Deployment and Administration Guide

Nymi Connect for Android
v3.0
2025-03-09

Contents

Preface

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

Purpose

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

This guides contains information about how to install, configure and use the Nymi Connect application on Android devices.

Audience

This guide provides information to CWP Administrators. A CWP the person in the enterprise that manages the CWP solution in their workplace.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	November 28, 2025	First release of this document.
2.0	January 2, 2026	Second release of this document. Updates include new content related to password changes and disabled AD accounts.
3.0	March 9, 2026	Third release of this document. Updates include: • New content to describe 2 new MDM configuration parameters device_info_1 and device_info_2 in the section *Preparing the Mobile Device Management System*.

Related documentation

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

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

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

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

  Separate guides are provided for authentication on iOS and Windows device.

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

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

- **Connected Worker Platform Release Notes**

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

How to get product help

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

How to provide documentation feedback

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

Nymi Connect for Android Deployment Overview

The Nymi Connect for Android software extends the use of the Nymi Band to provide user authentication and e-signatures with Android devices.

The following figure provides a high level overview of the components in the Nymi solution with Nymi Connect for Android and the TCP ports that are used between the components for communication.

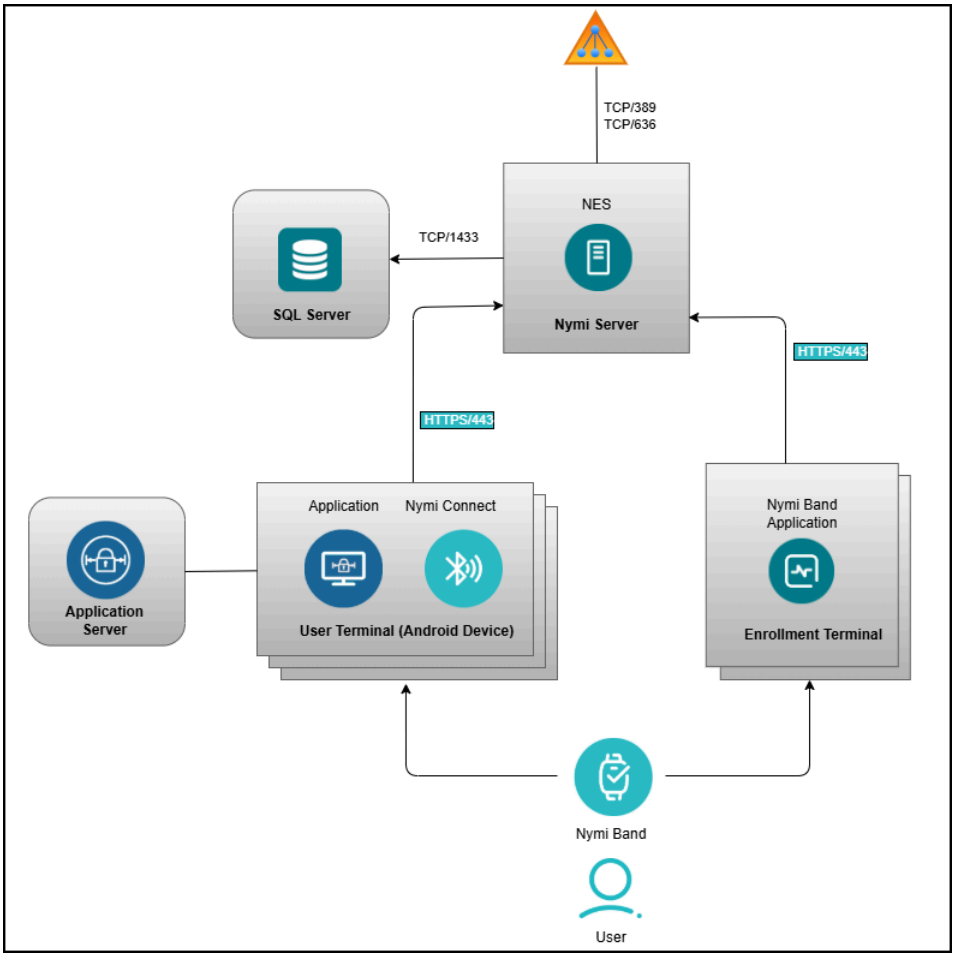


Figure 1: Connected Worker Platform with Nymi Connect components and connection ports

The Nymi solution with Nymi Connect for Android consists of the following components.

Table 2: Connected Worker Platform Components

Component	Description
Enrollment Terminal	Windows 10 or Windows 11 endpoint that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the Nymi Band Application Terminal, which you use to enroll a new user and link them to their Nymi Band. The Nymi Band Application requires the Nymi Runtime application, which the Nymi Band Application automatically installs. The Nymi Band Application communicates with the Nymi Band through the Nymi-supplied Bluetooth adapter, which you plug into a USB port on the enrollment terminal.
User Terminal	Android device on which you install Nymi Connect and an application that requires a username and password to complete authentication tasks, such as login or e-signatures.
Nymi Connect	A password provider application that detects Nymi Band taps and then securely autofills the username and password credentials of the Nymi Band user into the UI of an application on behalf of the user.
Application	A target application that performs authentication by using usernames and passwords, and which a customer plans to integrate with Nymi Connect to support secure authentication processes.
Nymi Band	A wearable device that is associated with the biometrics of a single user. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled. **Note:** Nymi Connect for Android supports the BLE component of the Nymi Band only.
Nymi Enterprise Server(NES)	Windows-based management server and collection of services that administrators access through a web-based application. NES coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates.
NES Administrator Console (not shown)	A web application that provides NES Administrator with an interface to manage the NES configuration and users.
Domain Controller (DC)	Windows server with Active Directory.

Firewall Port Requirements

The following tables summarizes the TCP port requirements for the Connected Worker Platform.

Component	Port Requirements
Enrollment Terminal	Port 443 to the NES server for HTTPS communication.
User Terminal	Port 443 to the NES server for HTTPS communication.
NES server	Port 1443 to the SQL server. Port 389 to the Active Directory server for LDAP communication. Port 636 to the Active Directory server for LDAPS communication.

Nymi Connect for Android Use Cases

Nymi Connect for Android supports various authentication use cases including login and e-signatures. Nymi Connect for Android leverages the Nymi Band for this purpose, which results in a more secure and convenient authentication experience.

Prepare for a Nymi Connect for Android Deployment

Review this section for information about the support application versions, prerequisite requirements and the steps that you must perform to prepare for the Nymi Connect for Android deployment.

Supported Devices

You can install the Nymi Connect for Android on Android devices that run Android versions 10 to 16.

Pre-requisites

Nymi Connect for Android has the following pre-requisite requirements:

- CWP 1.20.1 or later Nymi Enterprise Server (NES).
- CWP 1.20.1 or later Nymi Band Application.
- Mobile Device Management (MDM) system that allows you to install and configure the Nymi Connect for Android software on Android devices.
- Bluetooth-enabled Android device.

  Note: Confirm that your policies do not disable Bluetooth on the Android device.
- Network connectivity between the Android device and the Nymi Enterprise Server(NES).
- Nymi Band 3.0 with firmware 4.11.1.2 or later or Nymi Band 4.
- Ability to transfer log files from the Android device, as required for troubleshooting purposes.

Install and Configure Nymi Components in a Nymi Connect for Android Environment

To use the Nymi Band to complete authentication tasks on an Android device, you must deploy the following Nymi components:

- Nymi Connect for Android on your Android devices.
- Nymi Enterprise Server(NES) on a Windows server.
- Nymi Band Application on a Windows computer.

Note: This guide assumes that you have deployed Nymi Enterprise Server(NES). The *Nymi Connected Worker Platform—Deployment Guide* describes how to deploy NES.

Set up NES

Configure Nymi Enterprise Server(NES) to support Nymi Connect for Android and generate the client registration token that android devices use to register with NES.

Configuring the Required NES Policies Options

To allow the integration to store encrypted passwords, enable the Nymi Lock Control option in the active NES policy.

About this task

Before users enroll their Nymi Bands, perform the following tasks from a Web Browser to enable the Nymi Lock Control.

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 figure provides an example of the Lock Control policy settings.

