

Nymi Connect for Windows

Installation and Configuration Guide

Version v1.3

October 20, 2026

Contents

1 Preface 4
1.1 Purpose 4
1.2 Audience 4
1.3 Revision history 4
1.4 Related documentation 5
1.5 How to get product help 6
1.6 How to provide documentation feedback 6
2 Overview 7
3 Nymi Connect Architecture 8
4 Nymi Connect Deployment 10
4.1 Preparing for Nymi Connect Deployment 10
4.1.1 Supported Operating Systems 10
4.1.2 Supported Browsers 10
4.1.3 Supported Connected Worker Platform Versions 11
4.1.4 Pre-requisites 11
4.1.5 Required NES Policies Options 11
4.1.6 Firewall Port Requirements 12
4.1.7 Interaction with Browser Autofill 12
4.2 Deployment Architecture 13
4.3 Install Nymi Connect and Its Dependencies 15
4.3.1 Install Nymi Runtime 15
4.3.2 Install Nymi Connect 15
4.4 Provisioning CWP Mode 18
4.5 Configure Nymi Connect for Windows 20
4.5.1 Restricting Allowed Applications 21
4.5.2 Suppressing Processes 22
4.6 Restart Nymi Connect 23
4.7 Enabling Support for Java-Based Applications 24
4.7.1 Enabling Java Access Bridge 25
4.7.2 Resolving Conflicts with Other Java Accessibility Clients 26
5 Using Nymi Connect 28
5.1 Handling Password Changes 30

5.2 Performing Tasks that Require Two E-Signatures 31
6 Log Files 34
6.1 Log File Access Control 35
6.2 Centralized Audit Logging 35
7 Troubleshooting Nymi Connect 37
7.1 How to Troubleshoot Nymi Connect 37
7.1.1 How Nymi Connect Shows Messages 37
7.1.2 Finding and Reading the Error Code 39
7.1.3 Log File Locations 39
7.1.4 Restarting Nymi Connect 39
7.1.5 Tray Icon Context Menu 40
7.2 Resolving Issues 40
7.2.1 Start-up and Connection Problems 40
7.2.2 CWP Mode Provisioning Problems 52
7.2.3 Tap-to-Fill Problems 56
7.2.4 Password Problems 64
7.2.5 Other Issues 68
8 Upgrading Nymi Connect 69
8.1 Upgrading with the Installation Wizard 69
8.2 Upgrading Silently 69
9 Uninstalling Nymi Connect 70
9.1 Uninstalling with the Installation Wizard 70
9.2 Uninstalling Silently 70

1 Preface

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

1.1 Purpose

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

This guide contains information about how to install, configure, and use the Nymi Connect application.

1.2 Audience

This guide provides information to CWP Administrators, people in the enterprise who manage the CWP solution in their workplace.

1.3 Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	April 24, 2025	First release of this document.
1.1	April 30, 2026	Updated for NCW 1.1.0: compatibility mode, split architecture (NCW Client + NCS), remote user terminal support, centralized audit logging, new log locations, upgrade support, and new troubleshooting entries.
1.2	June 26, 2026	Updated for NCW 1.2.0: added support for Java-based applications, including

Version	Date	Revision history
		enabling Java Access Bridge, configuring bundled and system-installed JREs, resolving conflicts with other Java accessibility clients (for example, Evidian EAM), include/exclude guidance for Java processes, and new troubleshooting entries for the Java-accessibility, active-window-changed, and sign-in-timeout error messages.
1.3	October 20, 2026	Updated for NCW 1.3.0: added CWP Mode (OAuth 2.0) authentication with client registration token provisioning, the AD Mode and CWP Mode component authentication modes, a Restart Nymi Connect procedure, Webswing application support, and a restructured troubleshooting chapter with CWP Mode provisioning error codes.

1.4 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 devices.

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.

1.5 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

1.6 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

2 Overview

Nymi Connect allows users to use their Nymi Bands to log into and perform e-signatures in various web, native Windows, and Java-based applications. A broad spectrum of applications is supported without requiring explicit integration with the Nymi ecosystem, including Manufacturing Execution System (MES) applications such as PAS-X, Syncade, OpCenter, and LabWare.

Currently, Nymi Connect supports applications that utilize Active Directory credentials to authenticate their users. Nymi Connect provides credential injection only — it is not responsible for user authorization within the target application.

Note: Nymi Connect is not responsible for handling AD password changes. However, it provides the ability for the end user to update the encrypted password stored within Nymi infrastructure, after they have changed their AD password through the standard password change process, for example the Windows logon UI.

Authenticating a user is separate from authenticating the Nymi Connect software itself. Users sign in with their Active Directory credentials, as described above. Separately, the Nymi Connect software authenticates to Nymi Enterprise Server (NES) using one of two component authentication modes:

- **AD Mode** — the component authenticates to NES using the Active Directory (AD) computer account of the machine on which it runs. This is the default mode and requires no per-device provisioning, but it requires that the machine is joined to the NES domain, or to a domain that has a trust relationship with it.
- **CWP Mode** — the component authenticates to NES using OAuth 2.0, which removes the dependency on Active Directory for component authentication. A component in CWP Mode is provisioned with a Client Registration Token (CRT) and does not need to be joined to an AD domain to authenticate to NES.

Devices using AD Mode and devices using CWP Mode can coexist in the same deployment, and you can move a device from AD Mode to CWP Mode (see Provisioning CWP Mode). The component authentication mode affects only how Nymi Connect authenticates to NES; it does not change how users authenticate. Active Directory is still used for user identity and authentication in both modes.

3 Nymi Connect Architecture

Nymi Connect operates as part of Nymi Connected Worker Platform and thus requires that CWP be available in the target environment.

Nymi Connect for Windows (NCW) consists of two components:

- **NCW Client** — A user-context application that runs in the Windows system tray. The NCW Client detects Nymi Band taps, identifies the target application, and injects credentials into the application login fields.
- **Nymi Connect Service (NCS)** — A system-context Windows service that runs in the background. NCS handles secure communication with NES for authorization token retrieval, policy retrieval, user status retrieval, domain information retrieval, encrypted password retrieval and updates, and centralized audit logging.

Nymi Connect can be installed locally on compatible Windows machines or can be deployed through VDI systems like Citrix, RDP, etc. Nymi Connect supports both NFC and BLE connectivity for Nymi Band tap detection.

The Nymi Connect for Windows depends on the following CWP components:

Table 2: Connected Worker Platform Components

Component	Description
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.
Centralized Nymi Agent	Nymi Runtime component that you install in a central location on a single machine or a cluster of two or more machines that is accessible to all user terminals, for example on the server with the NES application. The Nymi Agent provides BLE management, manages operations and message routing, facilitates communication between an application and the Nymi Band, and maintains knowledge of the Nymi Band presence and authenticated states. In a thin client deployment, the Nymi Agent runs on the RDP or Citrix server.

Component	Description
Nymi Bluetooth Endpoint	A component of the Nymi Runtime that provides an interface between the Bluetooth Adapter (BLE) and the Nymi Agent. Nymi Bluetooth Endpoint communicates with the Nymi Bands through the Nymi-provided BLE Adapter, which you plug into a USB port on the user terminal.
Nymi Band	A wearable biometric authentication device that is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled.

4 Nymi Connect Deployment

This section describes how to deploy Nymi Connect for Windows, including system requirements and prerequisites, deployment architecture options, installation steps for Nymi Connect and its dependencies, and optional post-install configuration.

4.1 Preparing for Nymi Connect Deployment

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

4.1.1 Supported Operating Systems

You can install Nymi Connect on the following operating systems:

- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

4.1.2 Supported Browsers

This release of Nymi Connect supports the following browsers for web-based application credential injection:

- Google Chrome
- Microsoft Edge

4.1.3 Supported Connected Worker Platform Versions

This release of Nymi Connect is compatible with Connected Worker Platform (CWP) 1.20.0 and later. The CWP Mode for component authentication requires CWP 1.20.1 or later; see Provisioning CWP Mode.

4.1.4 Pre-requisites

The machine on which you install Nymi Connect must:

- Have network connectivity to Nymi Enterprise Server (NES).
- For AD Mode: Be either joined to the same domain as NES or joined to a domain that has trust relationships with the one the NES machine is on.
- For CWP Mode: Meet the CWP Mode prerequisites — the Connected Worker Platform must be version 1.20.1 or later (see Supported Connected Worker Platform Versions), Legacy Mode must be disabled (set the system environment variable `NYMI_NEA_SUPPORT_LEGACY_MODE` to `0`), each Nymi Band must run a supported firmware version, and the device must be provisioned with a Client Registration Token (CRT). See Provisioning CWP Mode for the full prerequisites and the procedure.
- For user terminal installations: Have Nymi Runtime (Nymi Bluetooth Endpoint and, in the case of a local installation, Nymi Agent) installed and USB type-A port(s) available for connecting a Nymi-supplied Bluetooth adapter and, optionally, an NFC reader.
- For Java-based target applications: Java Access Bridge enabled for each Java Runtime Environment used by those applications (see Enabling Support for Java-Based Applications). Enable it before users begin using Nymi Connect, because each Java application must be restarted after Java Access Bridge is enabled.

4.1.5 Required NES Policies Options

To allow Nymi Connect to store and retrieve encrypted passwords, the Nymi Lock Control option in the active NES policy must be enabled. This process is described in detail in Section 6.6 of the Nymi Connected Worker Platform—Deployment Guide.

