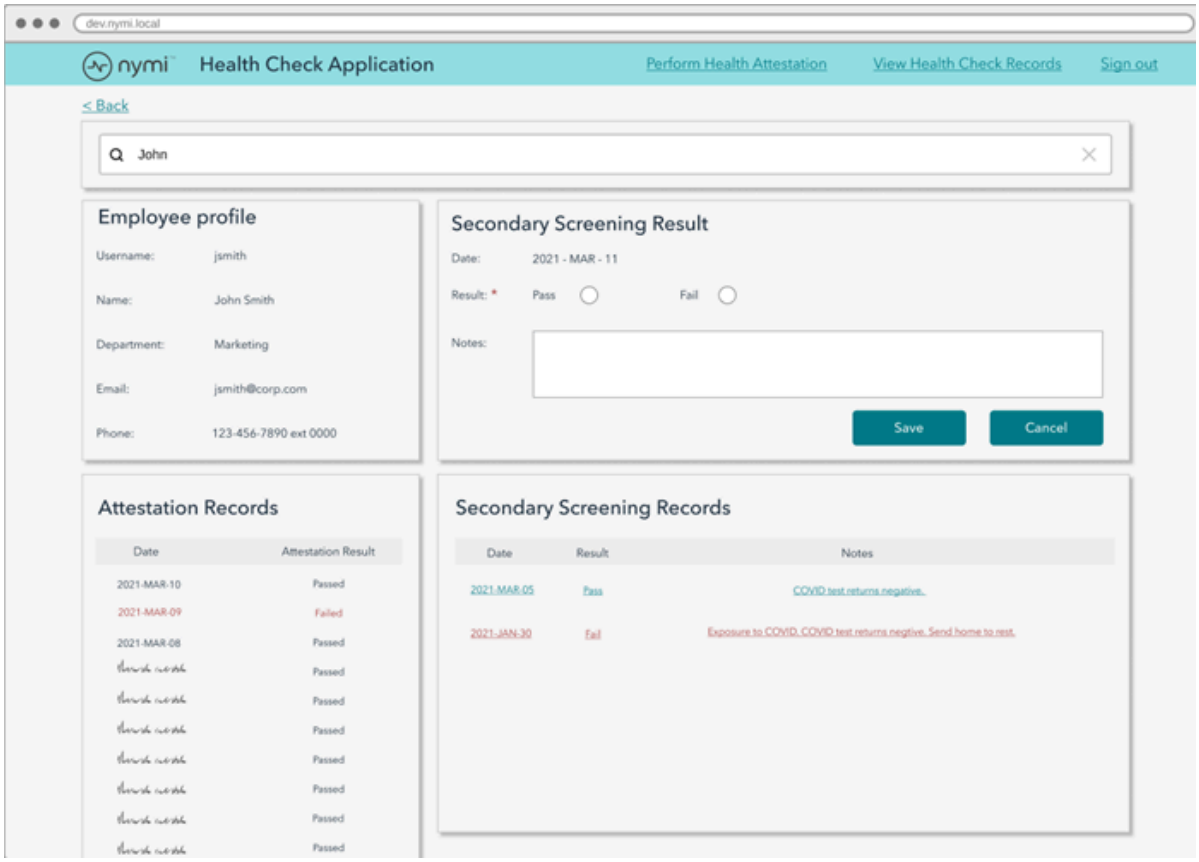


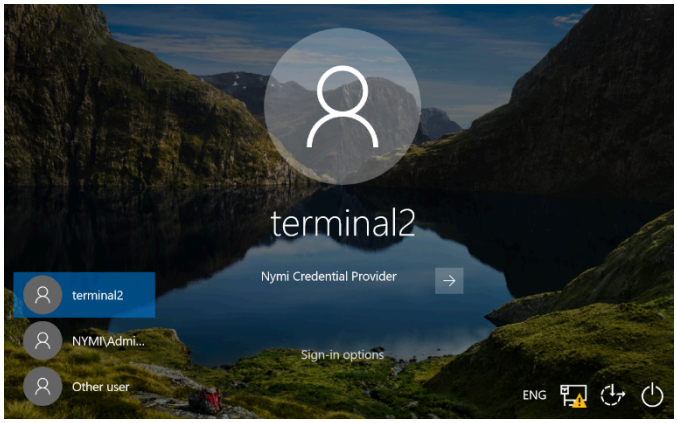
Figure 56: Employee Details page

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 57: User Terminal Log in Screen with Nymi Lock Control`

Initializing Nymi Lock Control

Perform the following while wearing an authenticated Nymi Band.

About this task

Procedure

1. Lock the desktop.
2. Press any key to display the Windows Login screen.
3. Click **`Other User`**.
4. Click **`Sign-in options`**.
5. Click the Nymi icon.
6. In the **`Username`** field, type your username.
7. Click **`Submit`**.

Confirming Nymi Lock Control Recognizes the Nymi Band

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

About this task

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

Procedure

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

   Note: `Nymi Lock Control` will NOT detect changes to a user's corporate credentials in the Nymi Band. If a user changes their corporate credentials or the password has expired while `Nymi Lock Control` is enabled, `Nymi Lock Control` will not unlock the terminal. To update the Nymi Band with the encrypted password, the user must first sign into the `Nymi Band Application` and re-authenticate their Nymi Band. Refer to Resetting an Expired Password on page 96 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.

About this task

Procedure

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

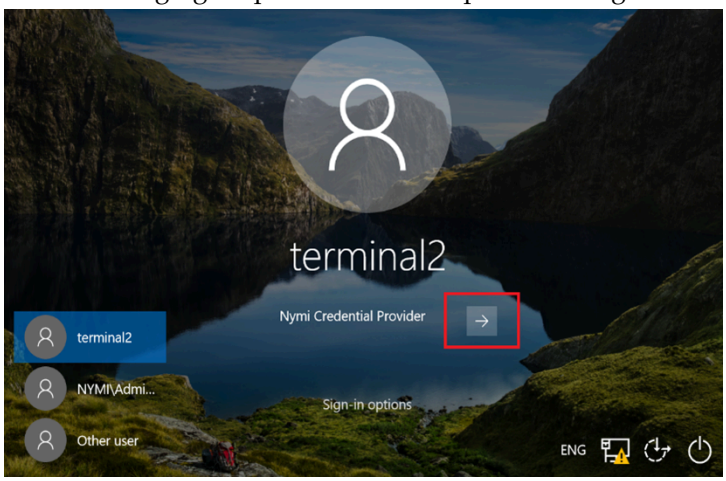
When `Nymi Lock Control` is installed on a terminal, the log in screen displays `Nymi Credential Provider` below the username of an enrolled user.

About this task

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

Procedure

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



`Figure 58: 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

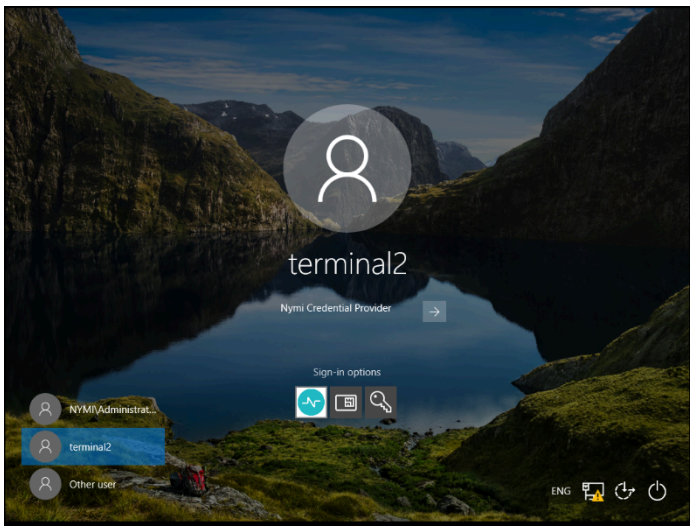
`Nymi Credential Provider` provides sign in options that allow users to log into the user terminal without an authenticated Nymi Band.

About this task

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

Procedure

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



`Figure 59: 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.

About this task

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

Procedure

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

Resetting an Expired Password

When a Nymi Band user uses Nymi Lock Control and the password for a user expires, when the user performs a tap to unlock the desktop, the unlock fails with the message Something went wrong.

About this task

After the user updates their password, before they can use Nymi Lock Control to unlock the desktop, they must log in to the Nymi Band Application on an enrollment terminal, which updates their password in NES.

Procedure

1. Perform the following steps on the user terminal:
   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.
2. If the user terminal does not have `Nymi Band Application`, log into the enrollment terminal.
3. Log into the `Nymi Band Application` with your new credentials while wearing your authenticated Nymi Band.

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 60: Deauthentication with Band Label enabled

Figure 61: 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

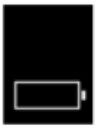
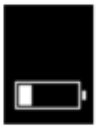
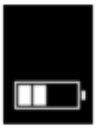
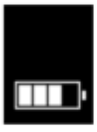
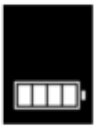
to 86°F). This will ensure the Nymi Band charges in a timely manner and will maintain the longevity of the battery.

Before you begin

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

Figure 62: 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%
				

About this task

To charge a Nymi Band, perform the following steps:

Procedure

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

appears on the side of the charging cradle to indicate that the user successfully connected the Nymi Band to the charging cradle and the Nymi Band is receiving power.

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

Figure 63: Charging battery indicator

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

Figure 64: 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 typical battery life of the Nymi Band depends on how the Nymi Band is used. The following table summarizes the usage scenarios, activities, and the typical battery life in each scenario.