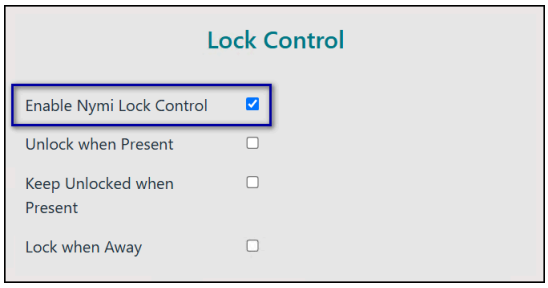


Figure 2: Enable Lock Control

Note: It is not necessary to select other Lock Control options.

5. Click **Save**.

Generating the Client Registration Token

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

Before you begin

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

About this task

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

Procedure

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

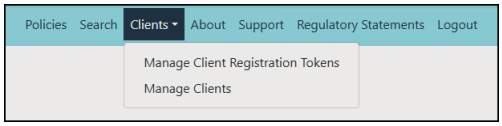


Figure 3: NES Clients menu

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

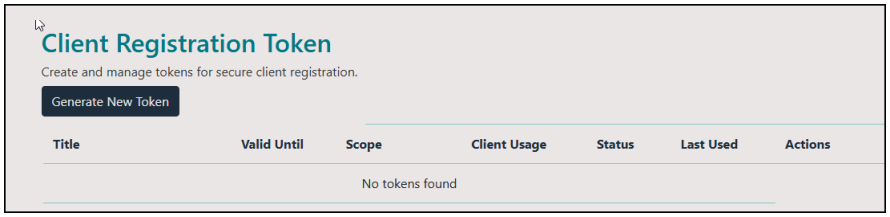


Figure 4: Generate New Token

The `Generate Client Registration Token` window appears.

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

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

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

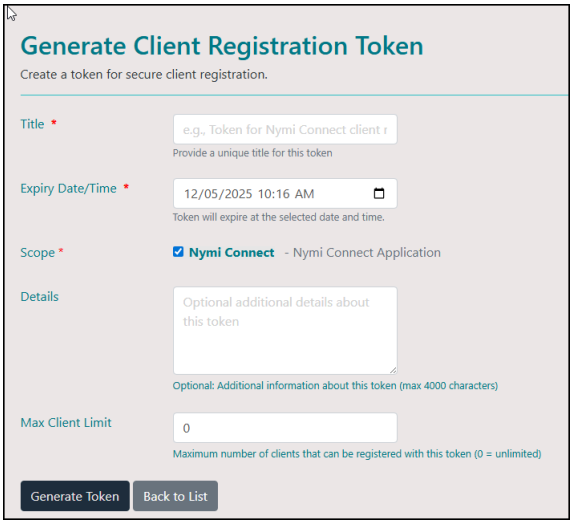


Figure 5: Generate Client Registration Token window

   The `Token Generated Successfully` window appears.

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

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

     a. Click **`Copy JSON`**.
     b. Open a text editor and paste the JSON string.
     c. Save the file.
   - When you manually install and configure Nymi Connect for Android on an Android device, click **`Download QR Code`**. NES saves an image of the QR Code in *PNG* format in the *Downloads* folder of the current user.

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

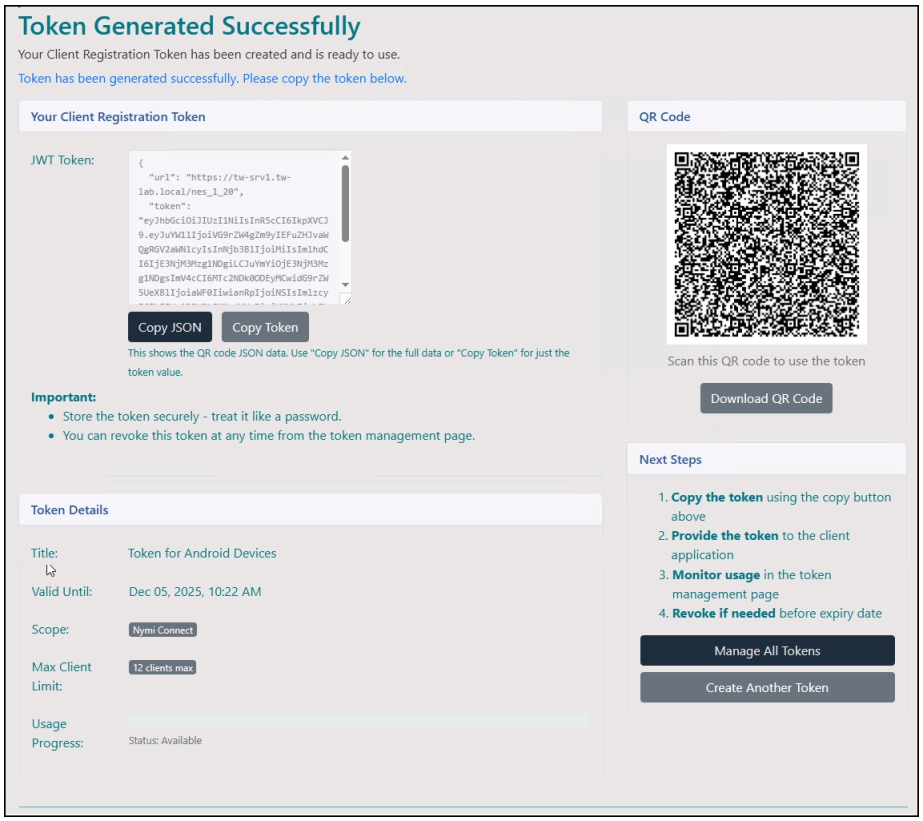


Figure 6: Token Generated Successfully window

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

What to do next

Ensure that you store the copy of the token securely.

Set Up Thick Client Enrollment Terminal

Install the Nymi Band Application, which also installs the Nymi Runtime software on a thick client.

Install the Nymi Band Application

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

You can perform a customizable installation or a silent installation.

Installing/Updating the Nymi Band Application

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Before you begin

For an update, uninstall the previous version of Nymi Runtime.

Procedure

1. Download the Nymi Band Application package.
2. Double-click the *Nymi-Band-App-installer-v_`version`.exe* file.
3. On the `User Account Control` window, click **`Yes`**.
4. On the `Prerequisites` window, click **`Next`**.
5. On the `Welcome` page, click **`Install`**.
6. On the `User Account Control` page, click **`Yes`**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
7. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **`Next`**.
8. On the `Nymi Runtime Setup` window, click **`Next`**.
9. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
   - Accept the default service account NTAuthority\LocalService, click **`Next`**.
   - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.

   Note: The service account must have permission to run as a service. Enable Service Log On provides more information about how to modify the local policy to enable this permission for the service account.

   The following figure shows the `Service Account` window.

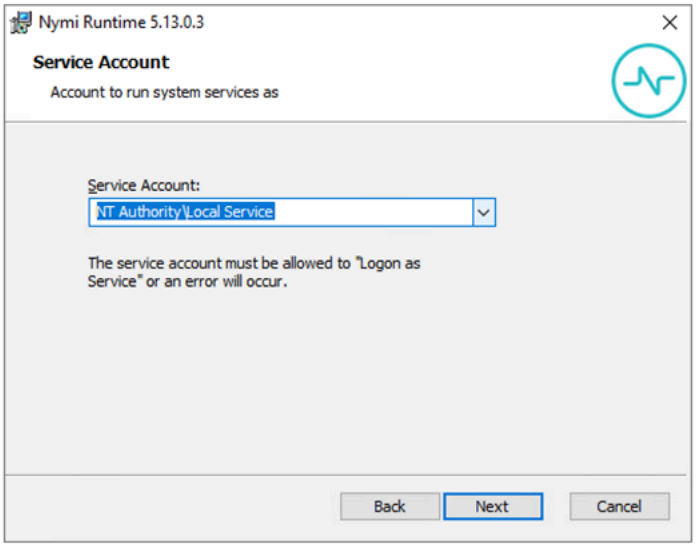


Figure 7: Nymi Runtime Service Account window

10. On the `(Optional) Nymi Infrastructure Service Account`, click **`Next`**.

Only deployments that use web-based Nymi-enabled Applications(NEAs) with a centralized Nymi Agent require you to configure the Nymi Infrastructure Service Account.