The NES token lifetime must be set to 30 minutes or longer. If you performed a fresh installation of CWP 1.17 or newer, this requirement is automatically met. If your CWP installation was upgrade from an older CWP release (for

example CWP 1.9.x), check the following lines in the file `C:\inetpub\wwwroot\NES\AuthenticationService\Web.Config`, and if needed, update the value to 00:30:00:

```
<setting name="WSTokenTTL" serializeAs="String">
    <value>00:30:00</value>
</setting>
```

4.1.6 Firewall Port Requirements

The following table summarizes the TCP port requirements for the Nymi Connect solution.

Table 3: Firewall Port Requirements

Component	Port Requirements
User Terminal	Port 443 to the NES server for HTTPS communication. Port 9120 to the centralized Nymi Agent server for web socket communications, if Nymi Agent is deployed on a server.
Citrix/RDP Server	Port 443 to the NES server for HTTPS communication. Port 9120 to the centralized Nymi Agent server for web socket communications, when the Nymi Agent runs on a separate server.

4.1.7 Interaction with Browser Autofill

The browser autofill feature may interfere with Nymi Connect operations. When Nymi Connect is used with an application that runs in the browser, when the user clicks on the username field, autofill suggestions may be shown by the browser. If the user moves the mouse at this point, the username text box may no longer be in focus. When the user taps their Nymi Band, Nymi Connect will not be able to inject the username and password.

To avoid this situation, Nymi recommends you to disable the browser autofill feature. Refer to the instructions provided by the specific browser vendor on how to disable browser autofill.

4.2 Deployment Architecture

Nymi Connect for Windows can be installed locally on compatible user terminals or it can be deployed in a VDI environment (e.g. Citrix, RDP). Nymi Connect directly depends on Nymi Runtime (Nymi Agent and Nymi Bluetooth Endpoint).

Deployment in a VDI environment requires installation of a Centralized Nymi Agent. Details on how this is done can be found in Section 4 of the Nymi CWP Deployment Guide.

The following table provides a breakdown of target locations for NCW and Nymi Runtime components in both deployment configurations (local and VDI).

	NCW	Nymi Agent	Nymi Bluetooth Endpoint
Local install	user terminal	user terminal	user terminal
VDI-based deployment	VDI server	central server	user terminal

Note: there are situations where local installs use server-based deployment of the Nymi Agent. In such cases, NCW and NBE are installed on user terminals, while Nymi Agent is on a central server.

The figure below provides a high-level overview of Nymi Connect for Windows deployed in a VDI environment as part of the Connected Worker Platform with a centralized Nymi Agent.

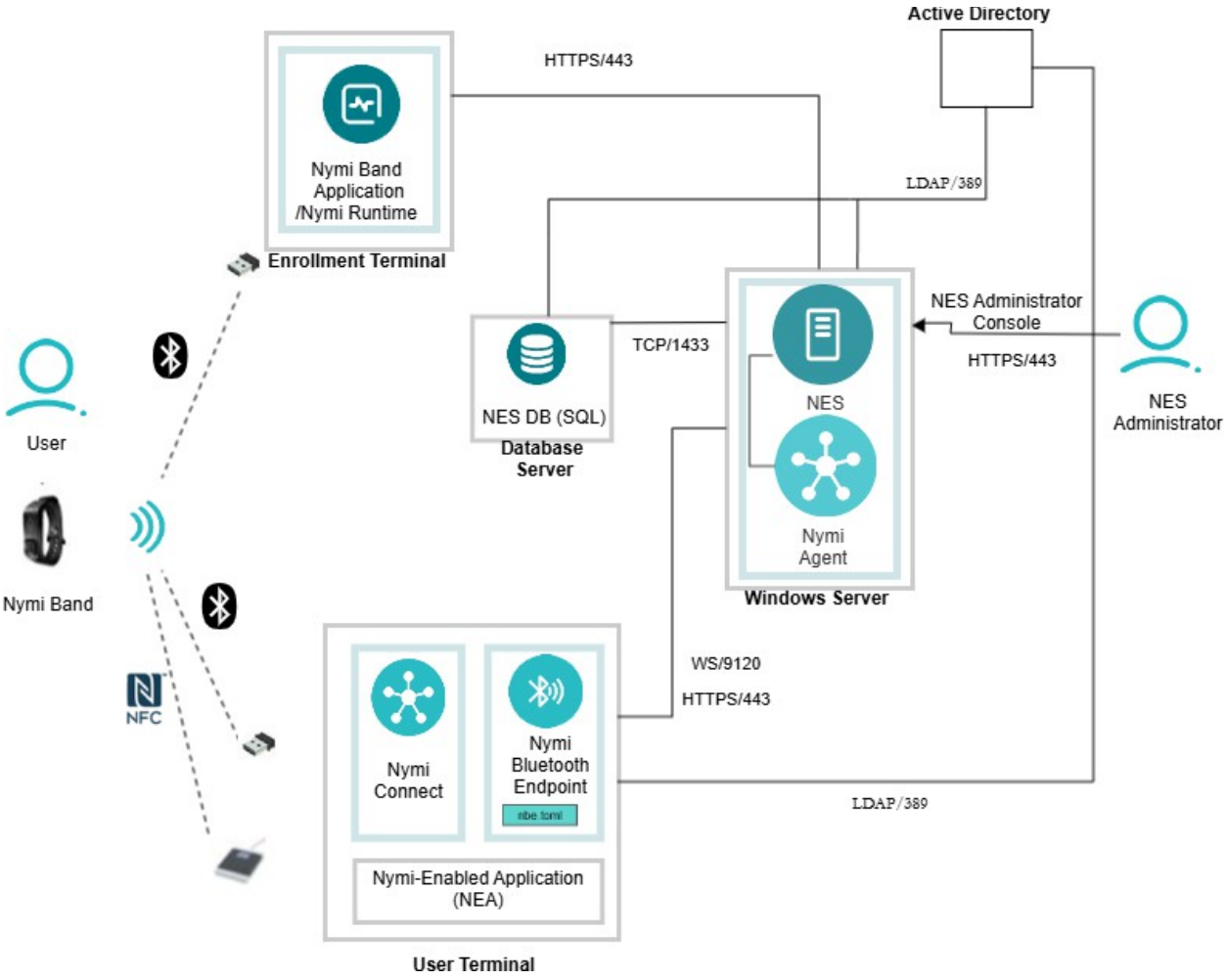


Figure 1. Diagram showing Nymi Connect components in a centralized Nymi Agent configuration, including NCW Client and NCS on the server, NBE on the client machines, and connections to NES and Active Directory

Figure 1: Connected Worker Platform with Nymi Connect components and connection ports in a Centralized Nymi Agent Configuration

Note: Nymi Connect does not support double-hop remote desktop configurations (for example, connecting from a thin client to an RDP server that in turn connects to another RDP server).

Note: You can have a deployment that uses a mixture of user terminals with centralized or local Nymi Agent, but for simplicity Nymi recommends that you choose one configuration and set all of your terminals accordingly.

4.3 Install Nymi Connect and Its Dependencies

Note: This guide assumes that you have deployed the NES in the environment and have an enrollment terminal set up. Nymi Connected Worker Platform—Deployment Guide describes how to deploy them both.

4.3.1 Install Nymi Runtime

Before you install Nymi Connect, install and configure the Nymi Runtime components (Nymi Agent and Nymi Bluetooth Endpoint) on each machine in your deployment as described in the Deployment Architecture section above.

For detailed instructions, see Chapter 8 of the Nymi Connected Worker Platform—Deployment Guide:

- **Local deployments:** Section 8.1 describes how to set up endpoints in a local Nymi Agent configuration, including Nymi Runtime installation, Bluetooth adapter placement, NES URL configuration, and communication protocol settings.
- **VDI-based deployments:** Section 8.2 describes how to set up endpoints in a centralized Nymi Agent configuration, including NBE installation on client machines, nbe.toml configuration, NES and AgentURL registry configuration, and Nymi Agent setup on the server.

4.3.2 Install Nymi Connect

You can install Nymi Connect silently or with the installation wizard.