Table 6: Typical Battery Life

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

Usage Scenario	Daily Activities	Typical Battery Life
Smart Distancing and Contact Tracing	120 smart distancing reminders (12 an hr over 10 hrs) About 25 unique users contacts within a day	20 active hours

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 section *Configuring Liveness Detection* in the section *Customizing the Nymi Band Authentication Method* for information about how to disable ECG liveness detection.

Figure 65: 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 66: Authentication Success Screen with Band Label

Figure 67: Authentication Success Screen without Band Label

Authentication Failures

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

Figure 68: Authentication Failure Screen with Retry message

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

- Fingerprint matching failure - when the authentication fails as a result of a fingerprint mismatch, the Nymi Band vibrates and displays the Retry message about 1 second after the user places their finger on the fingerprint sensor and bezel.
- Liveness failure - when the authentication fails due to the inability to detect a consistent ECG signal on the wrist, the Nymi Band vibrates and displays the Retry message about 13 seconds after the user places their finger on the fingerprint sensor and bezel.

Troubleshooting Fingerprint Mismatch Failures

If the fingerprint authentication fails, ensure the following:

- Fingerprint sensor is clean and dry.
    - If the fingerprint sensor is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.

    - If the fingerprint sensor is wet, dry completely with a lint-free towel, and then retry authentication.
- User does not press too hard or too softly on the fingerprint sensor.
- User's finger is clean and dry.
    - If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication
    - If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
    - If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication
- User places their finger on the centre of the sensor, touching the surrounding bezel.
- User keeps their finger still on the sensor and bezel during the authentication period.
- User does not lift their finger off the sensor or bezel until the authentication process completes.
- Ensure that the Nymi Band fits snugly on the wrist.

Troubleshooting Liveness Detection Failures

If the liveness detection fails, ensure the following:

- Bottom sensor is clean and dry.
    - If the bottom electrode is dirty, clean with a 70% isopropyl alcohol wipe, allow it to dry completely, and then retry authentication.
    - If the bottom electrode is wet, dry completely with a lint-free towel, and then retry authentication.
- User's finger is clean and dry.
    - If the finger is dirty, clean the hands and allow them to dry completely, and then retry authentication
    - If the finger is too dry, rub some lotion well into the finger, and then retry authentication.
    - If the finger is too wet, rub the finger with an alcohol wipe or with hand sanitizer, allow the finger to dry completely, and then retry authentication
- User keeps their finger still on the sensor and bezel during the authentication period.
- User's wrist is not too dry. Before authentication, wash and completely dry the wrist before putting on the Nymi Band, or rub some lotion well into the wrist, and then retry authentication.
- Nymi Band bottom electrode remains in contact with the wrist during the authentication period. If the position of bottom electrode prevents contact, remove the Nymi Band, reposition the Nymi Band on the wrist, and then try authentication again.
- User does not lift their finger off the sensor or bezel until the authentication process completes.
- Ensure that the Nymi Band fits snugly on the wrist and does not move around during the authentication process.

Note: The SQL database contains a record of the failed authentication attempt. The section *Collecting Data From a Nymi Band* provides more information.

Authentication Lockout

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

After 50 consecutive failures due to a fingerprint mismatch, the Nymi Band displays the See Admin icon and prevent the user from performing additional authentication attempts.

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

Clear the lockout by one of the following methods:

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

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.

About this task

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

Perform the following steps to restart the Nymi Band.

Procedure

1. Ask the user to remove the Nymi Band.
2. Plug the Nymi Band into a charger.

3. Press and hold the top button, the word **RESTART** and a countdown progress bar appears on the screen. Continue to hold the top button for 10 seconds to complete the countdown, and initiate the restart procedure. The following figure shows the **RESTART** message with countdown.

Figure 69: RESTART message

Results

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

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.

About this task

Procedure

1. Remove the Nymi Band from the wrist of the user.
2. Put the Nymi Band on the charger.
3. Press and release the top and bottom button.
   The firmware version appears on the screen, as shown in the following figure.

Figure 70: Nymi Band firmware version

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.

About this task

Searching for User or Nymi Bands Information

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

Searching for Nymi Band information is particular useful for:

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

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

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

Searching for Users

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

About this task

Procedure

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

   The Search page appears.
2. In the `Search` page, select the **`Users`** option.
3. In the **`Search`** field, type the full or partial criteria for the following:

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

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

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

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

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

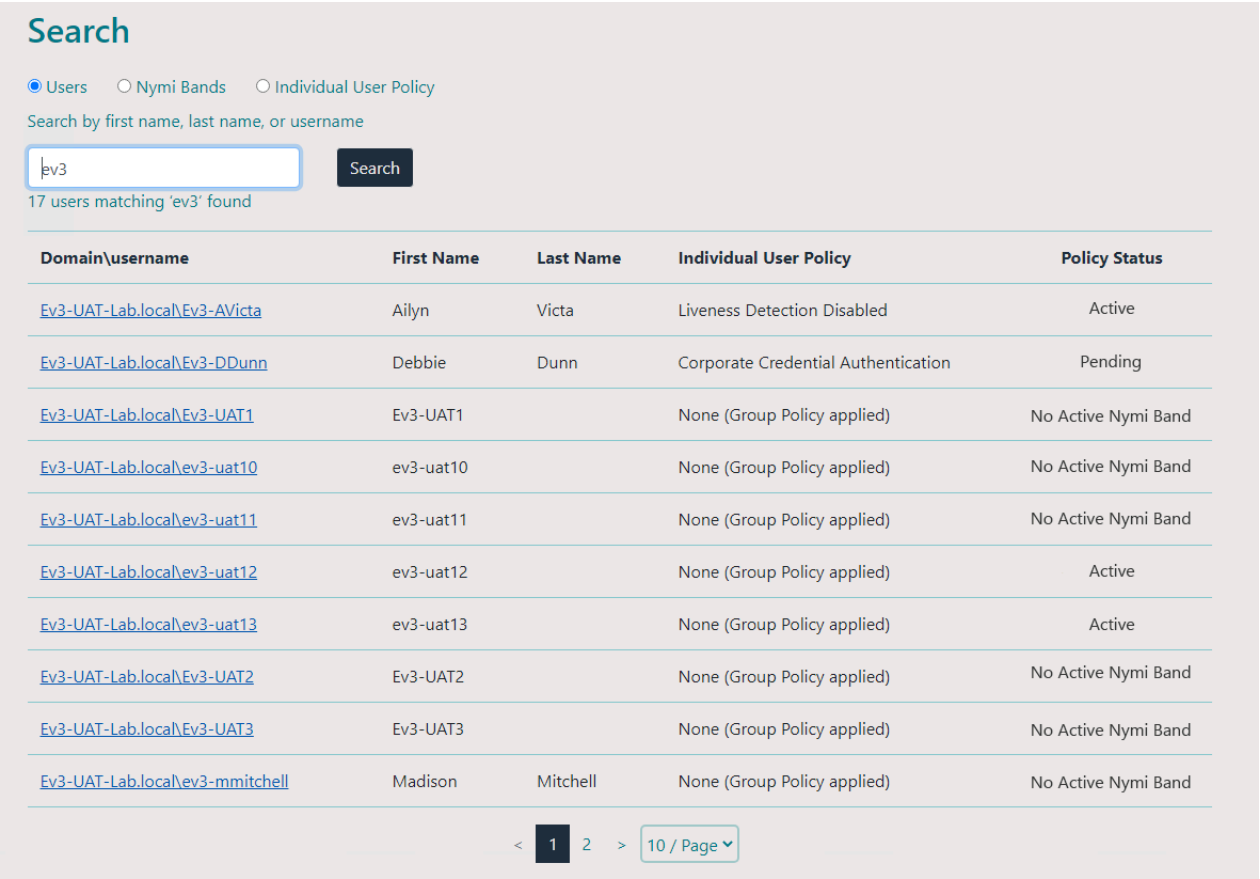


Figure 71: Users Search Results Page

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

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

User Details Page

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

The following figure provides an example of the User Details window.

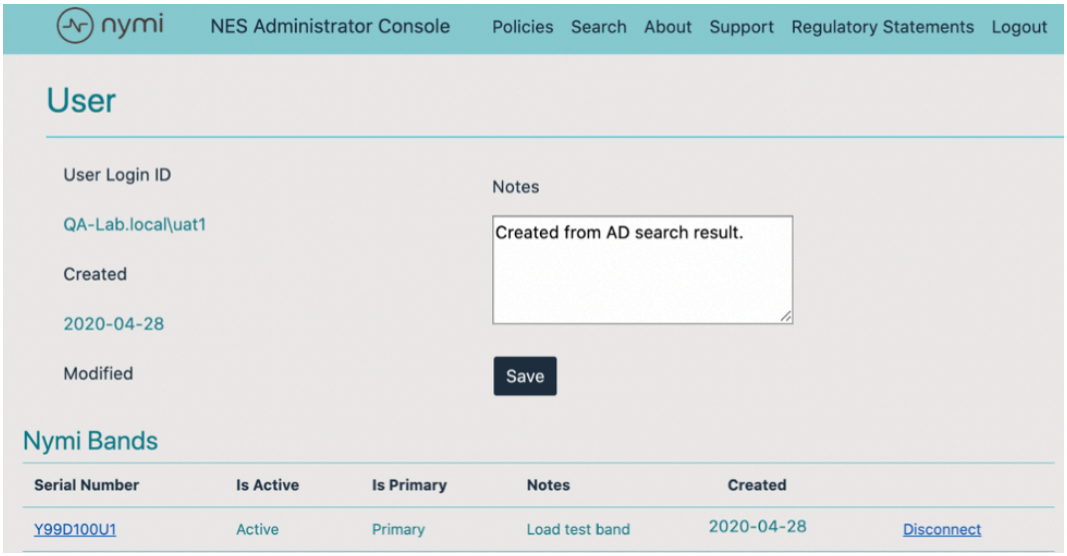


Figure 72: User Details Page

Table 7: 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 NES Administrators to search by a serial number for an enrolled Nymi Band.