11. On the `Ready to install` page, click **`Install`**.
12. Click **`Finish`**.
13. On the `Installation Completed Successfully` page, click **`Close`**.
14. On the `Welcome to Nymi Band Application Setup Wizard` window, click **`Next`**.
15. On the `Select Installation Folder` window, click **`Next`** to accept the default installation location.
16. In the `Ready to Install` window, click **`Install`**.
17. On the `Completing the Nymi Band Application Setup Wizard` window, click **`Finish`**.

What to do next

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

Installing the Nymi Band Application Silently

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

Before you begin

Before you install the Nymi Band Application, install the Nymi Runtime

Procedure

1. Save the Nymi Band Application package, provided to you by your Nymi Solution Consultant.
2. Launch the command prompt as administrator.
3. From the folder that contains the Nymi Band Application, type *Nymi-Band-App-installer-v_`version`.exe /exenoui /q*

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

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

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

Configuring the Nymi Enterprise Server URL

After you install the Nymi Band Application, perform the following steps to ensure that the enrollment process connect to the correct Nymi Enterprise Server(NES).

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software > Nymi`**.
4. Right-click **`Nymi`**, and then select **`New > Key`**. Name the key **`NES`**.
5. Right-click **`NES`**, and then select **`New > String value`**.
6. In the **`Value`** field, type ***URL***.
7. Double-click **`URL`** and in the **`Value Data`** field, type ***https://nes_server/NES_service_name/*** or ***http://`nes_server`/`NES_service_name`*** depending on the NES configuration

   where:

   - *`nes_server`* is the FQDN of the NES host. The FQDN consists of the ***hostname.domain_name***. You can also find the FQDN by going to the server on which you deployed NES viewing the properties of the computer. The *`nes_server`* is the value that appears in the **`Full computer name`** field.
   - *`NES_service_name`* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
8. Click **`OK`**.

Set Up Android Devices

To use the Nymi Band to perform authentication tasks in applications on Android devices, you must install Nymi Connect for Android on each Android device.

Nymi recommends that you use a Mobile Device Management (MDM) system to configure and deploy Nymi Connect for Android. You must perform the following actions for enrolled Android devices:

- Import the Root CA certificate for NES (when the Root CA that issued the certificate is not a trusted CA).
- Enable Bluetooth. The Nymi Connect for Android communicates with the Nymi Band by using the integrated Bluetooth Adapter on the Android device.
- Deploy Nymi Connect for Android.
- Configure Nymi Connect for Android.

Preparing the Mobile Device Management System

Perform the following steps to prepare your Mobile Device Management (MDM) system for the Nymi Connect for Android deployment to your Android devices.

Before you begin

Ensure that you receive the text file that contains the NES-generated JSON string from your NES Administrator.

About this task

Before you deploy the Nymi Connect for Android to all Android devices in your environment,Nymi recommends that you deploy the Nymi Connect for Android on one Android device, and then test the configuration. Perform the following steps in the MDM system.

Procedure

1. Add the Nymi Connect for Android APK package.
2. Enroll one Android device.
3. Create a device configuration profile.

   Ensure that you perform the following steps in the profile:

   - On all Android versions:
     - Enable **`Bluetooth`**.
     - Allow Nymi Connect for Android to access Bluetooth.
     - Allow Nymi Connect for Android to find, connect to and determine the relative position of nearby devices.
     - Do not allow Nymi Connect for Android to take pictures and record video.
     - Configure Nymi Connect as the default application for Autofill service.
   - On Android 10 and Android 11, enable **`Location`**.
   - On Android 12, enable **`Near BY`** and **`Location`**.
   - On Android 13, 14, and 15, enable **`Near BY`**.
   - Include the following Nymi Connect for Android-specific parameters:

Parameter	Purpose and Value
Initial Access Token	Specifies the token that the Android device uses to perform dynamic registration in Nymi Enterprise Server(NES). Copy the Token value that appears in the JSON string text file. **Note:** Do not include the quotation marks. When a user starts Nymi Connect for Android on the android device for the first time, Nymi Connect for Android uses the token to automatically register the device with NES.
NES URL	Specifies the URL for NES. Copy the NES URL value that appears in the JSON string text file.
Tap Threshold	Defines how close a user must place their authenticated Nymi Band near the Bluetooth Adapter on the Android device to perform a Nymi Band tap, as an RSSI value. A larger negative value (nearer to 0) means a closer distance to the Bluetooth Adapter. Recommended value: -42

Parameter	Purpose and Value
Tap window	Defines how long the user must keep their Nymi Band within the tap threshold distance of the Bluetooth Adapter to complete a Nymi Band tap. A larger value increases the amount of time that a user must keep their Nymi Band within bluetooth range of the Bluetooth Adapter and decreases the sensitivity. Recommended value: 10
Managed configuration	Identifies how to manage the Nymi Connect for Android configuration after you push the application to the device. Specify a value of ***1***, which means that users cannot modify the configuration parameters on the Android device.
Device Identifier 1	Identifies the Android device. Nymi recommends that you specify a value that is unique on each device and allows you to easily identify the device. For example, the device serial number.
Device Identifier 2	Identifies the Android device in a manner that ensures an independent security audit can validate the legitimacy of an NES-registered Android device. Nymi recommends populating this field with a device-specific identifier that is visible in MDM but not on the device. For example, when a mobile device enrolls with MDM, some MDM systems assign the device a randomly-generated UUID, which you can use to populate this field.

4. Associate the device configuration profile with the Android device.
5. Push the application and device profile configuration to the Android device.

What to do next

After your MDM system pushes the software and configuration options, Nymi Connect for Android appears as an application on the Android device.

Deploying Nymi Connect for Android

Nymi recommends that you start the Nymi Connect for Android application on the Android device, confirm that dynamic device registration completes in NES, and then test the tap performance of the Nymi Band with your application.

Before you begin

Ensure that you prepare in the following manner:

- Enroll a Nymi Band.
- Wear and authenticate your Nymi Band.
- If required, wear the PPE that an operator of the Android device wears over top of the Nymi Band.

Procedure

1. Launch Nymi Connect for Android.

2. Launch Nymi Connect, which automatically completes the dynamic client registration process in Nymi Enterprise Server.

   Note: Ensure that you complete the dynamic client registration before the date in which the client registration s token expires.

3. If you were unable to configure Nymi Connect as the default Autofill service in your MDM device configuration, perform the following steps:

   a) On the **`Configure Nymi Connect`** window, touch the **`Autofill`** toggle button to configure Nymi Connect as the default autofill service on the device.

   The following figure provides an example of the **`Configure Nymi Connect`** screen with Autofill enabled.

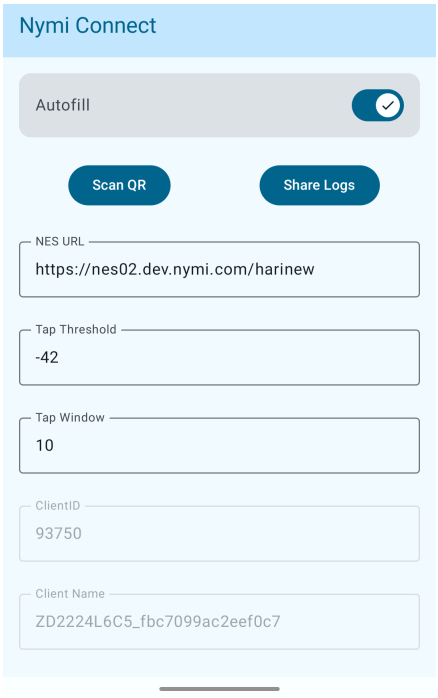


Figure 8: Nymi Connect Configuration screen

   b) On the `Autofill service` screen, select Nymi Connect, as shown in the following figure.

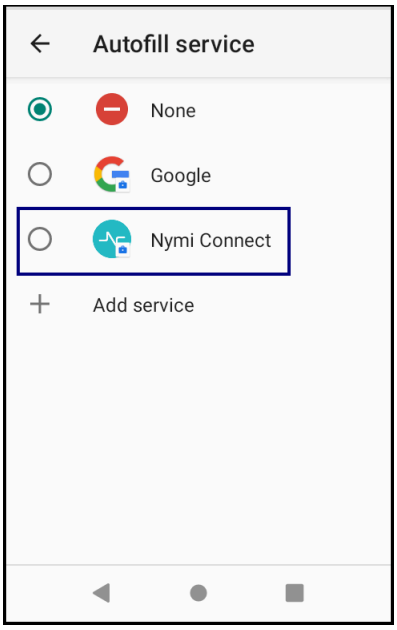


Figure 9: Autofill Services screen

c) On the `Make sure you trust this app` screen, click **OK**.