4.3.2.1 Installing Nymi Connect With the Installation Wizard

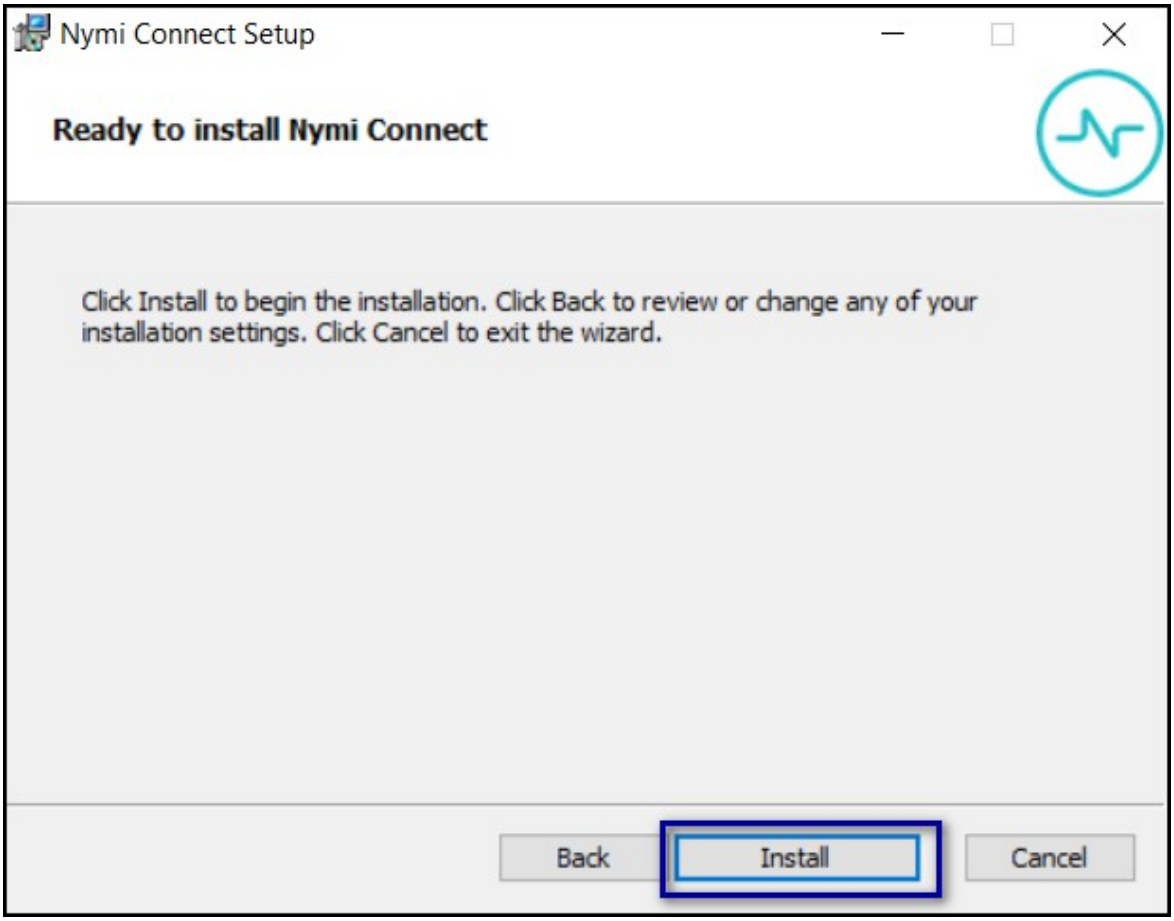
Perform the following steps on each target machine (user terminal or VDI server).

1. Double-click the Nymi Connect installer file.

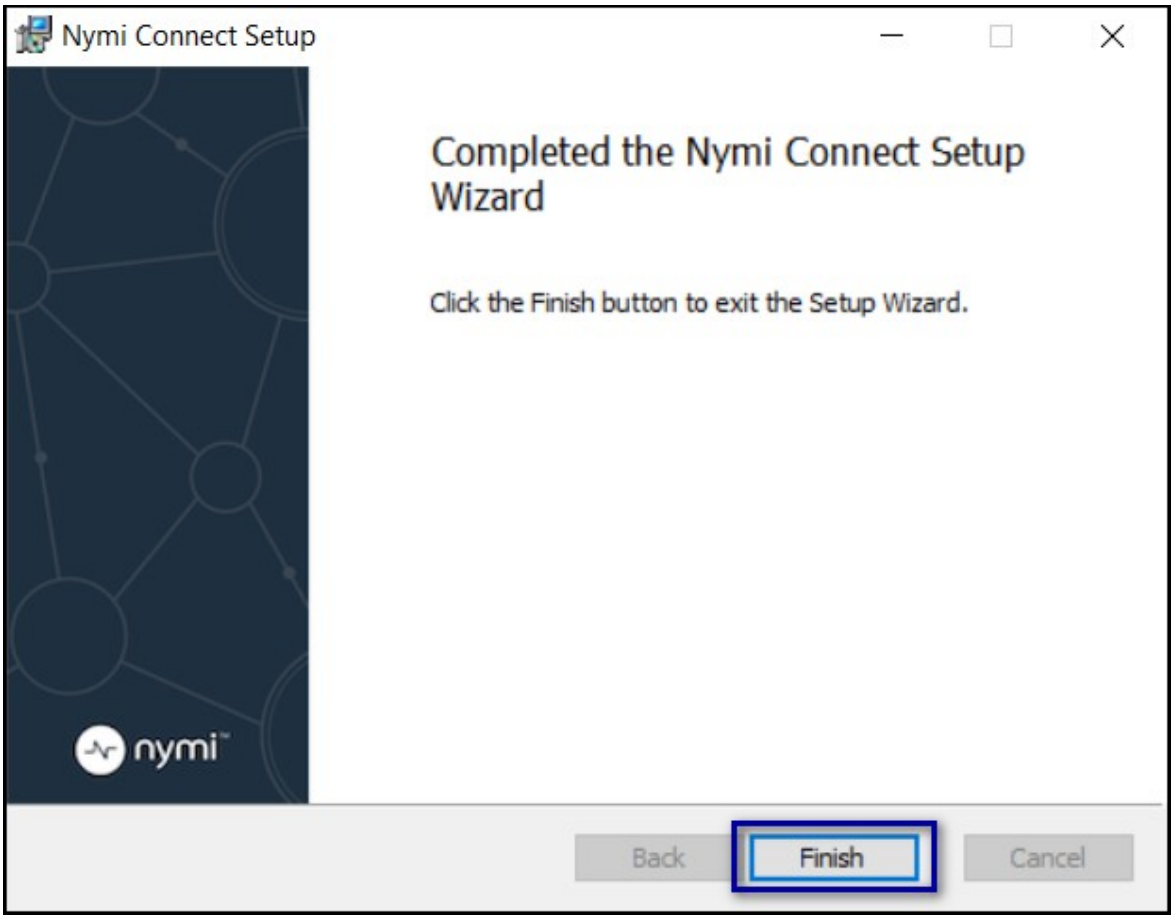
   > **Note:** If you see the “Windows protected your PC” pop-up warning about Windows Defender SmartScreen prevented an unrecognised app from starting, click **More info**, and then click **Run anyway**.

2. Click **Install**.
3. On the User Account Control pop-up, click **Yes**.

4. On the Ready to install Nymi Connect window, click **Install**.



5. On the Completed the Nymi Connect Setup Wizard window, click **Finish**.



4.3.2.2 Installing Nymi Connect Silently

Perform the following steps on each target machine (user terminal or VDI server).

1. Run a Command Prompt as administrator.
2. Type the following command, replacing `<version>` with the version in the installer's file name:

```
"Nymi Connect Installer-<version>.exe" /exenoui /q
```

> **Note:** If you use management software to push the Nymi Connect installation to user terminals or you run the installer as an administrator, you will need to restart the user terminal to ensure that all components initialize correctly and the Nymi Connect application runs under the user context.

4.4 Provisioning CWP Mode

In CWP Mode, Nymi Connect authenticates to Nymi Enterprise Server (NES) using a CRT instead of the Active Directory account of the machine (see Overview). To provision a device, you place the CRT file on it. Nymi Connect detects the file, switches to CWP Mode, and registers with NES, with no restart required.

A device uses AD Mode until a CRT is placed on it, so a device switches to CWP Mode only when you deliver its CRT. This lets you control when each device switches. When you move an existing site from AD Mode to CWP Mode, upgrade first so the site keeps working in AD Mode, and then deliver the CRT when you are ready to switch.

Before you provision a device in CWP Mode:

1. Confirm that the Connected Worker Platform is version 1.20.1 or later.

2. Confirm that each Nymi Band runs a supported firmware version: Nymi Band 3 with firmware 4.11.3.6 or later, or Nymi Band 4 with firmware 5.0.5 or later.

3. Turn off Legacy Mode on each machine where Nymi Connect is installed. Legacy Mode is not disabled by default: set the system environment variable `NYMI_NEA_SUPPORT_LEGACY_MODE` to `0`. The Nymi Connected Worker Platform—Deployment Guide describes the communication protocol and how to disable Legacy Mode (the legacy protocol), in "Configuring the Connected Worker Platform Communication Protocol". After you set this variable, sign out of Windows and sign back in, or restart the computer, so that Nymi Connect reads the new value (see Restart Nymi Connect).

4. Create a Client Registration Token in the NES Administrator Console and save it as a file named `nymi.ncconf`. The Nymi Connected Worker Platform—Administration Guide describes how to generate and manage Client Registration Tokens. For a large-scale deployment, use a single token that permits many devices to register.

You can place the CRT file manually on a small number of devices, or use your software management tooling to place it at scale.

> **Important:** You must have local Administrator rights on the device to provision it.

To provision a device in CWP Mode:

1. Copy the `nymi.ncconf` file into the `C:\Nymi\Configuration` folder on the device.

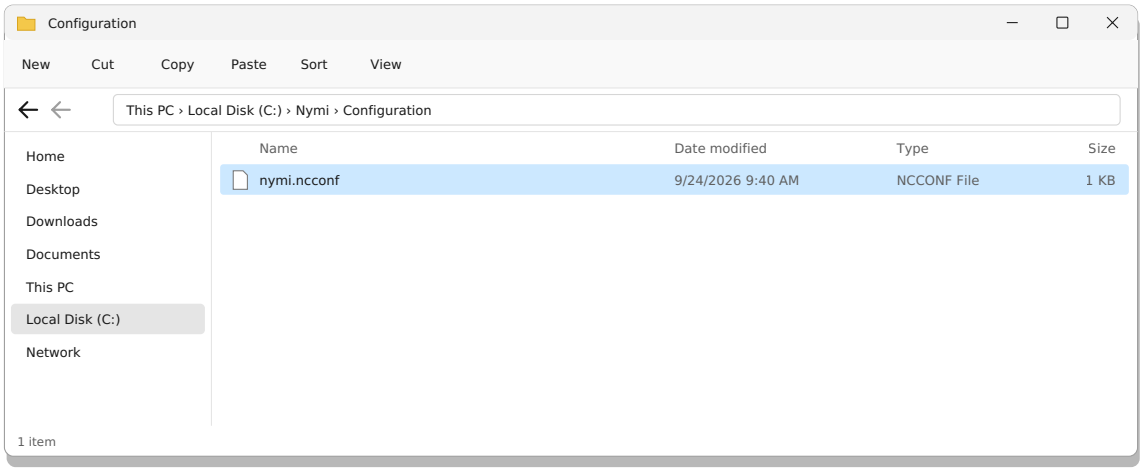


Figure 2. Placing the Client Registration Token file in the configuration folder

> **Note:** The Nymi Connect installer creates the `C:\Nymi\Configuration` folder and sets its permissions. You do not need to change them.