About this task

Procedure

1. From the NES Administrator Console, select **Search**.
   The Search page appears.
2. In the Search page, select the **Nymi Bands** option.
3. In the **Search** field, type the serial number of the Nymi Band (located on the back of the Nymi Band).
4. Click **Search**.
   The following figure provides an example of the Search page when searching by the Nymi Band serial number.

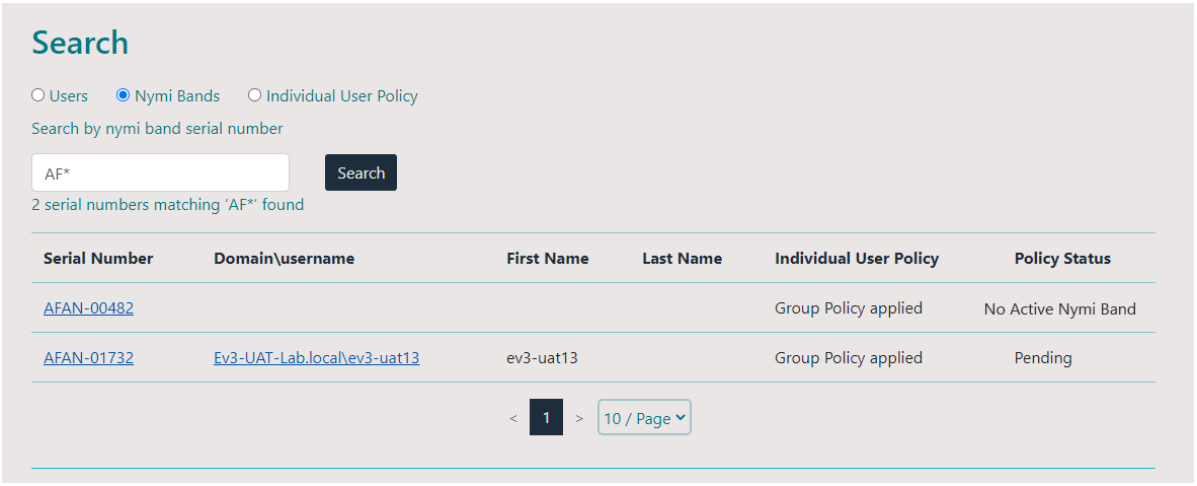


Figure 73: Nymi Band Search Results Page

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

5. Do one of the following:
   - In the returned search list, click the **Domain\username** link. The User Details page displays with the user's information.

- In the returned search list, click the `Serial Number` link. The `Nymi Band` details page displays with information about a Nymi Band.

Nymi Band Details Page

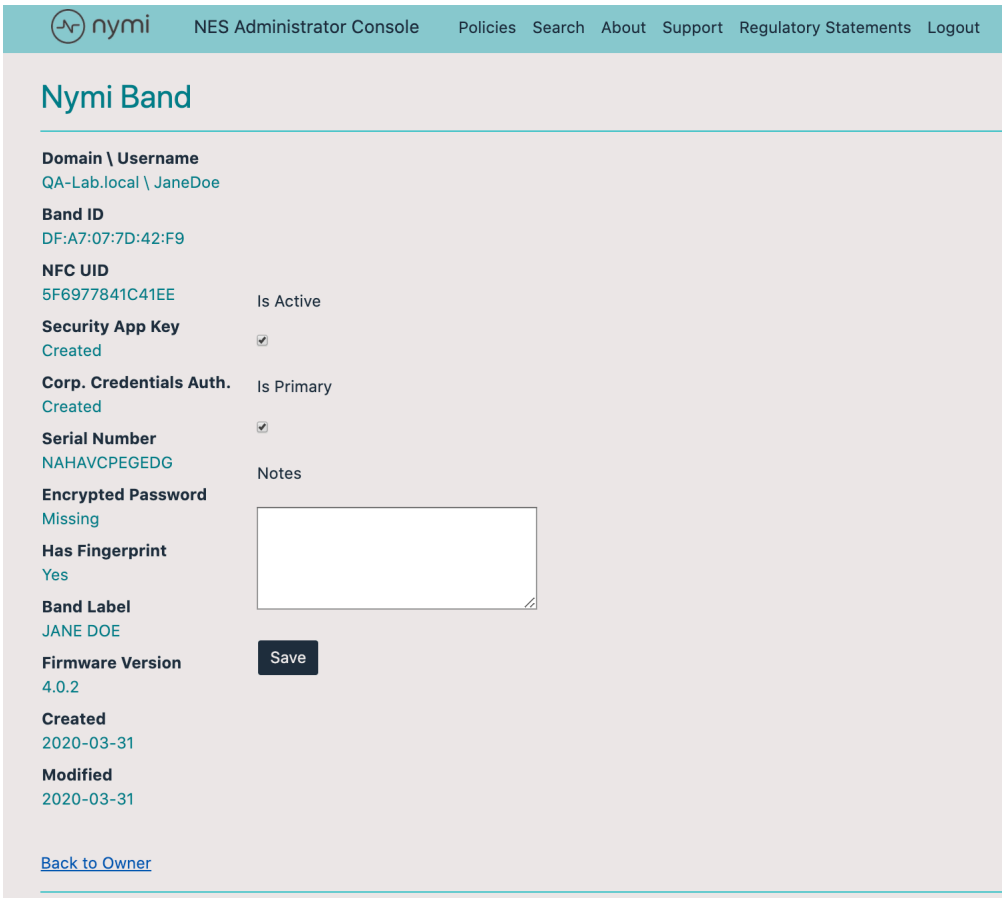
The `Nymi Band` details page displays information about a Nymi Band.

Table 8: Nymi Band Details Summary

Field	Description
Domain\Username	Provides the domain and username of the Nymi Band user. The domain is the AD server that stores this information about the user.
Band ID	Displays the MAC address number of the Nymi Band.
NFC UID	Displays the ID that is readable by Near Field Communication (NFC) technology when the Nymi Band is authenticated.
Security App Key	Displays the status of the symmetric key ID of the Nymi Band. • If the policy is configured to support the creation, ID is created the field displays, **`Created`** • If the ID is not created the field displays, **`Not Created`**
Corp Credentials Auth	Displays the status of the External Authenticator creation. • If a policy enables the use of External Authenticator, the field displays **`Created`** • If a policy is not configured to enable the use of an External Authenticator, the field displays **`Not Created`**
Serial Number	Displays the unique value that is located on the back of the Nymi Band.
Encrypted Password	Indicates if the user's password was encrypted and saved in NES database. • If the password was encrypted and saved, the field displays **`Stored`** • If the password was not encrypted and not saved, the field displays **`Missing`**
Has Fingerprint	Indicates if the user's fingerprint step was performed during enrollment. • If the fingerprint step was performed, the field displays **`Yes`** • If the fingerprint step was not performed, the field displays **`No`**
Band Label	Displays the Band Label assigned to the Nymi Band. Band Labels can only be assigned to Nymi Band 3.0, when the active policy is configured to support the option.

Field	Description
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.



`Figure 74: Nymi Band Details page`

Searching for Individual User Policy Membership

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

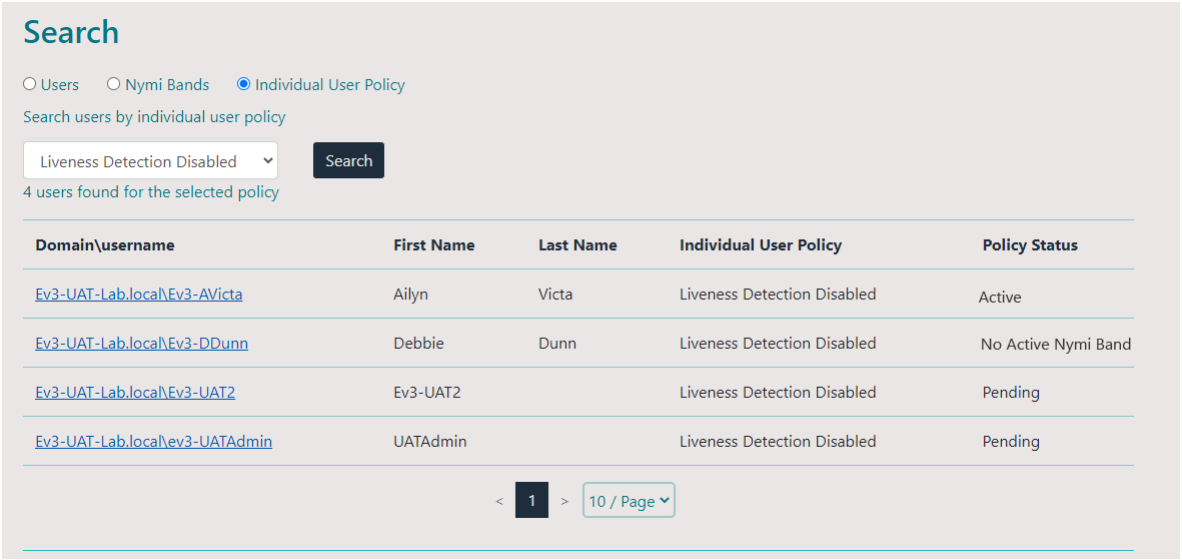
About this task

Procedure

1. From the NES Administrator Console, select **`Search`**.
   The Search page appears.
2. In the `Search` page, select the **`Individual User Policy`** option.
3. From the policy list, select the Individual User Policy, and then click **`Search`**.