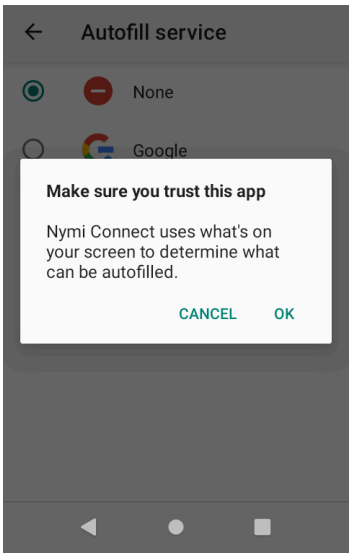


Figure 10: Make sure you trust this app screen

d) Confirm that Nymi Connect option is selected, and then exit the `Autofill service` screen.

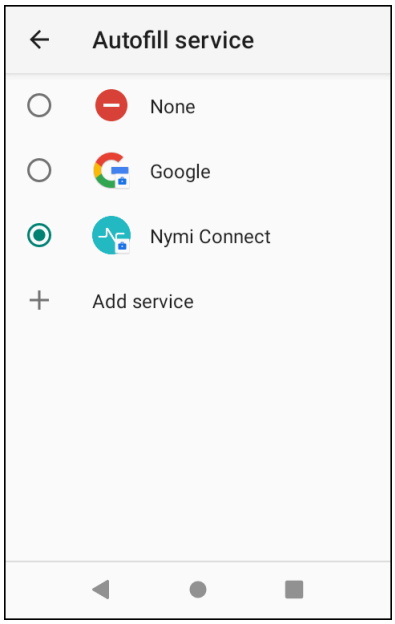


Figure 11: Autofill Services screen with Nymi Connect selected

4. Launch the target application and perform several operations that require a login or e-signature. *Using Nymi Connect for Android* describes how to use Nymi Connect for Android.
5. Confirm the following behaviour:
   - Nymi Connect appears on the screen and prompts you to tap the Nymi Band on the Bluetooth adapter.
   - Nymi Connect detects the Nymi Band tap and in response injects the credentials of the user into the target application.

   If testing reveals that Nymi Connect does not consistently detect Nymi Band taps, edit the device configuration profile in the Mobile Device Management (MDM) system, adjust the values for the *Tap Threshold* and **`Tap Window`** parameters, push the change to the Android device, and then retest. For more information, refer to the *Troubleshooting Bluetooth Taps* topic in the *Nymi Connected Worker Platform—Troubleshooting Guide*

What to do next

After you verify and customize the Nymi Connect for Android configuration, perform the following actions:

1. In your Mobile Device Management (MDM) system:
   - Add the remaining Android devices to the device configuration profile.
   - Push Nymi Connect and the configuration to all Android devices.
2. Launch Nymi Connect on each Android device to ensure that dynamic client registration process completes in Nymi Enterprise Server.

Using Nymi Connect for Android

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

Before you begin

The placement of Bluetooth adapter differs between Android device types. Ensure that you are familiar with the position of Bluetooth antennae on your device.

Procedure

1. Touch on the username field in the application.
   A toast message appears that prompts the user to use Nymi Connect to complete task. The following provides an example of the toast message that appears after the user touches the username field.

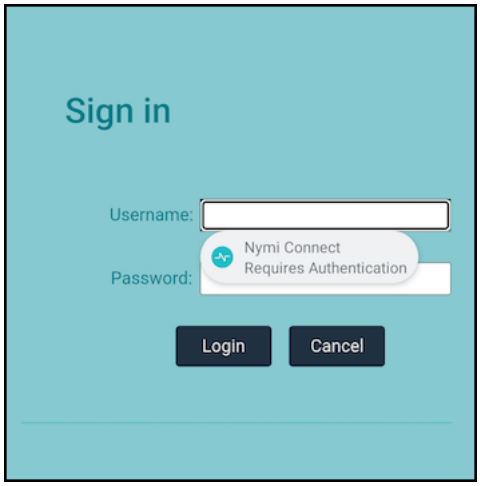


Figure 12: Nymi Connect Toast message

2. Touch the toast message.
   Nymi Connect for Android appears, and then displays a message that prompts to user to tap their Nymi Band. The following figure provides an example of the `Tap the Nymi Band` screen.

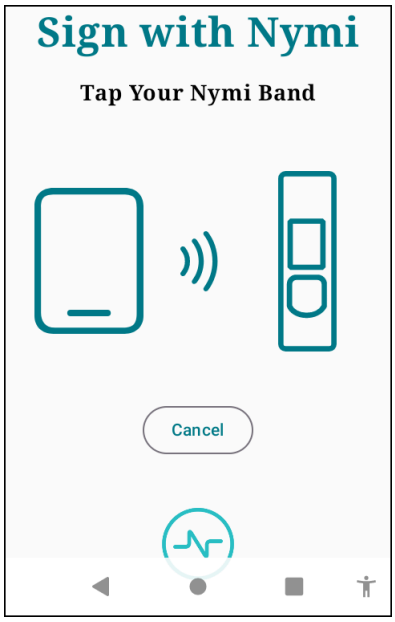


Figure 13: Tap Your Band screen

3. Tap the Nymi Band near the Bluetooth Adapter.
   The message Fetching user credentials appears. If the credentials are valid, Nymi Connect displays a Success message, and then injects the credentials into the username and password fields of the target application.
4. Touch the appropriate button, for example, Sign-in, Login or Ok, in the target application to complete the authentication task.

Managing Password Changes

The configuration of the environment affects how Nymi Connect detects password changes.

Single Site Deployment

If the user changes their password and they perform a tap in Nymi Connect, a screen appears that prompts the user to provide their current password.

The following image provides an example of the screen.

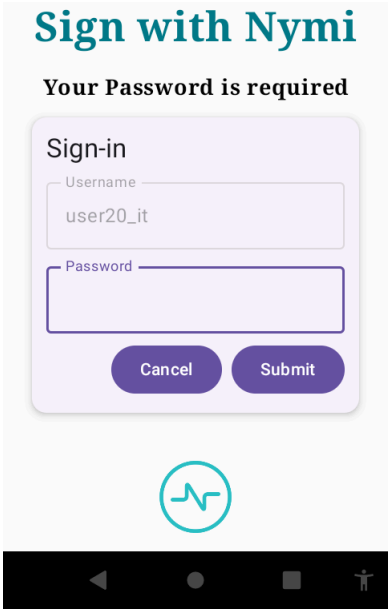


Figure 14: Your password is required screen.

After the user types their password and clicks **`Submit`**, Nymi Connect validates the credentials. If the credentials are valid, Nymi Connect displays a Success message, and then injects the credentials into the username and password fields of the target application.

Multi-site Deployment

In deployments with multiple Active Directory (AD) sites, password updates do not propagate synchronously across all sites. Consequently, when a user performs a tap in Nymi Connect, the system might retrieve and inject the previous password for the user into the **`Password`** field, and might not prompt the user to type their updated password until the AD site that hosts Nymi Enterprise Server (NES) receives the password change. To force a refresh of the cached credentials in NES, after a user changes their password, Nymi recommends that the user immediately log into the Nymi Band Application with their new password.

Auditing Nymi Connect Usage

NES stores audit information about Nymi Connect within several tables in the NES database.

`audit.client Schema`

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

Table 3: audit.client Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.
EventType	Type of event, denoted by a single character. There are three event types: • C—when the client was created in the NES. • U—when the client was updated in NES • D—when the client was deleted in NES.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
ID	Identifier in the oauth.client table.
ClientID	Unique identifier that NES assigned to the client.
ClientName	Logical name of the device as defined by Nymi Connect at the time of registration.
AppName	Name of Nymi application that runs on the device, for example Nymi Connect.
ClientSecret	Randomly generated secure secret key which NES and the client use for token requests.
OSType	Operating system of the client. For example, Linux, Windows, Android, and MacOS
CreatedBy	Machine name of the NES server that performed the client registration.
RegistrationType	Type of client registration. In this release, NES only supports dynamic client registrations.
HostName	Host name or device name of the client.