2. Nymi Connect detects the file and applies the configuration, and an alert, Configuration data was applied successfully, confirms that the configuration was applied.

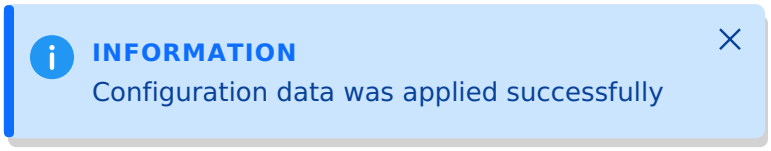


Figure 3. Configuration applied

3. Nymi Connect replaces `nymi.ncconf` with `nymi.provisioned.ncconf`, which contains no sensitive information, and registers with NES.

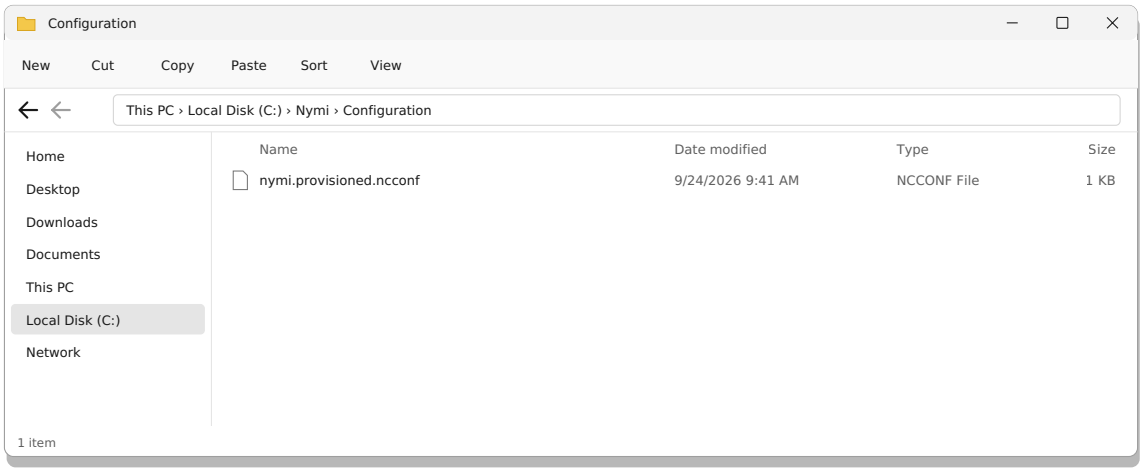


Figure 4. The configuration folder after provisioning has been started

4. Confirm that the device is ready:

    a. Check that the Nymi Connect tray icon does not show a red cross (a red cross indicates a persistent error).
    b. Perform a Nymi Band tap on the device's Bluetooth adapter or NFC reader.
    c. Optionally, open **Manage Clients** in the NES Administrator Console to confirm that the device is registered. The Nymi Connected Worker Platform—Administration Guide describes how to manage clients.

> **Note:** The **Manage Clients** list shows which devices have registered. This is a count of registrations, not a report of readiness. A registered device can still fail for other reasons, so Nymi recommends a Nymi Band tap to confirm that a device is ready. There is no central view of the readiness of every device.

If Nymi Connect cannot use the CRT, or registration fails, it displays a persistent error and the tray icon shows a red cross until the problem is fixed. See Troubleshooting Nymi Connect.

4.5 Configure Nymi Connect for Windows

By default, Nymi Connect allows credential injection into any application without requiring configuration. This is suitable for most deployments.

Administrators can optionally restrict which applications are eligible for credential injection, or suppress specific processes from being handled by Nymi Connect. Configuration is stored in the file:

`C:\Nymi\NymiConnectClient\appsettings.json`

Changes to the configuration file require a restart of Nymi Connect to take effect.

4.5.1 Restricting Allowed Applications

When the `included` list in the configuration file contains one or more application entries, Nymi Connect switches to restricted mode — only the listed applications are eligible for credential injection. If a user attempts to inject credentials into an application that is not in the list, Nymi Connect displays an error message.

Each application entry in the `included` list can be identified by one or more of the following attributes:

- **processName** — the process name of the application (without file extension), for example `msedge` or `chrome`.
- **windowTitle** — the window title (or partial title) of the application.
- **applicationUrl** — the URL or hostname of a web application, for example `https://myapp.domain.com`. Wildcards (*) can be used either in the domain name to support sub-domains, in the path, or both.

When multiple attributes are specified for an application entry, all must match (logical AND).

> **Note:** Java-based applications typically share the same process name (`javaw` for graphical applications, `java` for console applications, or `javaws` for Java Web Start), so `processName` alone cannot distinguish one Java application from another. To target a specific Java application, combine `processName` with a `windowTitle` that matches a stable portion of the application's window title.

Example configuration with an allowed application list:

```
{
  "included": [
    {
      // Matches web pages on Edge Browser with URL
      // https://myapp.domain.com with any window title
      "applicationUrl": "https://myapp.domain.com",
      "processName": "msedge",
      "windowTitle": ""
    },
    {
```

```
      // Matches web pages on Chrome Browser with any URL
      // and any window title
      "processName": "chrome"
    },
    {
      // Matches web pages on any browser, with any window
      // title, with URL under https://mysite.domain.com
      // with any path, for example
      // https://mysite.domain.com/login,
      // https://mysite.domain.com/process1/sign, and
      // https://mysite.domain.com.
      "applicationUrl": "https://mysite.domain.com/*"
    },
    {
      // Matches web pages on any browser, with any window
      // title, with URL under  any subdomains of domain.com,
      // for example https://mysite.domain.com/login,
      // https://emea.mymes.domain.com/process1/sign,
      // but does NOT match https://domain.com.
      "applicationUrl": "https://*.domain.com/*"
    }
  ]
}
```

4.5.2 Suppressing Processes

The suppressed list silently excludes specified processes from all Nymi Connect processing. When the active foreground process matches an entry in the suppressed list, Nymi Connect takes no action — no credential injection, no notification, and no error message.

This is useful for:

- **Co-existence with third-party SSO tools** (for example, Evidian EAM) — suppress the SSO tool's process so that Nymi Connect does not interfere when the other tool is handling authentication.
- **Temporarily disabling Nymi Connect** for a specific process during migration or troubleshooting.

Example configuration with a suppressed process:

```
{
  "suppressed": [
    {
      "name": "Evidian SSO Engine",
```

```
      "processName": "ssoengine"
    }
  ]
}
```

> **Note:** If a process appears in both the `included` and `suppressed` lists, the `suppressed` list takes priority and the process is excluded from credential injection.

> **Note:** Because Java-based applications commonly share the `javaw` (or `java`) process name, suppressing by that process name excludes all Java applications from Nymi Connect, not just one. Suppress a Java process only when you intend to exclude every Java application on the terminal.

4.6 Restart Nymi Connect

Some changes take effect only after a restart. What you restart depends on what changed.

To apply NES-related changes, restart the Nymi Connect Service (NCS). Restart the service after you change any of the following:

- the NES URL in the registry (AD Mode only),
- a root certificate used to establish secure communication with NES, or
- the active NES policy (for example, enabling Nymi Lock Control).

To restart the service, open the Services console (`services.msc`) as an administrator, select **Nymi Connect Service**, and then select **Restart**.