Results

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



`Figure 75: Individual User Policy Search Results`

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

- No active Nymi Band - The user does not have an active Nymi Band.
- Pending - The policy on the Nymi Band does not match the policy (individual user policy or global policy) that is applied to the user. For example, the policy was applied to the user after enrollment,

and the user has not signed into the Nymi Band Application while wearing their authenticated Nymi Band to activate the policy changes.

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

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

Issuing a temporary Nymi Band to a user

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

About this task

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

Procedure

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.

About this task

Procedure

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.

About this task

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.

Procedure

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.

About this task

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

Procedure

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.

About this task

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

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

Procedure

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.

Procedure

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

Figure 76: 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 77: 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.

About this task

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.

Procedure

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**.

Re-enrolling a User

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

About this task

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

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.

Procedure

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**.

Storage of Data

Nymi stores information related to NES in a SQL database. The `Data Exchange ServiceDES`) collects information related to health attestation, temperature alerts, authentications activities, and contact tracing events. The information is stored in a separate database within the Kubernetes cluster.

The `Health Check Application` does not depend on access to the NES server or database.

The *CWP Database Sample Queries* document on the Nymi Support website provides more information about the database in the Kubernetes cluster, and how to query the database for information.

Storage of NES Data

Nymi stores information related to specific `Connected Worker Platform` 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.

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

Adding additional users or groups to view and query audit database

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

About this task

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

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

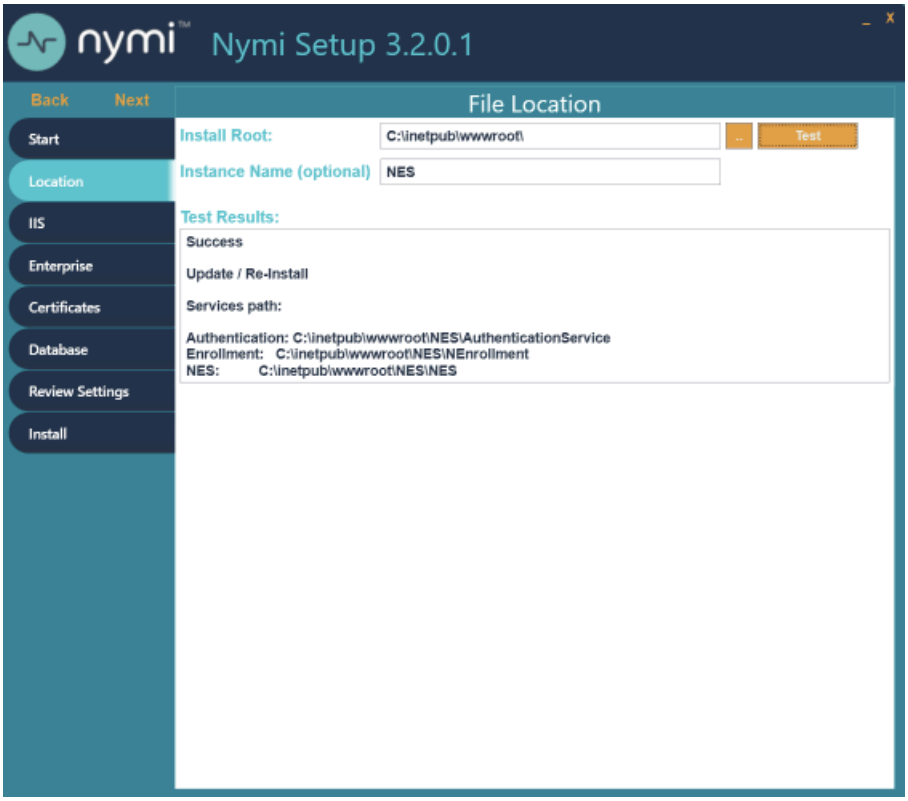
Procedure

1. Log in to the NES server with the account that performed the NES installation and configuration.
2. Navigate to the directory that contains the NES installation software.
3. From the directory that contains the extracted NES installation package, run ..*NesInstaller* *install.exe*.
4. On the `User Access Control` window, click **`Yes`**.
5. On the `Open File - Security warning` window, click **`Run`**.
6. If applicable, on the `User Access Control` page, review the Microsoft .NET EULA, and then click **`Accept`**. Complete the .NET installation and continue with the NES installation.
7. On the `Application Install Security Warning` window, click **`Install`**.

8. On the `Open File - Security warning` window, click **Run**.
9. On the left navigation pane, click **Location**, and then perform the following steps.
   a) In the **Install Root** field, confirm that the path to the NES services is correct, as it was specified during the initial deployment.

      The default location is *C:\inetpub\wwwroot*.
   b) In the **Instance Name** field, type the descriptive name that was specified during the initial deployment for the NES web application instance name. For example, NES. See Configuration Attribute Values in the Nymi Connected Worker Platform 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 78: Update / Reinstall installation type`

10. On the **Database** page, click right-click in the Users table and select **Add**.
    The `Database Credentials Editor` window appears.
11. From the **Login Type** list, select **Auditor**.
12. In the **Domain Account** field, type the domain and username (or group name) of the user in the format *domain_name\user_name*.
13. In the **Database User** field, type the name of the SQL user to associate with the user or group.

14. Click **OK**.
15. Click **Verify Users**.
    If the NES installer finds the user or group in active directory, the message `No errors found` appears in the status window. If an error appears, right-click on the user or group in the **Database** table, and select **Edit** to correct the credential information.
16. On the **Install** tab, click **Apply Settings**.
    The output displays `Creating Database Auditor Login is done`.

NES SQL Database Overview

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

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

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

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

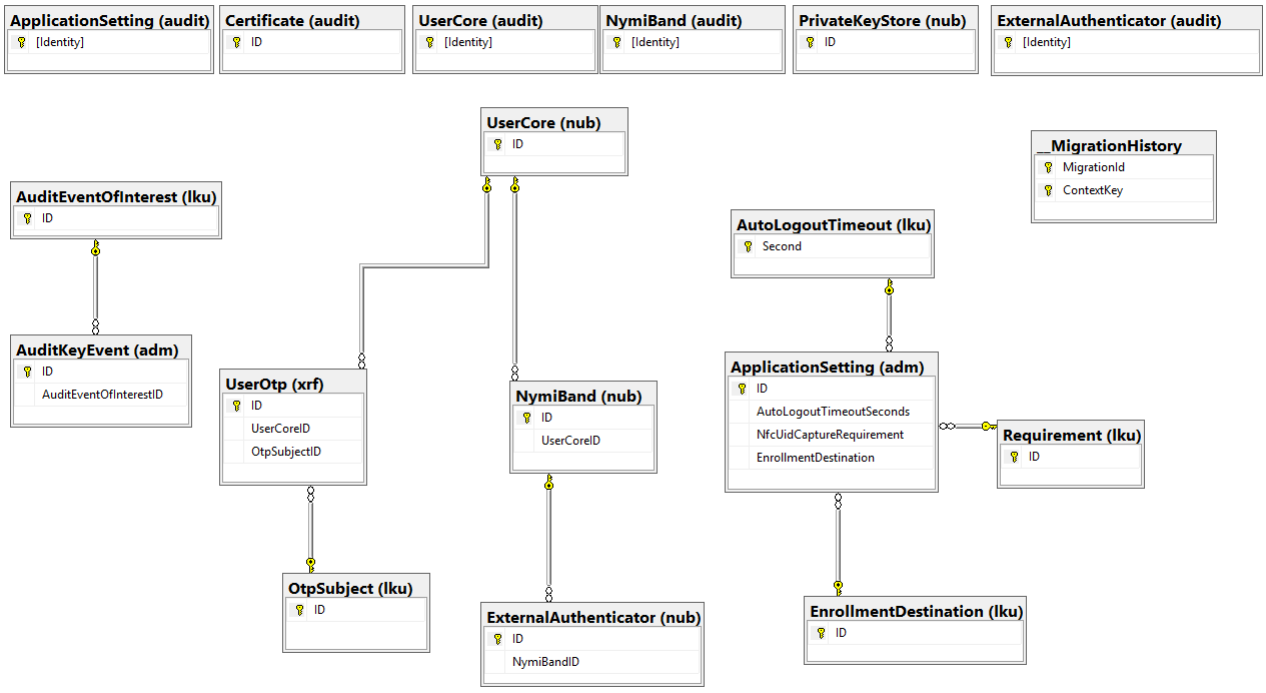


Figure 79: NES Database Structure

adm and nub Schemas

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

Table 9: adm and nub Schemas

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

dbo.__MigrationHistory

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

lku Schema

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

Table 10: lku schema

Table Name	Purpose
lku.AuditEventsOfInterest	Legacy option.
lku.EnrollmentDestination	Contains a list of acceptable values for the **`Enrollment Destintation`** setting.
lku.OtpSubject	Legacy option.