Column Name	Description
InitialAccessTokenID	Hashed copy of the client registration token that Nymi Connect used to register the client.
CreatedAt	Date and time that the object entry was created in the table.
ModifiedAt	Date and time that the object entry was modified in the table.
ModifiedBy	User account that modified the object entry in the table. For example, when the user performs an enrollment, the AD user account for the user appears.

`audit.InitialAccessToken Schema`

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

Table 4: audit.IntialAccessToken Schema

Column Name	Description
Identity	Unique identifier for the schema entry.
EventTime	Date and time associated with the event that is defined by EventType.
EventType	• C—when the CRT was created in NES Administrator Console. • U—when the CRT was modified in the NES Administrator Console. • R—when the CRT was revoked in NES Administrator Console. • D—when the CRT was deleted in the NES Administrator Console.
SystemUser	Account that is specified as the Application Pool Identity for the NES application pool.
TokenID	Unique identifier that NES assigned to the CRT.
Token	Hashed copy of the client registration token.
Title	User-defined title of the CRT.
ValidUntil	Expiration date and time of the CRT.
Scope	Application associated with the CRT. Values include: • 2—Nymi Connect for Android
Details	User-defined notes about the CRT.
MaxClientLimit	User-defined value that defines how many devices can use the CRT to register with NES. A value of 0 means that there is no limit on the number of devices that can use the CRT.

Column Name	Description
LastUsedTime	Date of the last time a client used the CRT to register with NES.
CreatedAt	Date and time that the object entry was created in the table.
ModifiedAt	Date and time that the object entry was modified in the table.
ModifiedBy	User account that modified the object entry in the table. For example, when the user performs an enrollment, the AD user account for the user appears.
IsRevoked?	Status of validity of the CRT. Values that can appear: • 0—Token is valid. • 1—Token is revoked.
IsDeleted?	Status of the presence of the CRT in the NES Administrator Console. Values that can appear: • 0—Token appears in NES Administrator Console. • 1—Token deleted from NES Administrator Console.

oauth Schema

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

Table 5: oauth schema

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

Telemetry Schema

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

Table 6: Telemetry.log Schema

Field	Description
ID	Unique identifier for the schema entry.
TimeStamp	Date and time that the log event was recorded in UTC timezone format.

Field	Description
Severity	Severity level of the log event. Values that can appear: • Error • Warning • Information
[Level]	Application-defined level or category for the log event. Values that can appear: • Error • Warning • Information
Message	Description of the log event.
Exception	For logs events that have an Error severity level, contains exception details or stack trace. For log events that have a Warning of Information severity level, the value is NULL.
TraceId	Placeholder for future functionality, in this release the value that appears in NULL.
SpanId	Placeholder for future functionality, in this release the value that appears in NULL.
Source	Name of the component or subsystem that generated the log event. For example, JWTAuthenticationFilter and ClientRegService.

Field	Description

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

Field	Description
CreatedAt	Date and time that the object entry was created in the table.
ModifiedAt	Date and time that the object entry was modified in the table.
ClientIp	IP address of the client device.

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

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

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

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

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

-- From UserCore and NymiBand tables
uc.[Domain],
uc.[Username],
nb.[NymiBandID],
nb.[NfcUID],
nb.[FirmwareVersion],
nb.[IsActive]
FROM [telemetry].[log] AS l
JOIN [nub].[NymiBand] AS nb
ON nb.[NymiBandID] = JSON_VALUE(l.[Attributes], '$.AuthenticatorId')
OR nb.[NymiBandID] = JSON_VALUE(l.[Attributes],
'$.SecondaryAuthenticatorId')
```

```
JOIN [nub].[UserCore] AS uc
ON uc.[ID] = nb.[UserCoreID]
WHERE uc.[Username] = 'username'
ORDER BY l.[Timestamp] DESC;
```

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

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

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

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

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

-- Extract JSON Attributes

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

-- From UserCore and NymiBand
uc.[Domain],
uc.[Username],
nb.[NymiBandID],
nb.[NfcUID],
nb.[FirmwareVersion],
nb.[IsActive]
FROM [telemetry].[log] AS l
JOIN [nub].[NymiBand] AS nb
ON nb.[NymiBandID] = JSON_VALUE(l.[Attributes], '$.AuthenticatorId')
OR nb.[NymiBandID] = JSON_VALUE(l.[Attributes], '$.SecondaryAuthenticatorId')
```

```
JOIN [nub].[UserCore] AS uc
ON uc.[ID] = nb.[UserCoreID]
WHERE nb.[NymiBandID] = 'band_id'
ORDER BY l.[Timestamp] DESC;
```

Manage Nymi Connect for Android

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

Managing Client Registration Tokens

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

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

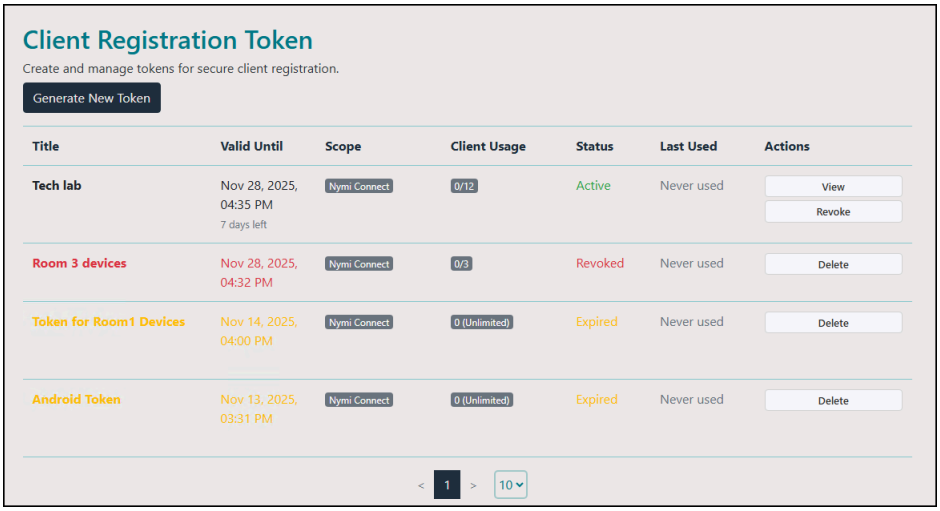


Figure 15: Manage Client Registration Tokens

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

Column	Description
Title	Displays the descriptive name of the CRT.
Valid Until	Displays the expiration date for the token.
Scope	Displays the Nymi application that is associated with the token.