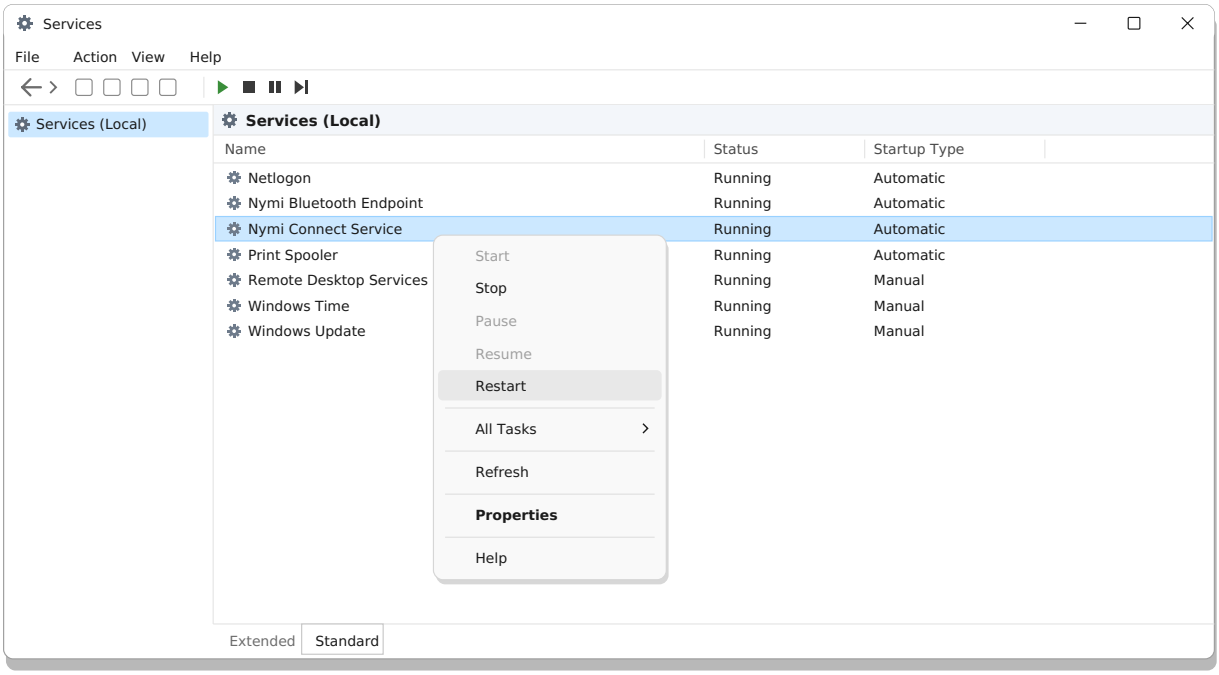


Figure 5. Restarting the Nymi Connect Service in the Services console

To apply application-list changes, restart the NCW Client. The application lists in `appsettings.json` (see Configure Nymi Connect for Windows) are read by the NCW Client, which runs separately for each signed-in user. A user can restart their own NCW Client from the **Restart** option on the Nymi Connect tray icon menu; to apply the change for every user on the machine, restart the computer.

To apply a change to the `NYMI_NEA_SUPPORT_LEGACY_MODE` environment variable, sign out of Windows and sign back in, or restart the computer. Because this system environment variable is read when the user session starts, restarting the NCW Client from the tray icon menu does not apply the change (see Provisioning CWP Mode).

A Client Registration Token does not require a restart — Nymi Connect detects a new token and switches to CWP Mode on its own (see Provisioning CWP Mode).

4.7 Enabling Support for Java-Based Applications

Nymi Connect detects and populates login and e-signature fields through the Windows accessibility layer. Applications built with Java render their windows using Java's own UI toolkit and their fields are not visible to this layer unless **Java Access Bridge (JAB)** is enabled. Until JAB is enabled, Nymi Connect

cannot detect the username and password fields in a Java-based application and credential injection does not occur.

You must enable Java Access Bridge for each Java Runtime Environment (JRE) used by your target Java applications. If an application ships with its own bundled JRE, enable JAB for that JRE; if multiple JREs are installed, repeat the steps for each one. Nymi recommends enabling Java Access Bridge as part of preparing the terminal, before users begin using Nymi Connect, because each Java application must be restarted after the bridge is enabled.

Nymi Connect has been tested for compatibility with the following Java Runtime Environments:

- Java Runtime Environment 8 (32-bit and 64-bit)
- Java Runtime Environment 11 (32-bit and 64-bit)
- Java Runtime Environment 17 (32-bit and 64-bit)
- Java Runtime Environment 21 (32-bit and 64-bit)

4.7.1 Enabling Java Access Bridge

In enterprise deployments, where a JRE is installed for all users of a machine, enable Java Access Bridge at the JRE level so that the setting applies to every user of that machine:

1. Open the JRE's accessibility configuration file in a text editor (create it if it does not exist). The location depends on the Java version:
   - **Java 8:** `<install-folder>\lib\accessibility.properties`
   - **Java 9 and later:** `<install-folder>\conf\accessibility.properties`

   where `<install-folder>` is the base location of the JRE or JDK used by the target application.
2. Add the following line (or uncomment it if it is already present):

   ```
   assistive_technologies=com.sun.java.accessibility.AccessBridge
   ```

3. Save the file and restart the Java application so that it loads the Access Bridge.

An application may use its own bundled JRE or it may use one from a system location. Be sure to enable Java Access Bridge for the correct one.

Example: Locating the configuration file

Enable Java Access Bridge for whichever JRE the target application uses:

Application-bundled JRE. Some applications install their own JRE in a non-standard location — under `C:\Program Files`, `C:\ProgramData`, or even a user's profile. A `jre` sub-folder (for example `C:\ProgramData\<Vendor>\<App>\jre`) indicates the Java 8 layout, so edit `C:\ProgramData\<Vendor>\<App>\jre\lib\accessibility.properties`.

System-installed JDK or JRE. Other applications use a Java installation shared system-wide. On Java 9 and later there is no `jre` sub-folder, so edit the `accessibility.properties` file in the installation's `conf` sub-folder. For example, for Eclipse Adoptium 17, `C:\Program Files\Eclipse Adoptium\jdk-17.0.10.7-hotspot\conf\accessibility.properties`.

If you are unsure of the Java version, run `java.exe -version` from the JRE's `bin` folder.

Note: To enable Java Access Bridge for the current user only, apply the same change to your own copy of the file: create or edit `%USERPROFILE%\.accessibility.properties` (note the leading dot) and add the `assistive_technologies` line. Running `jabswitch -enable` from the JRE's `bin` folder does this for you. A per-user file takes precedence over the JRE-level file for that user.

4.7.2 Resolving Conflicts with Other Java Accessibility Clients

Nymi Connect reads the fields of a Java application through the standard Java Access Bridge provider loaded in that application's JVM. Some other products install their own Java accessibility provider. For example, **Evidian EAM**. Because a JVM selects its accessibility provider through a single setting, another product installed on the operating system can displace the provider Nymi Connect relies on, so that Nymi Connect cannot detect or populate the fields of a Java application.

To allow Nymi Connect to operate on Java-based applications on a machine where such a product is installed, disable that product's Java accessibility (Java application support) function for the affected JREs. For Evidian EAM, perform this through Evidian's own configuration tooling — refer to the Evidian EAM administrator documentation, or contact your Evidian administrator, for the procedure for your version.

Note: This is separate from suppressing the Evidian SSO process described in Suppressing Processes. Process suppression governs which application windows Nymi Connect acts on; disabling the other product's Java

accessibility prevents the two products from contending for the Java accessibility interface itself.

To confirm whether a conflicting product is active on a machine, see Nymi Connect Cannot Detect Fields in a Java Application in the troubleshooting section.

5 Using Nymi Connect

Nymi Connect works out of the box with the majority of web-based and native Windows applications, with no application-specific configuration required. This includes applications delivered through Webswing in a supported browser, such as web-based Manufacturing Execution System (MES) clients. Java-based applications additionally require Java Access Bridge to be enabled (see Enabling Support for Java-Based Applications). The following workflow describes how a user authenticates with their Nymi Band in a login or e-signature window.

Note: Nymi Connect requires network connectivity to NES at the time of each authentication.

Note: Nymi Connect injects credentials into the username and password fields but does not click the submit or login button. The user must click the submit button after credentials are injected.

1. Nymi Connect appears in the system tray. The following table gives messages that can appear when you hover over the icon:

Icon	Status	Message
	Connected with all the required components.	Nymi Connect
	Disconnected from one or more required components.	Troubleshooting Nymi Connect Status Messages provides more information.

   Note: Upon start-up, Nymi Connect initializes components and establishes a connection to the Nymi Agent. When you hover over the Nymi Connect Desktop System Tray icon, the status appears as Nymi Connect - Application initializing. If a user performs a Nymi Band tap in Nymi Connect immediately after installation or a restart, Nymi Connect might not detect the tap until initialization completes.

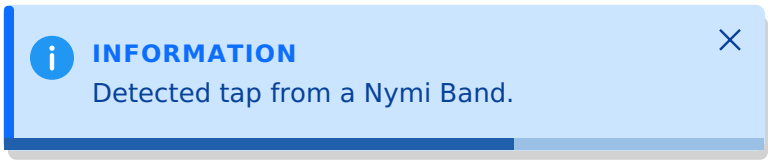
2. User opens the application and navigates to a screen that requires their credentials.

3. User performs a left mouse click on the **Username** field.

   > **Important:** Click into a credential field before tapping the Nymi Band; Nymi Connect injects into the field that has focus. If you click

the username field, Nymi Connect injects the username there and then detects and populates the password field. If you click the password field instead, only the password is injected.

4. User performs an NFC Tap or BLE Tap with their authenticated Nymi Band. A message appears above the Desktop system tray that displays Tap Received - Detected tap from a Nymi Band, as shown in the following figure. A bar along the bottom of the alert fills while it is shown, for about two seconds, and then the alert closes.



5. Nymi Connect retrieves the credentials of the Nymi Band user and populates the username and password fields.

   If credential injection fails, a pop-up appears that displays an error message.

   Troubleshooting Nymi Connect Usage Errors provides more information.