Table Name	Purpose
lku.Requirement	Contains a list of acceptable values for the **`NfcUIDCapture`** setting.
lku.AuditLogoutTimeout	Contains a list of acceptable values for the **`Auto Logout Timeout`** setting.

xrf.UserOtp Schema

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

audit Schemas

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

`audit.UserCore SQL Schema`

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

Table 11: audit.UserCore SQL Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.
EventType	Type of event, denoted by a single character. There are three event types: • C - when the user is enrolled or for an unenrolled user, the first time that an NES Administrator performs a search for the user in the `NES Administrator Console`. • U - when the properties of the user is updated.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	ID of the user in the audit.UserCore table.
Domain	Domain of the user.
Username	Login name of the user.

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

audit.NymiBand SQL Schema

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

Table 12: audit.NymiBand SQL Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.
EventType	Type of event, denoted by a single character. There are three event types: • C - when the Nymi Band is enrolled. • U - when the properties of the Nymi Band is updated. • D - when the Nymi Band to user association is deleted.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	ID of the Nymi Band in the audit.NymiBand table.

Column Name	Description
UserCoreId	ID of the user that is associated with the Nymi Band, as it appears in the audit.UserCore table. When an NES Administrator disassociates a Nymi Band from a user in the `NES Administrator Console`, the UserCoreId value is as NULL for the associated Update and Delete Event Type entries in the table.
NymiBandID	MAC address of the Nymi Band.
NfcUID	NFC address of the Nymi Band.
AuthorisationID	N/A. The value appears as NULL.
HardwareID	Nymi Band serial number.
SymmetricKeyID	SymmetricKey ID that was created on the Nymi Band. Values that can appear: • An encrypted key sequence when **`Corporate Credentials Authenticator`** is enabled in the policy or the **`Enrollment Destination`** is set to **`NES and Evidian`**. • NULL when in the policy the **`Corporate Credentials Authenticator`** is not enabled and the **`Enrollment Destination`** value is **`NES only`** at the time of enrollment.
EncryptionIV	Encryption Initialization Vector that is used to support encrypting the password for a user. A value appears in this field when the `Nymi Lock Control` option is enabled in the default policy at the time that the Nymi Band is enrolled.
EncryptedPassword	Encrypted password for a user. A value appears in this field when the `Nymi Lock Control` option is enabled in the default policy at the time that the Nymi Band is enrolled.
IsActive	Status of the Nymi Band as set in the NES Administrator Console. Values that can appear: • 0 when the Nymi Band inactive. • 1 when the Nymi Band is active.
IsPrimary	Status of the Nymi Band as set in the NES Administrator Console. Values that can appear: • 0 when the Nymi Band not the primary Nymi Band. • 1 when the Nymi Band is primary.
HasFingerprint	Status of the fingerprint enrollment for the Nymi Band. Values that can appear: • 0 when a fingerprint enrollment has completed. • 1 when a fingerprint enrollment has not been completed.
EnrollmentStatus	N/A. The value appears as NULL.

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

audit.ApplicationsSetting SQL Schema

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

Table 13: audit.ApplicationsSetting SQL Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.
EventType	Type of event, denoted by a single character. There are three event types: • C - when a new policy is created or change to an existing policy is created. • U - when a setting in a policy is modified. • D - when a policy is deleted.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.

Column Name	Description
ID	The database ID of application settings on audit.ApplicationSettings table.
IsActive	Status of the policy as set in the NES Administrator Console. Values that can appear: • 0 when the policy is not the active policy. • 1 when the policy is the active policy.
Description	Name of the policy that contains the setting.
AutoLogoutTimeoutSeconds	Length of time after which the Nymi Band Application and the NES Administrator Console automatically disconnects an idle user.
NfcUIDCaptureRequirement	Status of the requirement to capture the NFC UID of the Nymi Band during enrollment. The value is always M (Mandatory).
FingerprintRequirement	Legacy option that defines the status of the requirement to capture the fingerprint of the user during enrollment. The value is always M (Mandatory).
PassworthAuthOption	Status of the option to allow authentication by corporate credentials. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
FingerprintOption	Legacy option that defines the status of the fingerprint capture option. The value is always 1 (enabled).
LockControlSupportOption	Status of the option to allow Nymi Lock Control. Values that can appear: • 0 - when the setting is disabled. • 1 - when the setting is enabled.
DoorSecurityOption	N/A
AdCheckUserStatus	Status of the Check User Status setting. Values that can appear: • 0 - when the setting is disabled. • 1 - when the setting is enabled.
AdCacheUserStatus	Status of the **`Cache User Status`** setting. Values that can appear: • 0 - when the setting is disabled. • 1 - when the setting is enabled.
AdCacheExpiryTimeSeconds	Expiry time of user status cache in seconds. When the **`Cache User Status`** setting is disabled, NULL appears.
ManualOtpOption	Legacy option.
ManualNeaOtpOption	Legacy option.

Column Name	Description
LockWhenAway	Status of the **`Lock When Away`** setting for Nymi Lock Control. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
MonitorProximity	Legacy option.
KeepUnlockedWhenPresent	Status of the **`Keep Unlocked When Present`** setting for Nymi Lock Control. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
CheckProximityForUnlock	Legacy option.
LockProximitySphera	Proximity distance for `Nymi Lock Control` that is defined in the adm.ApplicationSettings table. Nymi recommends that you leave the default value of 3.
UnlockProximitySphera	Proximity distance for `Nymi Lock Control` that is defined in the adm.ApplicationSettings table. Nymi recommends that you leave the default value of 2.
ProximityLockCountdown	Starting time for the countdown timer in seconds, that `Nymi Lock Control` displays to the user when the Nymi Band moves out of close proximity to the BLE adapter.
BandLabelOnBandEnabled	Status of the **`Display Band Label on Nymi Bands`** setting. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
BandLabelOnBandCustomizationEnabled	Status of the **`Allow Band Label Customization`** setting. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
CreatedAt	Date and time that the object entry was created in the table.
ModifiedAt	Date and time when the object entry was modified in the table.
ModifiedBy	User who modified the object entry in the table.
EnrollmentDestination	Status of the **`Enrollment Destination`** setting. Values that can appear: • 1 when enrollment data is sent to NES only. • 2 when enrollment data is sent to NES and Evidian.

Column Name	Description
SDCTEnabled	Status of the **Smart Distancing and Contact Tracing** setting. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
SDRemindersEnabled	Status of the **Smart Distancing Reminders** setting. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.
UnlockWhenPresent	Status of the **Unlock When Present** setting for Nymi Lock Control. Values that can appear: • 0 when the setting is disabled. • 1 when the setting is enabled.

audit.ExternalAuthenticator SQL Schema

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

Table 14: audit.ExternalAuthenticator SQL Schema

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

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

`audit.Certificate SQL Schema`

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

Table 15: audit.Certificate SQL Schema

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

Viewing and Querying Audit Schema

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

About this task

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

Procedure

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

`Tracing changes in the audit tables`

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

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

Performing More Complex Queries of the Audit Tables

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

Overview of SQL queries

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

1. Define a SELECT statement then list the subsequent table columns data values that the query retrieves.

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

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

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

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

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

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

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

```
SELECT TOP (1000)
nb.[Identity]
,nb.[EventTime]
,nb.[EventType]
,nb.[SystemUser]
,nb.[ID]
,nb.[UserCoreID]
,nb.[NymiBandID]
,nb.[NfcUID]
,nb.[IsActive]
,nb.[IsPrimary]
,nb.[HasFingerprint]
,nb.[EnrollmentStatus]
,nb.[MiscNote]
,nb.[CreatedAt]
,uc.Domain
,uc.Username
FROM [Nymi.NES].[audit].[NymiBand] AS nb
JOIN [Nymi.NES].[audit].[UserCore] AS uc
ON nb.UserCoreID = uc.ID
WHERE nb.EventType = 'C'
```

In this query the:

a. SELECT statement returns the first 1000 rows and the subsequent table columns define the table columns data values that the query retrieves.
b. FROM clause defines [Nymi.NES].[audit].[NymiBand] as the primary table from which to retrieve the column data values, and shortens the table name to nb.

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

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

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

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

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

Log Files

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

Configuring Contact Tracing Logging

The *.prod-env* contains variables that allow you to adjust the logging levels for CWP components, the location of the logs files, and the name of the log files in a Kubernetes cluster.

To troubleshoot deployment issues, it might be necessary to modify the level at which CWP components log information. Each variable supports the following log level values:

- info
- warn
- error
- debug

Table 16: Configuration Parameters for Logging

Environment Variable	Description
KAFKA_LOG_LEVEL	Specifies the default logging level for Kafka. The default value is `info`.
CT_LOG_LEVEL	Specifies the CT Processor default log level. The default value is `info`.
CT_HTTP_LOG_LEVEL	Specifies the CT Processor HTTP client log level. The default value is `debug`.

Environment Variable	Description
CT_KAFKA_LOG_LEVEL	Specifies the CT Processor kafka log level. The default value is `info` .
CT_KAFKA_CLIENT_LOG_LEVEL	Specifies the CT Processor kafka client log level.The default value is `debug` .
CT_KAFKA_STREAM_LOG_LEVEL	Specifies the CT Processor kafka stream log level.The default value is `info` .
CT_KAFKA_CONSUMER_LOG_LEVEL	Specifies the CT Processor kafka consumer log level. The default value is `info` .
CT_CONSUMER_LOG_LEVEL	Specifies the CT consumer log level. The default value is `debug` .
CT_STREAMER_LOG_LEVEL	Specifies the CT streamer log level. The default value is `debug` .
CT_LOG_FOLDER	Specifies the location of the CT Processor log folder. Nymi recommends that you do not change the default value `logs` .