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

Viewing CRTs

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

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

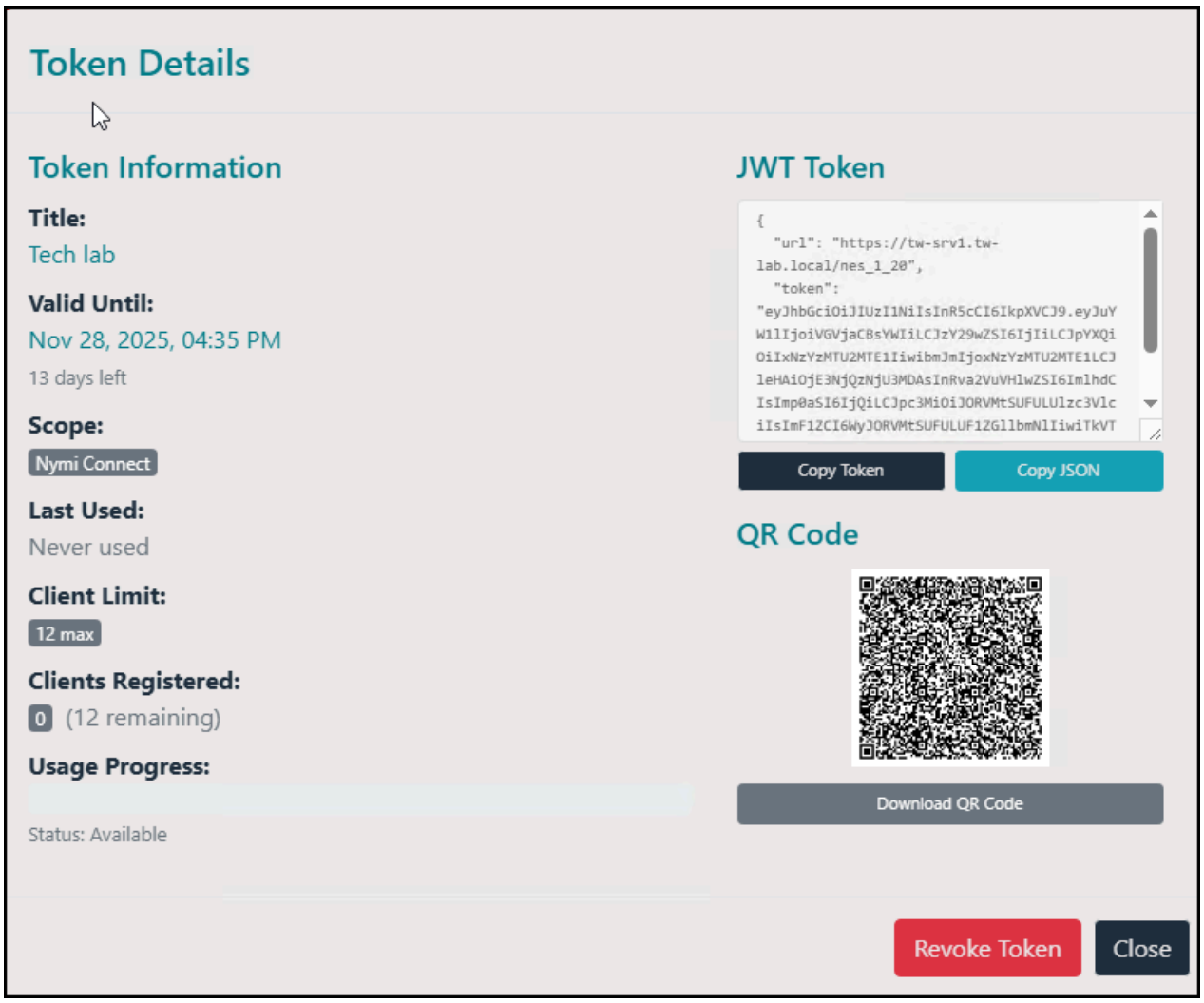


Figure 16: Token Details window

Revoking CRTs

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

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

Deleting CRTs

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

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

Managing Clients that use Client Registration Tokens

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

Viewing Clients

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

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

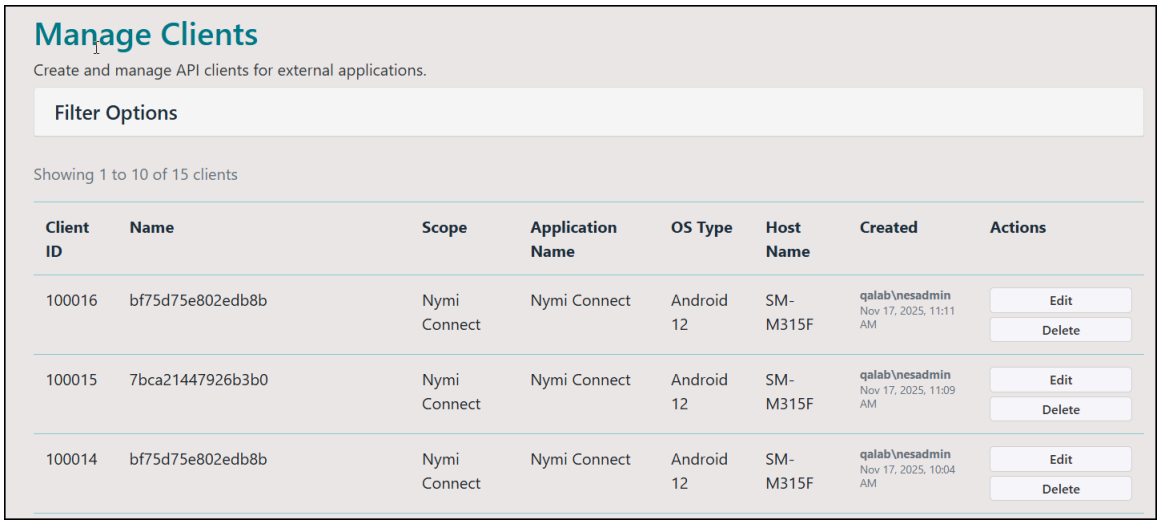


Figure 17: Manage Clients window

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

Column	Description
Client ID	Displays a unique identifier for the client.

Column	Description
Name	Displays a unique name for the Android device, which you can use to easily identify the Android device. The name that appears depends on the MDM parameter configuration for Nymi Connect: • If the MDM configuration includes values for the *device_info_1* and *device_info_2* parameters, the Name value that appears is a combination of the two parameter values. • If the MDM configuration does not include the device parameters, the Name value that appears is the Android ID.
Scope	Displays the Nymi application that is used by the client.
Application Name	Displays the name of the application on the client.
OS Type	Displays the operating system of the client.
Hostname	Displays the hostname of the client.
Created	Displays the date that the client was dynamically registered in NES and the user that performed the action.
Actions	Provides the user with two buttons to perform management actions on the client: • Edit the client. • Delete the client.

Editing Clients

You can edit a client to change the client name.

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

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

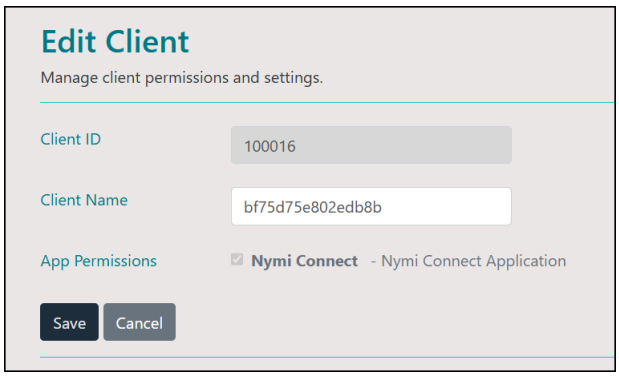


Figure 18: Edit Client window

Deleting Clients

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

1. In the **`Manage Clients`** table, from the **`Actions`** column of the appropriate client, click **`Delete`**.
2. On the `Delete client` popup, click **`Delete`**. When you delete an client, the action removes the client from the NES Administrator Console but not the NES database. To allow a client to use Nymi Connect and a Nymi Band, you must push an CRT to the client and complete dynamic registration.

Troubleshoot Nymi Connect for Android Errors

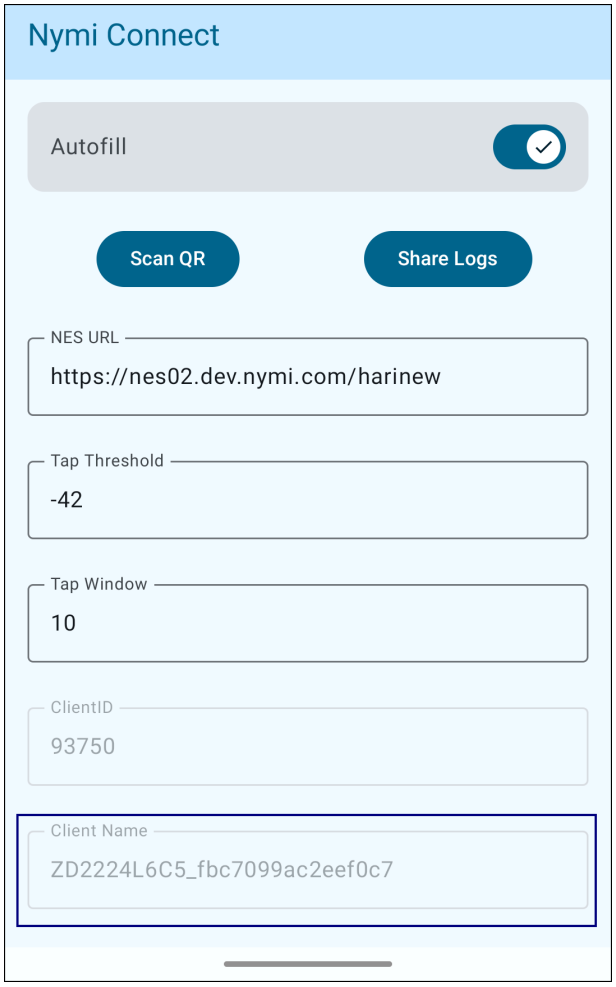
This section provides information about how to troubleshoot and resolve error messages that can appear when you use Nymi Connect for Android.