6. The user clicks the **Submit** or **Login** button to complete the authentication.

7. The application authenticates the user credentials and completes the authentication or rejects the authentication.

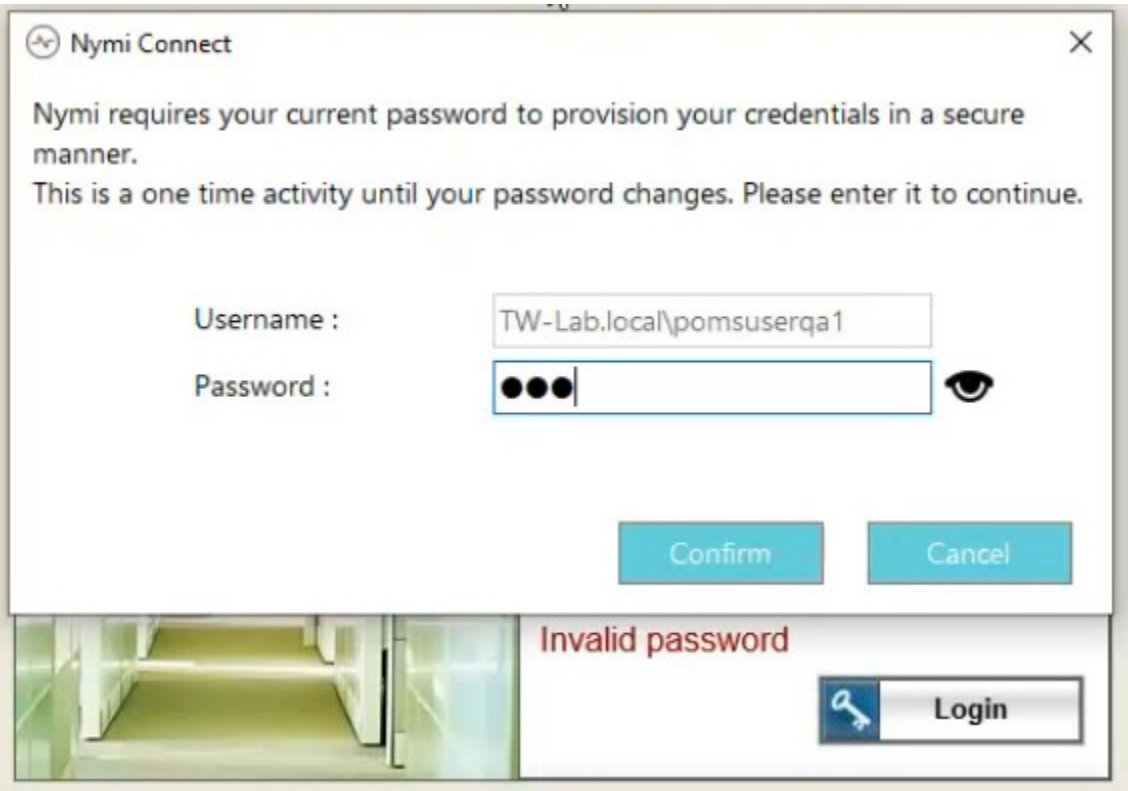
Note: Nymi Connect does not support injection into domain fields. If the application requires a domain, the user must enter it manually.

Note: Passwords are never displayed in clear text during credential injection. Nymi Connect injects password values directly into password-type fields, which display masked characters. The Password Update Form also uses a masked input field.

Note: Nymi Connect supports multi-display environments. Credential injection targets the application window that has focus, regardless of which display it is on.

5.1 Handling Password Changes

After a user changes their password in Active Directory, the first time the user performs a Nymi Band tap to complete an authentication task, Nymi Connect detects that the password has changed, and displays the Password Update Form for the user to supply their new password.



The user should enter their current (new) password, and click **Confirm**. Nymi Connect verifies that the password has been entered correctly, and then displays the following success alert:

SUCCESS
Password update completed successfully.

After a successful password update, the user should select the **Username** field in the application login page again, and perform another Nymi Band tap. Nymi Connect will inject the username and the updated password.

Note: When the user performs the first Nymi Band tap, in addition to displaying the Password Update Form, Nymi Connect also injects the username and the **old** password into the application authentication page. This is normal behaviour for Nymi Connect, since Nymi Connect performs the

password injection and password check simultaneously to optimize response time. If the user clicks the **submit** or **login** button on the application authentication page, the authentication will fail. The user should complete the Password Update Form, and then retry the application authentication.

Note: Nymi Connect may also show the Password Update Form whenever the user's encrypted password is not stored on the Nymi Enterprise Server. The user should follow the same procedure as in the case of password change - supply their current password, and then retry the application authentication.

5.2 Performing Tasks that Require Two E-Signatures

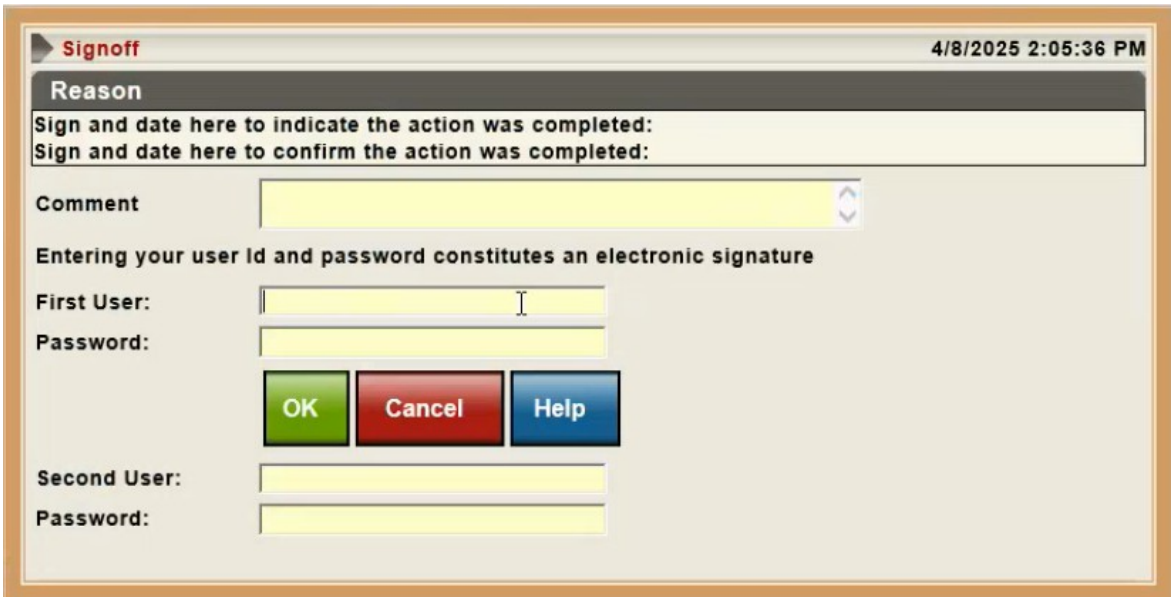
Some tasks require a sign off from two different users (maker-checker). Each tap is an independent credential injection — the first user taps to inject their credentials, then the second user taps to inject theirs.

Note: Nymi Connect does not verify that the two users are different or hold distinct roles. Role enforcement is the responsibility of the target application.

Procedure

1. Perform an operation that requires two e-signatures.
2. The first user performs a left mouse click in the **first username** field.

   The following figure provides an example of a dual e-signature window where the cursor is active in the first username field:



3. The first user performs a Nymi Band tap with their authenticated Nymi Band. Nymi Connect injects the username and password of the first user into the first set of credential fields.

4. The second user performs a left mouse click in the **second username** field.

   The following figure provides an example of a dual e-signature window where the cursor is active in the second username field:



5. The second user performs a Nymi Band tap with their authenticated Nymi Band. Nymi Connect injects the username and password of the second user into the second set of credential fields.

6. The user clicks the **Submit** or **OK** button to complete the operation.

6 Log Files

Nymi Connect generates log files for troubleshooting, performance analysis, and auditing. The NCW Client writes application and profile logs per user session. The Nymi Connect Service (NCS) writes audit logs at the system level.

The following table summarizes the available log files contained in `C:\Nymi\NymiConnectClient\Logs\`:

Log file	Location	Purpose
Application Log	`{USERNAME}\App\ncc_yyyyMMdd.log`	Contains information related to general application behavior and operational activities, including process flow, application events, and errors. Use these logs for troubleshooting.
Profile Log	`{USERNAME}\Profile\ncc_yyyyMMdd.log`	Contains performance information that measures the execution time of each tap-to-injection operation. Daily rotation.

The following table summarizes the available log files contained in `C:\Nymi\NymiConnectService\Logs\`:

Log file	Location	Purpose
Service Log	`App\ncs_yyyyMMdd.log`	Contains information related to the Nymi Connect Service (NCS) application behavior and operational activities. Use these logs for troubleshooting service-level issues.
NCC Log	`Core\core.log`	Contains logging from the Nymi Connect core (NCC), which implements Nymi's cross-platform logic for Nymi Connect. Use these logs for troubleshooting issues in the core logic.
Audit Log	`Audit\ncs_yyyyMMdd.log`	Contains security-relevant events recorded by the Nymi Connect Service (NCS) at the system level. Events include credential injection success and failure, password update,

Log file	Location	Purpose
		and unregistered band taps. Daily rotation.

Note: Application and profile logs are written per user session. Audit logs are written at the system level by NCS and are not per-user.

Note: Log files do not contain passwords, credentials, or personally identifiable information.

6.1 Log File Access Control

The following table describes access control for log files:

Log type	Write access	Read access
Application and Profile	NCW Client process only	All users (read-only), Local System and Administrators (full access)
Audit	NCS process only	All users (read-only), Local System and Administrators (full access)

Note: If log files are missing, verify that Nymi Connect is running and that the NCW Client and NCS processes have write permissions to their respective log directories.

6.2 Centralized Audit Logging

The Nymi Connect Service (NCS) records audit events for security-relevant actions such as credential injection, password update, and authentication failures.

Audit events are written to the centralized audit log table on NES, and also locally on the machine where Nymi Connect is installed, in the directory `C:\Nymi\NymiConnectService\Logs\Audit`.