Environment Variable	Description
CT_LOG_FILE	Specifies the name of the CT Processor log file that is stored in the*CT_LOG_FOLDER*. The default filename is =CTlog .
CT_CONSUMER_LOG_FILE	Specifies the name of the CT Processor consumer log file that is stored in the *CT_LOG_FOLDER*. The default filename is consumer .
CT_STREAMER_LOG_FILE	Specifies the name of the CT Processor streamer log file that is stored in *CT_LOG_FOLDER*. The default filename is =streamer .

Enrollment Terminal 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.

About this task

Procedure

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

Viewing Nymi Band Application log files

Perform the following actions to view the log files.

About this task

Procedure

1. In the Nymi Band Application, from the navigation bar, select **`Logs > Explore Logs`**.

   Windows Explorer opens and displays the content of the log files folder. The default path to the log files is *C:\users\username\AppData\Roaming\Nymi\NEM\Logs*.
2. Double-click the log file to open the contents in the default text editor. The Nymi Band Application logs information in two files:

   - *nem.log*—Contains information about the Nymi Band Application.
   - *nymi_api.log*—Contains information about the Nymi SDK.

User Terminal Log Files

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

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

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

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

Nymi Lock Control Log Files

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

Security log

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

Collecting log files and contacting support

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

1. Right-click the `Nymi Lock Control` icon on the system tray and select **`Contact Nymi Support`**.
2. On the `Include Logs?` window, click **`Yes`**.
3. On the `Submit a Request` page, in the drop-down, select **`Nymi Customer - Technical Support`**.
4. On the next page, fill in the appropriate details, and in the **`Attachments`** section, click **`Add file`**.

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

Nymi Edge Agent Log Files

The location and log files generated for `Nymi Edge Agent` differ in a local and remote configuration.

When you install `Nymi Edge Agent` locally on a user terminal, the *edge_agents.log file* appears in the *C:\Nymi\Edge_Agents\Logs* directory.

When you install the `Nymi Edge Agent` on an RDP or Citrix sessions host, the following log files are created:

- *C:\Nymi\Edge_Agents\Logs\edge_agents.log* file - Stores information about the `Nymi Edge Agent` service.
- *C:\Nymi\Edge_Agents\Logs\edge_agents`IPAv4ddress`.log* file - Stores information about the `Nymi Edge Agent` process that is started for a user session, where`IPAv4ddress` is the IP address of the host that connects to the RDP/Citrix session host. Each user session will have a separate log file.
- *%appdata%\Nymi\Edge_Agents\Logs\EdgeAgentsLauncher.log* - Stores information about the EdgeAgentsLauncher process that is started for a user session.

  Note: %appdata%

  applies to the *AppData\Roaming* directory of the user that starts the session.

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 Verbose Logging

By default, Nymi Enterprise Server (NES) logs information level messages to the log files. When you encounter an issue, Nymi Support might request that you enable verbose mode for each web service, retry the operation, and then review the messages that appear in each log file. NES has a feature that writes previously encountered error messages to log files when you increase the logging level, so it is not necessary to leave NES in debug mode after troubleshooting completes. Logging levels include Critical, Error, Warning, Information, and Verbose.

About this task

To enable verbose logging mode, perform the following steps:

Procedure

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*

Nymi Support Tool

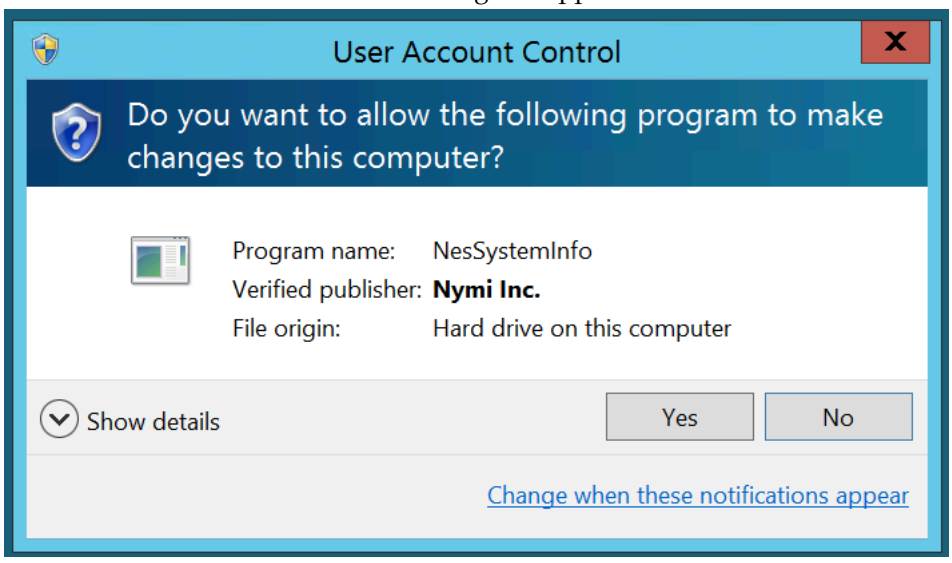
The Nymi Support Tool enables you to collect log information and generate a zip file that Nymi can review for troubleshooting purposes. The following logs and information is collected: NES Installation log files, Windows event logs, NES log files and NES instance configuration files.

About this task

Follow these steps to generate a log zip file.

Procedure

1. On 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 80: 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.

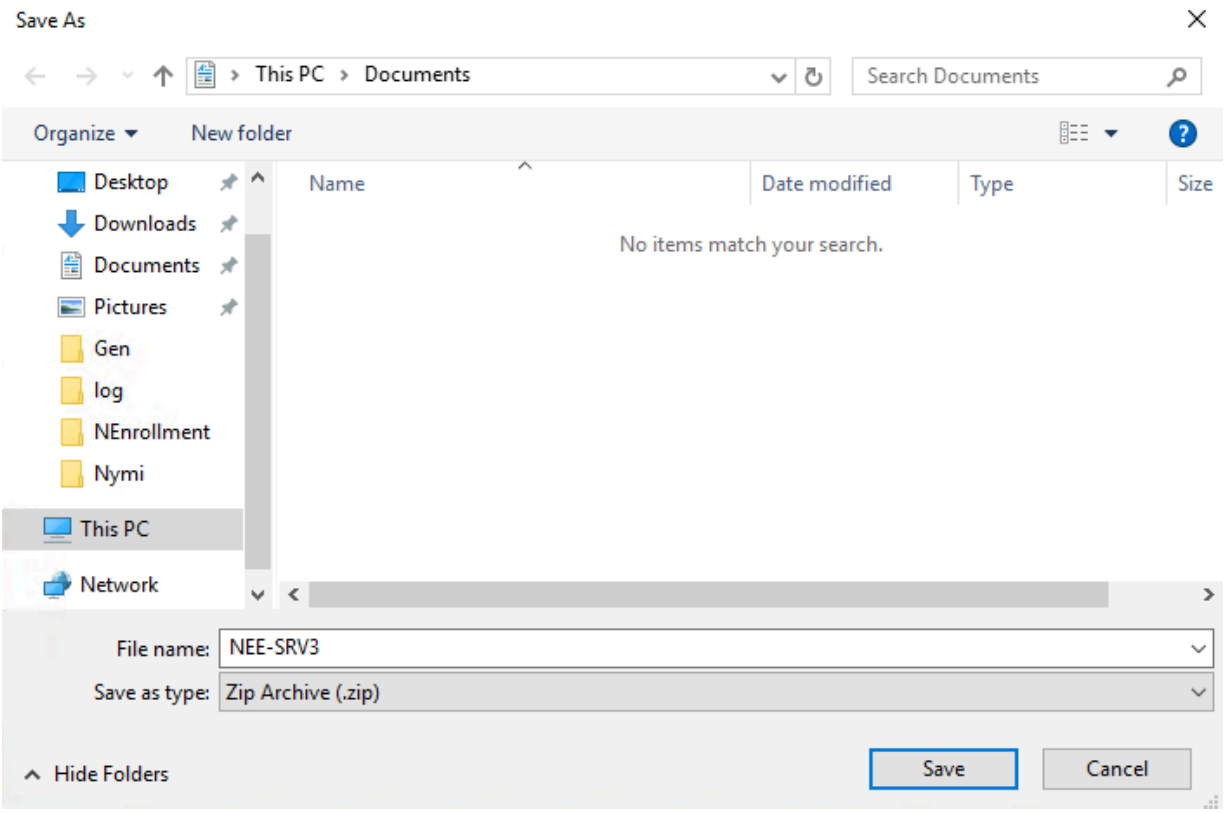


Figure 81: Saving Nymi Support Tool zip

Firmware log files

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

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

Firmware log retrieval

About this task

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

Procedure

1. Place the Nymi Band on the charger and move the Nymi Band and charger close to the BLE radio antenna on the terminal (BLED112 adapter). This will ensure the logs are retrieved from the correct Nymi Band.
2. Download and extract the firmware package into a directory of your choice on a Windows computer. For example, *C:\Nymi_firmware*.

3. If the Windows machine has the Nymi Band Application installed on it, stop the `Nymi Bluetooth Endpoint` service.
4. Navigate to the *C:\nymi_firmware\build\exe.win32-2.7* directory.
5. Run the `nsp_logs_download.exe`. A command prompt window opens with the status of the log file download. When the download completes, the command window closes and the firmware log file is saved to the folder that contains the `nsp_logs_download.exe` file.