Identifying the Android Device

When troubleshooting Nymi Connect for Android issues with your MDM team, the MDM team might require you to identify the problematic device by client name, which is a combination of two values that the MDM team defines in the MDM device profile. You can view the client name from the Android device and the NES Administrator Console.

Identifying the Android Device from the Android Device

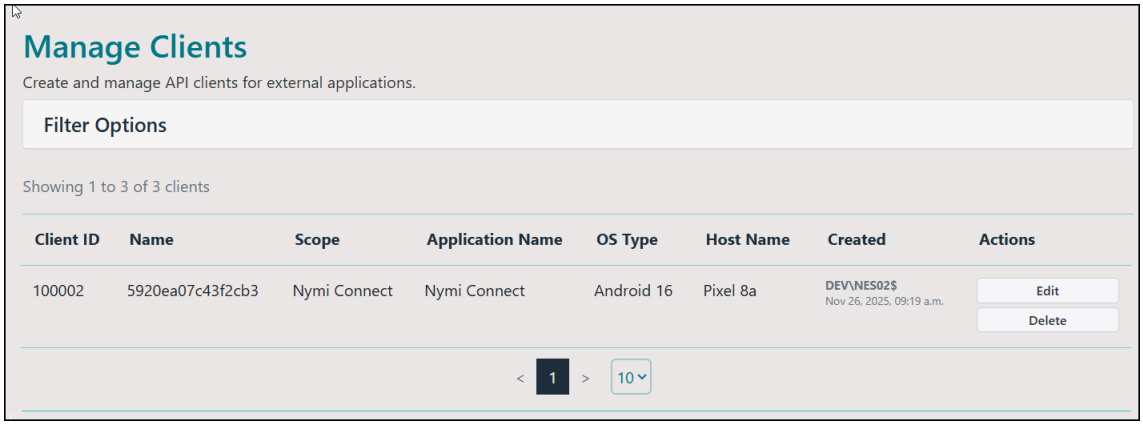
To determine the client name from the Android device, tap the Nymi Connect icon in the app drawer/list. The `Nymi Connect` screen appears and the client name is at the bottom, as highlighted in the following figure.



Identifying the Android Device from the NES Administrator Console

To determine the client name from the NES Administrator Console perform the following actions:

1. Log into the NES Administrator Console as an NES Administrator.
2. From the top menu, select **`Clients > Manage Clients`**.
3. In the **`Manage Clients`** table, the client name appears for each Android device. The following figure provide an example of the **`Manage Clients`** table with the client name of one registered Android device highlighted.



.

Nymi Connect for Android Log Files

The Android devices uses a log buffer to store Nymi Connect for Android log information.

Log File Management

Nymi Connect automatically manages log files on the Android device in the following ways:

- The maximum size for the *nymi_connect.log* file is 2MB.
- When the file size reaches 2 MB (approximately 300 Nymi Band taps), Nymi Connect for Android archives the log file in the format *nymi_connect-YYYY-MM-DD.version#.log*, and then creates a new *nymi_connect.log* file.
- Nymi Connect for Android automatically deletes log files older than 14 days.
- You cannot change the Nymi Connect for Android log maintenance settings in this release.

Log File Collection

Nymi Support might require you to collect log information from the Android device for troubleshooting purposes.

Note: A user might require administrative privileges on the Android device to share log files.

To collect Nymi Connect log files, perform the following steps:

1. Tap the Nymi Connect icon in the app drawer/list. The `Nymi Connect` screen appears.
2. Click **`Share Logs`**, as shown in the following figure:

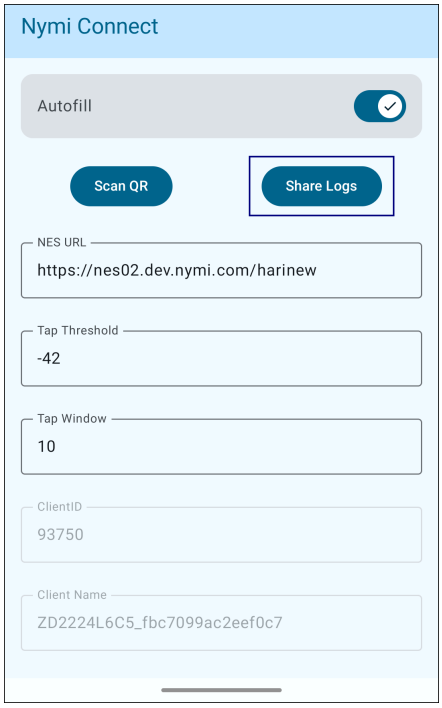


Figure 19: Share Logs button

A bottom sheet that appears that displays the name of the log file and a list of applications that are available for log file delivery. The available applications depend on your device configuration.

3. Select the appropriate application to share the log file. Nymi Connect for Android generates a compressed file that contains all Nymi Connect for Android log files

Troubleshooting Dynamic Client Registration Errors

Review this section for information about error messages that might appear the first time you launch Nymi Connect on an Android device.

Nymi Connect - OAuth2 dynamic client registration failed - Initial access token expired

This error message can appear the first time any user launches Nymi Connect for Android.

The following figure provides an example of the screen with the error message:

Figure 20: OAuth2 dynamic client registration failed - Initial access token expired

Cause

Nymi Connect cannot dynamically register the device in NES because the Client Registration Token (CRT) is not valid.

Resolution

To resolve this issue, perform one or more of the following actions:

- Log into the NES Administrator Console and review the expiration date of the CRT. If the token defined in the Android has expired:
  1. Create a new CRT in NES.
  2. Update the MDM configuration with the new CRT.
  3. Push the configuration update to the Android devices.
- Resolve connectivity issues and ensure that the Android device can communicate with NES over TCP port 443.
- Correct the NES URL value for Nymi Connect for Android in the MDM configuration and push the changes to the Android devices.

Nymi Connect - OAuth2 dynamic client registration failed - Initial access token has been revoked

This error message can appear the first time any user launches Nymi Connect for Android.

The following figure provides an example of the screen with the error message:

Figure 21: OAuth2 dynamic client registration failed - Initial access token has been revoked

Cause

An NES Administrator has revoked the Client Registration Token (CRT) in Nymi Enterprise Server (NES), and Nymi Connect cannot use the token to dynamically register the device.

Resolution

To resolve this issue, perform one or more of the following actions:

- Log into the NES Administrator Console perform the following actions:
  1. Create a new CRT in NES.
  2. Update the MDM configuration with the new CRT.
  3. Push the configuration update to the Android devices.

Nymi Connect - OAuth2 token fetching failed

This error message can appear when a user launches Nymi Connect for Android.

The following figure provides an example of the screen with the error message:

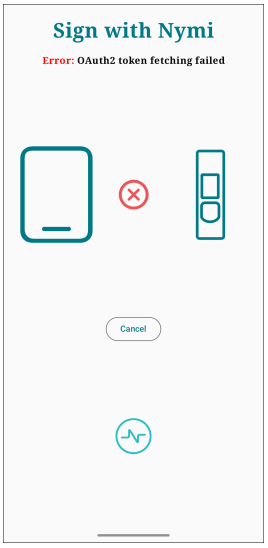


Figure 22: OAuth2 token fetching failed

Cause

Nymi Connect cannot retrieve or refresh the authorization token from Nymi Enterprise Server (NES).

Resolution

To resolve this issue, perform one or more of the following actions:

- Resolve connectivity issues and ensure that the Android device can communicate with NES over TCP port 443.
- Correct the NES URL value for Nymi Connect for Android in the MDM configuration and push the changes to the Android devices.
- Confirm that the NES server is up and running. For example, confirm that you can log into the NES Administrator Console.
- Re-register the client(s), by performing the following steps:

  1. Create a new CRT in NES.
  2. Update the MDM configuration with the new CRT.
  3. Push the configuration update to the Android devices.

Troubleshooting Nymi Connect for Android Usage Errors

Review this section for information about error messages that can appear when you use Nymi Connect for Android and a Nymi Band to complete authentication tasks.

Nymi Connect - Configuration is missing or invalid

This error message can appear when a user launches Nymi Connect for Android.