The following table describes the audit events that NCS records:

Event	Description	Trigger
PasswordAutofillSuccess	Credential injection completed successfully	Tap received, credentials injected
PasswordAutofillFailed	Credential injection failed	

Event	Description	Trigger
		Field not found, timeout, or other injection error
PasswordValidationFailed	Active Directory validation failed	Stored password does not match AD
EncryptedPasswordUpdated	Password updated successfully	User completes password update
EncryptedPasswordRemoved	Password cleared from NES	User cancels password update or invalid password cleared
UnknownAuthenticatorDetected	Unregistered Nymi Band tap	Tap from a band not enrolled in NES

Note: If password autofill fails due to NES being unreachable, the corresponding PasswordAutofillFailed event is written only to the local audit log.

7 Troubleshooting Nymi Connect

This section describes how to troubleshoot Nymi Connect and how to resolve the messages that can appear when you use Nymi Connect and the Nymi Band to complete authentication tasks.

It has two parts:

- How to Troubleshoot Nymi Connect describes how Nymi Connect shows messages, how to read an error code, where to find the log files, and how to restart Nymi Connect.
- Resolving Issues lists specific problems, grouped by when they occur. Each entry gives the message, its error code (where one applies), and how to resolve it.

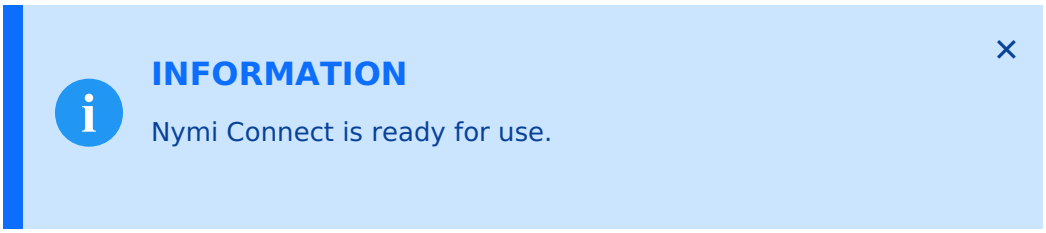
7.1 How to Troubleshoot Nymi Connect

7.1.1 How Nymi Connect Shows Messages

Nymi Connect uses four display mechanisms to communicate with users.

Alert Popup

A custom alert form that appears in the bottom-right corner of the screen. An example of an alert popup looks like this:



Each alert has a **Title** (displayed in uppercase) and a **Message** (displayed below the title). Most alerts auto-fade after 3–7 seconds and do not steal focus.

Each message has a severity:

Severity	Color	Meaning
`ERROR`	Red	A failure that prevents an operation.
`WARNING`	Yellow	A non-critical issue.
`INFORMATION`	Blue	An informational notice.
`SUCCESS`	Green	An operation completed.

If an issue prevents Nymi Connect from becoming ready, the tray icon shows a red cross until the issue is resolved.

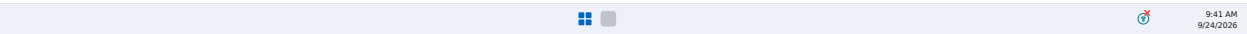


Figure 6. The tray icon with a red cross, shown while an issue prevents Nymi Connect from being ready

While a persistent issue is unresolved, every Nymi Band tap re-displays the alert, so the error code is always available to report to an administrator.

Tray Tooltip

Text shown when hovering over the Nymi Connect system tray icon. An example of the tray tooltip looks like this:



- When connected: `Nymi Connect`
- When disconnected: `Error: <message>`
- When initializing: `Nymi Connect - Application initializing`

> **Note:** The tray tooltip truncates messages longer than 127 characters. The full error message is recorded in the Application Log (see Log File Locations).

Message Box

A modal Windows dialog that blocks interaction until dismissed. Used for startup errors and system dialogs.

Form Status Label

Red or black text on the Password Update Form.

7.1.2 Finding and Reading the Error Code

For the errors introduced for CWP Mode authentication, the alert displays an error code such as `10-030-001`. The same code is recorded in the NCW Client application log (see Log File Locations).

To resolve a problem by its code, find the code in the sections below, where the entry matches the code in question. If an operator reports a code to you, use it to go directly to the matching entry.

7.1.3 Log File Locations

Component	Log Path	File Pattern
NCW Client — App Logs	`C:\Nymi\NymiConnectClient\Logs\{USERNAME}\App\`	`ncc_{yyyyMMdd}.log`
NCW Client — Profile Logs	`C:\Nymi\NymiConnectClient\Logs\{USERNAME}\Profile\`	`ncc_{yyyyMMdd}.log`
NCW Client — Startup Logs	`C:\Nymi\NymiConnectClient\Logs\{USERNAME}\Startup\`	`ncc_{yyyyMMdd}.log`
NCS Service — App Logs	`C:\Nymi\NymiConnectService\Logs\App\`	`ncs_{yyyyMMdd}.log`
NCS Service — Audit Logs	`C:\Nymi\NymiConnectService\Logs\Audit\`	`ncs_{yyyyMMdd}.log`
NCS Service — Profile Logs	`C:\Nymi\NymiConnectService\Logs\Profile\`	`ncs_{yyyyMMdd}.log`
NCS Service — NCC Logs	`C:\Nymi\NymiConnectService\Logs\Core\`	`core.log`

When contacting support, include logs from both the NCW Client and NCS Service directories.

7.1.4 Restarting Nymi Connect

Some problems are resolved by restarting Nymi Connect so that it re-reads a changed setting, such as the NES URL, a root certificate, the active NES policy, or the application lists in `appsettings.json`. For the procedure, see Restart Nymi Connect. Changing the `NYMI_NEA_SUPPORT_LEGACY_MODE` environment variable also requires a restart, but you must sign out of Windows and sign back in, or restart the computer, rather than restart the application.

A Client Registration Token does not require a restart — Nymi Connect detects a new token and switches to CWP Mode on its own.

7.1.5 Tray Icon Context Menu

Right-click the Nymi Connect icon in the Desktop System Tray to access the following options:

Menu Item	Description
Open the Logs Folder	Opens the log directory in Windows Explorer.
Restart	Restarts the NCW Client.

7.2 Resolving Issues

This part lists specific problems, grouped by when they occur: at start-up and while connecting, while provisioning CWP Mode, during tap-to-fill, and while handling passwords. Problems that do not have an error code are grouped under Other Issues.

7.2.1 Start-up and Connection Problems

These problems appear when Nymi Connect starts, or while it is running, and prevent it from connecting to the components it needs.

7.2.1.1 Nymi Connect Service is Not Responding

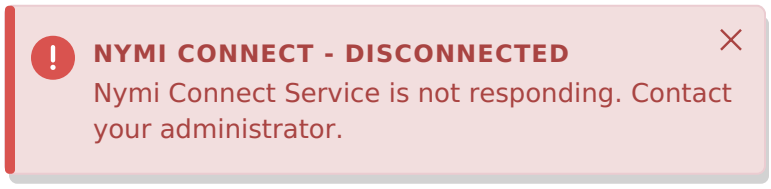


Figure 7. The Nymi Connect Service Not Responding alert

This error appears during Nymi Connect startup, when the user performs a Nymi Band tap, or any time Nymi Connect is running. The tray icon changes to the disconnected state and its tooltip shows the error. The Nymi Connect Service (NCS) Windows Service is stopped, crashed, or unresponsive; the

NCW Client performs periodic health checks against NCS, and this message appears when those checks fail.

1. Open `services.msc` and locate **Nymi Connect Service**.
2. If the service is stopped, start it. If it appears hung, restart it (see Restart Nymi Connect).
3. If the service fails to start, check the NCS Service app log at `C:\Nymi\NymiConnectService\Logs\App\ncs_{yyyyMMdd}.log` for errors.

7.2.1.2 Nymi Connect Cannot Communicate with NES

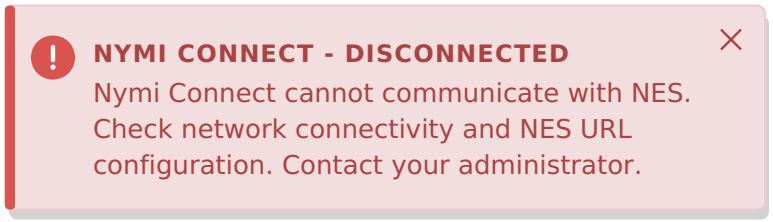


Figure 8. The Cannot Communicate with NES alert

This error appears during Nymi Connect startup, when the user performs a Nymi Band tap, or any time Nymi Connect is running. The tray icon changes to the disconnected state and its tooltip shows the error. Nymi Connect cannot reach the Nymi Enterprise Server (NES); the cause is one of the following.

Network connectivity or DNS issues	The user terminal cannot reach the NES server because of network or DNS resolution failures. 1. Verify that the NES server hostname resolves correctly using `nslookup <NES hostname>` on the user terminal. 2. If DNS is failing, correct the DNS configuration or add a host entry for the NES server. 3. Verify that the NES server is reachable using `ping` or `Test-NetConnection`. 4. If the connectivity check fails, verify that Windows Firewall and the network firewall allow connections from the Nymi Connect host to TCP port 443 on the NES server. 5. Once all issues are resolved, Nymi Connect automatically reconnects after a few minutes.
Expired or misconfigured TLS certificate	The TLS certificate on NES has expired, or there are IIS configuration issues. 1. Confirm the expiration date of the TLS certificate and replace it as required. The Nymi Connected Worker Platform—Troubleshooting Guide provides more information. 2. Review the IIS configuration. The Nymi Connected Worker Platform—Deployment Guide provides more information. 3. Once all issues are resolved, Nymi Connect automatically reconnects after a few minutes.
NES application or service is not running	The NES application or its underlying services (IIS, SQL Server) are stopped on the NES server. 1. On the NES server, verify that the IIS web server and NES application pool are running. 2. Verify that the SQL Server instance used by NES is running. 3. Restart the NES application pool or IIS if needed. 4. Once all issues are resolved, Nymi Connect automatically reconnects after a few minutes.