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

Submitting a support request

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

About this task

Procedure

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

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

Manage the Connected Worker Platform Environment

This section provides you with information about how to maintain and mange 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.

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

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.

About this task

Procedure

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

Adding and Removing NES Administrator Access

Access to the NES Administrator Console as an NES Administrator is defined through the addition and removal of user accounts in the Windows group that you specified during the configuration of the NES server.

Before you begin

To determine the Windows group that was defined during the NES deployment, edit the *C:\inetpub\wwwroot\nes_\NES\web.config* file and search for the *string name="AdminGroup"*. The value that appears between the value tags immediately after the string name is the Windows group name. Alternatively, log into the NES Administrator Console as an NES Administrator, click **About**, and then click **View Full System Diagnostics**, a list of the NES Administrator groups appear in the **Local Domain** section.

About this task

Perform the following steps to add or remove NES Administrator for a user.

Procedure

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

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.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing `https://nes_server/NES_service_name` or `http://nes_server/NES_service_name`

   depending on the NES configuration, where:

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

     For example, `https://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.

What to do next

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 17: NES Application Details

Service	Description
Version	Version of the NES Application.
Branch	The branch from which the build was created.
Application Name	The service names of the NES web application.
Physical Path	The physical path of the NES application

Table 18: Local Domain

This section of the system diagnostics page describes the domain where NES is running.

Service	Description
Name	The name of the local domain of the NES application.
Service Account	The name of the domain service account.
Short Name	The short name of the local domain.
Domain trust	Tests if the machine has a trusted relationship with the domain controller. Provides a Pass or Fail status indicator. A failed status requires domain trust to be reestablished between the machine and domain controller.

Table 19: Configured Domains

This section of the system diagnostics page describes domains that are configured in the NEnrollment web configuration file.

Service	Description
Name	The name of the domain account in the configuration file.
Short Name	The short name of the domain account in the configuration file.
FQDN	The fully qualified domain name under which the service is running configured in the configuration file.
NetBios Name	The NetBios name of the domain in the configuration file.
Trust	Tests if the NES machine has a trusted relationship with the domain controller. Provides a Pass or Fail status indicator. A failed status requires domain trust to be reestablished between the NES machine and domain controller.

Table 20: Authentication Service

This section of the system diagnostics page describes the status of the NES Authentication Service.

Service	Description
Service is Up and Running	Provides a link to system Authentication Service information page. Provides a Pass or Fail indicator.

Service	Description
Negotiate Authentication	Provides a Pass or Fail indicator.
NTLM Authentication	Provides a Pass or Fail indicator.
Secured Communication	Provides a Pass or Fail indicator.

Table 21: Directory and Policy Service

This section of the system diagnostics page describes the status of directory and policy services.

Service	Description
Service is Up and Running	Provides a link to NES Administrator Console page. Provides a Pass or Fail indicator.
Negotiate Authentication	Provides a Pass or Fail indicator.
NTLM Authentication	Provides a Pass or Fail indicator.
Secured Communication	Provides a Pass or Fail indicator.
TLS Certificate	Provides a Pass or Fail for the validity of the TLS certificate. Provides the expiry date (m,d,y) of the TLS certificate within three months of the expiration date.

Table 22: Enrollment Service

This section of the system diagnostics page describes the status of the Enrollment Service.

Service	Description
Service is Up and Running	Provides a link to NES Enrollment Service page. Provides a Pass or Fail indicator. Configure the Enrollment Service using the Policy option from the main menu.
Negotiate Authentication	Provides a Pass or Fail.
NTLM Authentication	Provides a Pass or Fail.
Enrollment Service Loop	Provides a Pass or Fail.
Secured Communication	Provides a Pass or Fail.
L2 Private Key	Tests the certificate creation. Indicates a Pass or Fail.
Certificate Issuer	Indicates if the certificate was issues by the Nymi Token Server.
L2 Cert Validity	Indicates if the certificate is valid. Provides the expiry date (m,d,y) of the NES L2 certificate.

Table 23: Database

Service	Description
AE State	Provides information about the always encrypted state of the SQL database.
Database Name	Provides the name of the NES database.

Service	Description
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 token 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 token renewal is not possible and results in service disruption.

About this task

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

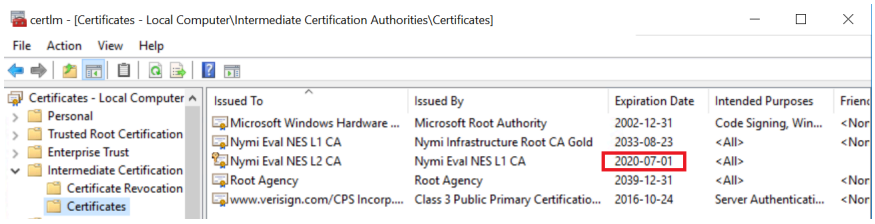
Note: The `NES Administrator Console` reports the L2 expiration date 3 months before the expiry date, as described in the next section.

Procedure

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 82: 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 83: NES Administrator Console Enrollment Service

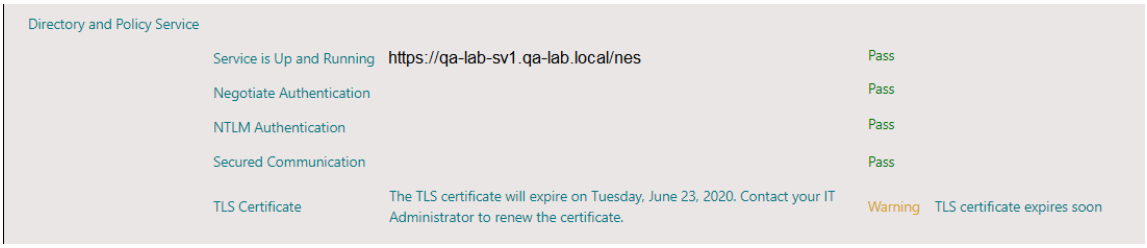


Figure 84: NES Administrator Console Directory and Policy Service

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.

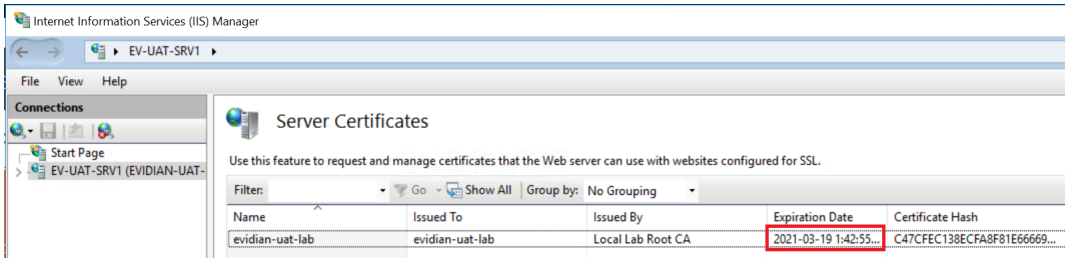
About this task

Perform the following steps to determine the TLS expiration date.

Procedure

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.

About this task

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.

About this task

Procedure

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.

About this task

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.

About this task

Procedure

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`**.

Managing Private Keys

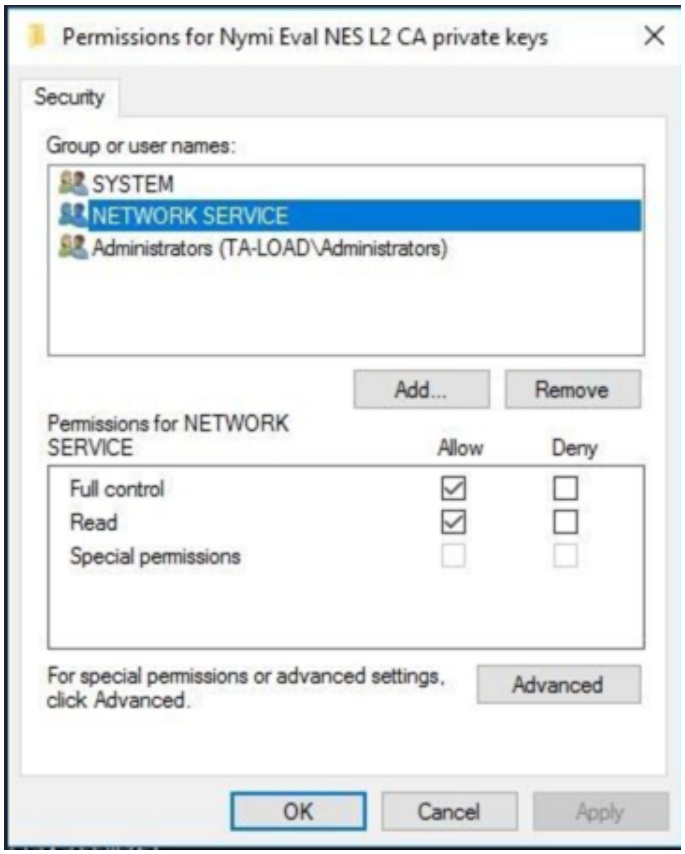
If the account used for the NES Application Pool is not LocalSystem, perform the following procedure to grant NES access to the L2 private key.

About this task

Procedure

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 85: 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.

About this task

Procedure

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.

About this task

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.

Backup and Restore the Kubernetes Environment

You can use Velero (Apache 2 License) to backup and restore the whole cluster for disaster recovery purposes in a self-managed or managed Kubernetes cluster.