The following figure provides an example of the screen with the error message:

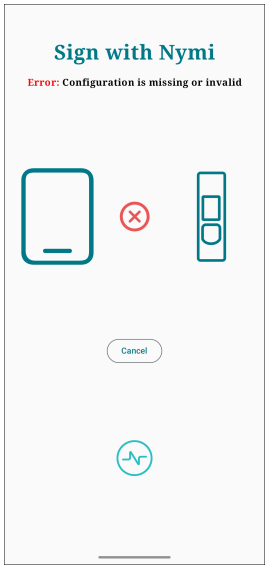


Figure 23: Configuration is invalid

Cause

There is a configuration error in the Nymi Connect application settings or the settings were not pushed from the Mobile Device Management (MDM) system.

Resolution

Correct the NES URL value for Nymi Connect for Android in the MDM configuration and push the changes to the Android devices.

Nymi Connect - Nymi Enterprise Server is unreachable

This error message can appear when a user launches Nymi Connect for Android.

The following figure provides an example of the screen with the error message:

Figure 24: NES is unreachable

Cause

Nymi Connect cannot communicate with Nymi Enterprise Server(NES).

Resolution

To resolve this issue, perform one or more of the following actions:

- Confirm that the NES server is up an running.
- Resolve connectivity issues and ensure that the Android device can communicate with NES over TCP port 443.
- Correct the NES URL value for Nymi Connect for Android in the MDM configuration and push the changes to the Android devices.

Nymi Connect - Failure Communicating With the Nymi Band

This error message can appear on the `Sign on with Nymi` screen.

The following figure provides an example of the screen with the error message:

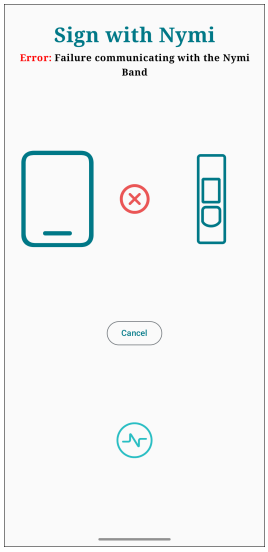


Figure 25: Failure communicating with the Nymi Band

Cause

Nymi Connect cannot detect or communicate with the Nymi Band.

Resolution

To resolve this issue, perform one or more of the following actions:

- Enable Bluetooth on the Android device and allow Nymi Connect to access Bluetooth.
- Instruct the user to ensure that the Nymi Band remains authenticated and near the Bluetooth Adapter until Nymi Connect injects the user credentials into the target application.

Nymi Connect - Nymi Band Firmware is Out of Date

This error message can appear when a user performs a Nymi Band tap on the `Sign on with Nymi` screen with Nymi Band 3.

The following figure provides an example of the screen with the error message:

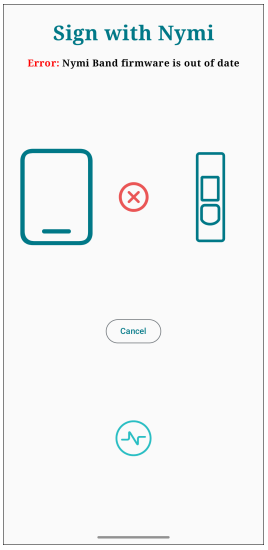


Figure 26: Nymi Band Firmware is out of Date

Cause

Nymi Connect does not support the firmware version of the Nymi Band.

Resolution

To resolve this issue, update the firmware version on the Nymi Band to 4.11.1.2 or later.

Nymi Connect - User is not authorized to use Nymi Connect

The error message can appear when a user performs a Nymi Band tap on the `Sign on with Nymi` screen.

Error Message

The following figure provides an example of the screen with the error message:

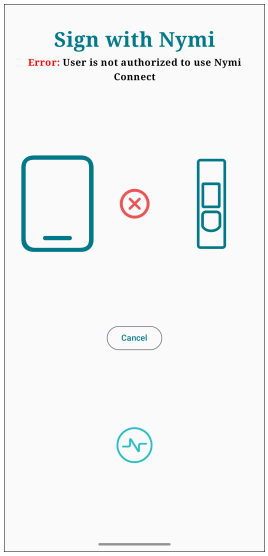


Figure 27: User is not authorized to use Nymi Connect

Cause

This error message appears when the user enrolled the Nymi Band with a different Nymi Enterprise Server(NES) instance. For example, the user enrolled the Nymi Band with a Development NES but the user accessed Nymi Connect in the production environment.

Resolution

To resolve this issue, instruct the user to enroll a Nymi Band with the correct NES instance.

Nymi Connect - The Nymi Band is not configured to work with Nymi Connect

This error message can appear when a user performs a Nymi Band tap in Nymi Connect.

Error Message

The following figure provides an example of the screen with the error message:

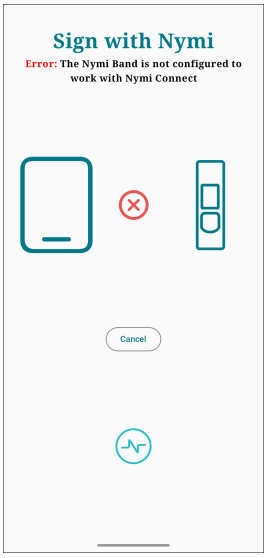


Figure 28: The Nymi Band is not configured to work with Nymi Connect

Cause

The Lock Control option was not enabled in the Nymi Enterprise Server(NES) policy at the time that the user enrolled the Nymi Band.

Resolution

To resolve this issue, perform the following steps:

1. Log into the NES Administrator Console as an NES Administrator.
2. Edit the active policy and enabled **`Lock Control`**, as shown in the following figure.

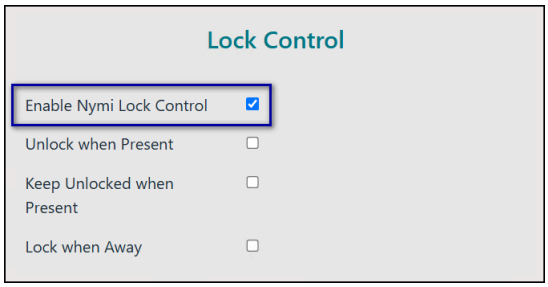


Figure 29: Enable Lock Control

3. Save the policy.
4. Instruct the user to wear and authenticate their Nymi Band, and then log into the Nymi Band Application.

Nymi Connect - User password is invalid

The error message can appear when a user types their updated password when prompted by Nymi Connect.

The following figure provides an example of the screen with the error message:

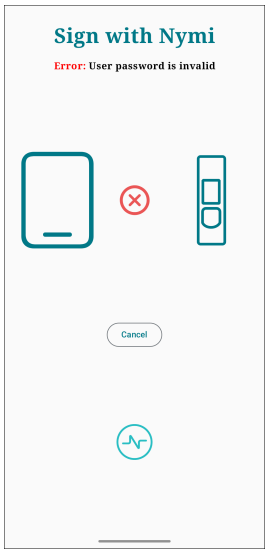


Figure 30: User password is invalid

Cause

When prompted, the user provided an incorrect password.

Resolution

To resolve this issue, instruct the user to re-enter the password.

Nymi Connect - Password has expired

When a user performs a Nymi Band tap, Nymi Connect might prompt the user to type their password. This error might appear after the user types their password.

Cause

The password of the user has expired in AD.

Resolution

To resolve this issue, instruct the user to perform the following steps:

1. On the `Password has expired` screen, click **`Cancel`**.
2. Change the AD password by using the method outlined in your standard operating procedures, for example, in the self-service password portal.
3. Re-attempt the authentication task on the Android device.
4. When Nymi Connect prompts the user for their password, type the new password.

Nymi Connect - Cannot log in using this account

When a user performs a Nymi Band tap, Nymi Connect might prompt the user to type their password. This error might appear after the user types their password.

Cause

This error message can occur for several reasons:

- Account does not exist in AD.
- Account is disabled.
- Account is locked.
- Account has expired.

Resolution

To resolve this issue, perform the following steps:

1. On the `Cannot log in using this account` screen, instruct the user to click **`Cancel`**.
2. Engage your AD administrator to correct the properties of the user account in AD.
3. Instruct the user to re-attempt the authentication task on the Android device.

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