About this task

Note: Currently the installation script for Velero supports backups to an AWS S3 bucket. The installer requires full IAM and S3 privileges, with the ability to install and edit user policies, and create new users.

Procedure

1. Peform the following steps to install the AWS CLI.
   a) Create an AWS API access key for your AWS account, if an AWS API access key does not already exist..
   b) Open a **`bash`** terminal.

c) Change to the */CWP_12_deployment_folder/deploy/kube/init/aws/client* directory

Note: This directory may be under either the *cwp* or *cwpall* folder.

d) Type the `./install-aws-cli` script, and then provide the API access key and ID when prompted.

2. Perform the following steps to install Velero.

a) Change to the *CWP_12_deployment_folder/deploy/kube/init* directory.

b) Type `./install-velero -b <S3-Bucket-Name> [-h [n] | -d [n]] [-I <awsaccess-key-id>] [-k <aws-access-key>] [-u <velero user>]`

Where:

- *--s3-bucket* or *-b*: name of the S3 bucket to store backups. Default name is `cwp-backup`.
- *--aws-region* or *-r*: name of the AWS region. Default region is *us-east-2*.
- *--hourly* or *-h*: backup every *n* hours. This option cannot be used with *-daily* or *-d* option.
- *--daily* or *-d*: backup every *n* days. This option cannot be used with *-hourly* or *-h* option.
- *--user* or *-u*: AWS user account. Default is `velero`. A new Velero user is created if a Velero user does not already exist.
- *--access-key-id* or *-i*: AWS access key ID associated with the Velero backup account. The script will create one if none is specified. An account can only have 2 access keys at any time.
- *--access-key* or *-k*: AWS access key associated with the Velero backup account (with access-key-id specified above). The script will create one if none is specified.

The script creates the S3 bucket,the AWS user account, installs Velero CLI on the user computer, and installs Velero Snapshot Controller in the Kubernetes cluster. This script will also schedule a backup every "n" hours or days.

For example:

- To install Velero with an S3 bucket called BUCKETNAME for a user without an AWS account (no access key ID and no access key), and no Velero account, with backup every 12 hours, type: `./install-velero -b BUCKETNAME -h 12`
- To install Velero with an S3 bucket called BUCKETNAME for a user with a known access key ID, and a known access key. There will also be a Velero account, and backup every 2 days. `./install-velero --s3-bucket BUCKETNAME --daily 2 -i <AWS ACCESS KEY ID> -k <AWS ACCESS KEY> --user <VELERO USER>`

3. (Optional) To review the backups, type `velero get backups`.

Backups of the Kubernetes cluster are stored in the S3 bucket name specified in the above steps. They contain timestamps that you can use to identify potential restore points for the cluster.

Restoring Kubernetes from a Backup

Use Velro to Restore a Kubernetes cluster from a backup to the same cluster or to a new one, after or disaster or after a change. Ensure that Velero and git is installed on the machine.

About this task

Procedure

1. Open a **bash** terminal.
2. To check the backups for the restore name and timestamp, type `velero get backups`.
3. To restore the backup, type `--velero restore create <RESTORE NAME> --from-backup <S3 BUCKET NAME>-backup-<TIMESTAMP>`

   Where,

   `S3 BUCKET NAME` is the name of the bucket. Obtained when creating a bucket during the installation of Velero.

   `RESTORE NAME` is the name of the restore object. (Optional) Enter a name for this variable. If no name is specified, then a default name is created, "`<S3 BUCKET NAME>-<TIMESTAMP>`".

   `TIMESTAMP` is the timestamp of the latest backup. Obtained by looking at backup logs.

   This creates a restore object named <RESTORE NAME> from the backup bucket <S3 BUCKET NAME>.

   For example:`--velero restore create restorename --from-backup BUCKETNAME-backup-20200729154634`
4. To check the restore status, type `velero restore logs <RESTORE NAME>`

Restoring Kubernetes from a Disaster on the Same Kubernetes Cluster

Perform the following steps after a disaster, to restore the Kubernetes cluster from a backup.

About this task

Note: You can restore from disaster to another Kubernetes cluster. To do this, deploy a new Kubernetes cluster with Velero and use the same S3 Bucket and Velero credential file.

Procedure

1. To change the backup storage location to read-only, type `kubectl patch backupstoragelocation default --namespace <AWS USER ACCOUNT> --type merge --patch '{"spec":{"accessMode":"ReadOnly"}}`

   If the *`AWS USER ACCOUNT`* was not specified during the installation of Velero, the default namespace is "`velero`".

   Note: The backup storage name can be retrieved using

   ```
   velero backup-location get -o yaml
   ```
2. Open a **bash** terminal.
3. To check the backups for the restore name and timestamp, type `velero get backups`.
4. To restore the backup, type `--velero restore create <RESTORE NAME> --from-backup <S3 BUCKET NAME>-backup-<TIMESTAMP>`

   Where,

S3 BUCKET NAME is the name of the bucket. Obtained when creating a bucket during the installation of Velero.

RESTORE NAME is the name of the restore object. (Optional) Enter a name for this variable. If no name is specified, then a default name is created, "<S3 BUCKET NAME>-<TIMESTAMP>".

TIMESTAMP is the timestamp of the latest backup. Obtained by looking at backup logs.

This creates a restore object named <RESTORE NAME> from the backup bucket <S3 BUCKET NAME>.

For example:`--velero restore create restorename --from-backup BUCKETNAME-backup-20200729154634`

5. To check the restore status, type `velero restore logs <RESTORE NAME>`
6. To change the backup storage location back to read-write, type `kubectl patch backupstoragelocation default --namespace velero --type merge --patch '{"spec":{"accessMode":"ReadWrite"}}'`

Recycling the CWP Kubernetes Cluster Passwords

CWP Kubernetes cluster uses the following account passwords:

- Active Directory service account password.
- `CWP Database` access account password.
- Contact Tracing Nymi Edge Agent password.

As a best practice, organizations should regularly recycle the passwords. This involves changing the passwords in the Kubernetes cluster and changing the passwords for all Contact Tracing Nymi Edge Agent components in the deployment.

Changing Passwords in the Kubernetes Cluster

Perform the following steps to change the Active Directory service account password and `CWP Database` access account password, and then update the password in the Kubernetes cluster.

About this task

Procedure

1. Change the Active Directory account password on the Active Directory.
2. Change the Contact tracing database access account password on the database server.
3. Log into the computer that you used to deploy CWP Kubernetes cluster.
4. For a Windows computer, launch the Bash Terminal to access the respective Linux distribution.
5. Change to the CWP deployment folder.
6. Type `.\init-crypto prod`
7. Update the Kubernetes cluster by typing `.\cwp prod update broker ctapi ctprocessor`

Changing passwords for the Nymi Edge Agent

About this task

Edge agents uses two passwords:

- Active Directory service account that is used to query for Nymi Bands in NES.
- Contact Tracing Nymi Edge Agent password that is configured in the CWP Kubernetes cluster.

Perform the following steps to change the passwords.

Procedure

1. Log onto the computer with `Nymi Edge Agent` software.
2. On a Windows computer, launch a WSL 2 Linux distribution.
3. Change to the `Nymi Edge Agent` deployment folder.
4. Type the following command to encrypt the Active Directory service account password:
   `secretutil.ps1 -enc` *`ad_acct_password`*
   The output displays the encrypted password.
5. Copy the output of the command.
6. Edit the *edge_agents.conf* file and search for the *`nes.password`* property.
7. Paste the encrypted password, replacing the current value for the *`nes.password`* property.
8. Type the following command to encrypt the Contact Tracing`Nymi Edge Agent` password:
   `secretutil.ps1 -enc` *`edge_agents_password`*
9. In the *edge_agents.conf* file, search for the *`sasl.password`* property.
10. Paste the encrypted password, replacing the current value for the *`sasl.password`* property.
11. Copy *edge_agents.conf* to the *C:\Nymi\Edge_Agents\conf* directory of each computer on which you have installed the `Nymi Edge Agent` software.

Uninstalling Nymi Components

This section provide information about how to uninstall the `Nymi Band Application`, `Nymi Runtime` and Nymi Lock Control .

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

About this task

Perform the following steps to uninstall `Nymi Lock Control`.

Procedure

1. On the System Tray, right-click the `Nymi Lock Control` icon, and select **`Quit`**.
2. Open **`Add or Remove Programs`**.
3. In **`Apps and Features`**, search for `Nymi Lock Control`.
4. Select `Nymi Lock Control`, and then click **`Uninstall`**.
5. On the `User Account Control` window, click **`Yes`**.

Uninstalling the Nymi Runtime

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

Uninstalling on Nymi Bluetooth Endpoint on HP Thin Pro

Perform the following steps to remove the `Nymi Bluetooth Endpoint` application from an HP Thin Pro client.

Procedure

1. Connect to the HP Thin Pro client and open an X Terminal session.
2. Type `dpkg --purge nbed_`*`x.y.z`*`_amd64.deb`

Where you replace `x.y.z` with the actual version number of the file.

Uninstalling the Nymi Edge Agent

Perform the following actions to uninstall the `Nymi Edge Agent` application.

About this task

Procedure

1. Open the **`Task Manager`** and go to the **`Processes`** tab. Right-click *javaw.exe* and click **`End Task`**.
2. From the desktop, go to **`Start > Settings > Apps > Apps and Features`**.

   Note: You may also go to **`Start > Control Panel > Programs > Programs and Features`**.
3. Click `Nymi Edge Agent` and select **`Uninstall`**.

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