NES URL in registry is incorrect or missing	The NES URL registry key is not present or contains an incorrect value. Nymi Connect reads the NES URL from the registry during startup. 1. On the user terminal, run `regedit.exe` and navigate to **HKLM > Software > Nymi > NES**. 2. Verify that the NES URL registry key exists and contains the correct NES server URL. 3. If the key is missing, create it with the correct value. 4. Restart Nymi Connect (see Restart Nymi Connect).
Root certificate missing	The Root CA certificate is missing on the user terminal. This may happen if the NES TLS certificate is issued using a private Root CA or an enterprise Root CA. 1. Confirm that the Root CA certificate is missing: open the NES URL in a web browser on the user terminal. If the browser shows a “Connection is not secure” warning, the Root CA certificate is missing. 2. Import the Root CA certificate on the user terminal. 3. Restart Nymi Connect (see Restart Nymi Connect).

Computer is not domain joined (AD Mode)	In AD Mode, the user terminal is not joined to the Active Directory domain, so Nymi Connect cannot obtain the Negotiate authentication token that NES requires in AD Mode. 1. Verify that the user terminal is joined to the same domain as the NES server, or to a domain that has a trust relationship with the NES machine's domain. 2. If the machine was recently joined to the domain, restart the user terminal. 3. Restart Nymi Connect (see Restart Nymi Connect). Alternatively, provision the device in CWP Mode, which authenticates to NES with a Client Registration Token and does not require the computer to be domain joined. CWP Mode requires Connected Worker Platform 1.20.1 or later, and Legacy Mode must be turned off (set `NYMI_NEA_SUPPORT_LEGACY_MODE` to `0`). See Provisioning CWP Mode.

7.2.1.3 Nymi Connect Cannot Communicate with the Nymi Agent

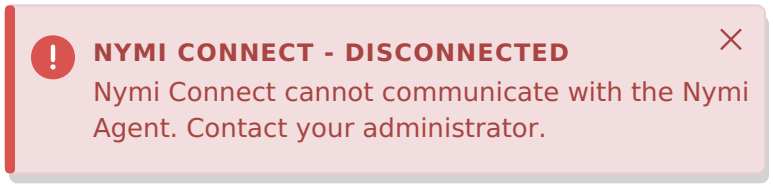


Figure 9. The Cannot Communicate with the Nymi Agent alert

This error appears during Nymi Connect startup, or any time Nymi Connect is running. The tray icon changes to the disconnected state and its tooltip shows the error. Nymi Connect cannot reach the Nymi Agent; the cause is one of the following.

Centralized Nymi Agent server is unreachable	Nymi Connect cannot connect to the centralized Nymi Agent server. 1. Confirm that the status of the Nymi Agent service is **Running** on the centralized Nymi Agent server. Start or restart the Nymi Agent service if necessary. 2. On the machine where Nymi Connect is installed, run `regedit.exe` and navigate to **HKLM > Software > Nymi > NES**. Ensure that the `AgentURL` registry key correctly defines the Nymi Agent server. 3. Verify that Windows Firewall and the network firewall allow connections from the Nymi Connect host to TCP port 9120 on the Nymi Agent server. The **Network connectivity or DNS issues** steps under Nymi Connect Cannot Communicate with NES provide general network diagnostics that are also worth trying when the Nymi Agent server cannot be reached.
Local Nymi Agent not running	In a local Nymi Agent configuration, the Nymi Agent service is not running on the user terminal. Start the Nymi Agent service on the user terminal.
Nymi Runtime not installed	The Nymi Runtime software was not installed when Nymi Connect runs on the user terminal. Install the Nymi Runtime software on the user terminal.

7.2.1.4 Nymi Bluetooth Endpoint Service is not Running

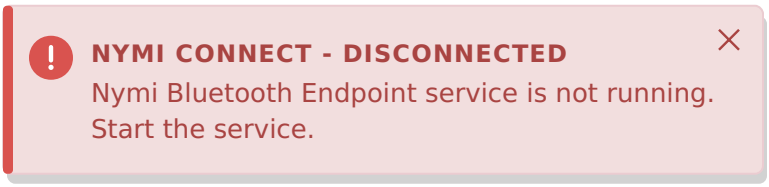


Figure 10. The Nymi Bluetooth Endpoint not running alert

This error appears during Nymi Connect startup, or any time Nymi Connect is running. The tray icon changes to the disconnected state and its tooltip shows the error. The cause is one of the following.

Nymi Bluetooth Endpoint service is not running	The Nymi Bluetooth Endpoint service is stopped. 1. On the user terminal, launch the Services control panel (`services.msc`), and start the **Nymi Bluetooth Endpoint** service. 2. If the service does not appear, run the Nymi Runtime installer and choose to install the Nymi Bluetooth Endpoint component only.
nbe.toml misconfiguration	The `nbe.toml` configuration file is pointing to the wrong Nymi Agent. 1. On the user terminal, open `C:\Nymi\Bluetooth_Endpoint\nbe.toml` and verify the `agent_url` parameter. Set it to match the deployment: a local Nymi Agent, or the correct remote Nymi Agent server. 2. If you change `agent_url`, restart the Nymi Bluetooth Endpoint service for the change to take effect.
IP address on the user terminal has changed	The IP address of the user terminal has changed. 1. Restart the Nymi Bluetooth Endpoint service on the user terminal. 2. Right-click the Nymi Connect icon in the System Tray and select **Restart**.

Multiple IP addresses on the user terminal	The user terminal has multiple IP addresses, which can cause Nymi Connect to subscribe to the Nymi Bluetooth Endpoint at the wrong IP address, when a centralized Nymi Agent is used. 1. Ensure that the user terminal has only one IP address, for example by disabling unused network adapters. 2. Right-click the Nymi Connect icon in the System Tray and select **Restart**. If you cannot reduce the terminal to a single IP address, set the `ENDPOINT_ID_MODE` system environment variable so the Nymi Bluetooth Endpoint is identified by hostname (or hostname and IP address) instead of IP address, then restart the computer. See Setting the Nymi Bluetooth Endpoint ID Format in the Nymi Connected Worker Platform—Deployment Guide.

7.2.1.5 Nymi Bluetooth Adapter is Missing

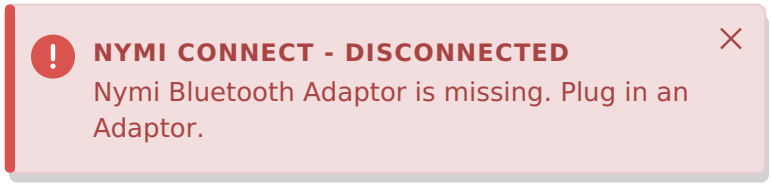


Figure 11. The Nymi Bluetooth Adapter missing alert

This error appears during Nymi Connect startup, or any time Nymi Connect is running. The tray icon changes to the disconnected state and its tooltip shows the error. The Nymi Bluetooth adapter is not plugged in or not detected by the system.

1. Plug a Nymi-provided Bluetooth Adapter into a USB port on the user terminal.
2. Try a different USB port if the adapter is not detected.
3. Check Device Manager for the adapter and verify drivers are installed.
4. Replace the adapter if it is physically damaged.

7.2.1.6 Nymi Connect Stays in Application Initializing

In CWP Mode, Nymi Band taps do not work, and when you hover over the Nymi Connect tray icon the status remains Nymi Connect - Application initializing. This can happen when Legacy Mode is still enabled: the `NYMI_NEA_SUPPORT_LEGACY_MODE` system environment variable is not set to `0` on the machine, so Nymi Connect uses the pre-CWP 1.15 communication protocol instead of the current protocol.

1. On the machine where Nymi Connect is installed, set the system environment variable `NYMI_NEA_SUPPORT_LEGACY_MODE` to `0`. The Nymi Connected Worker Platform—Deployment Guide describes this in "Configuring the Connected Worker Platform Communication Protocol."
2. Sign out of Windows and sign back in, or restart the computer, so the NCW Client starts with the new value.

7.2.1.7 Nymi Connect Feature is Disabled

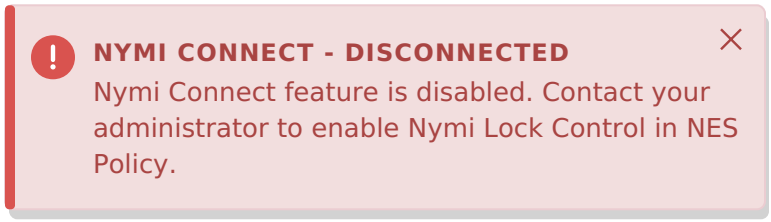


Figure 12. The Nymi Connect Feature Disabled alert

This error appears during Nymi Connect startup. The tray icon changes to the disconnected state and its tooltip shows the error. The active NES policy does not have the Lock Control feature enabled.

1. Log into the NES Administrator Console.
2. Edit the active policy. In the **Lock Control** section, select the **Enable Nymi Lock Control** option.
3. Click **Save**.
4. Restart Nymi Connect (see Restart Nymi Connect).

7.2.1.8 appsettings.json File is Missing

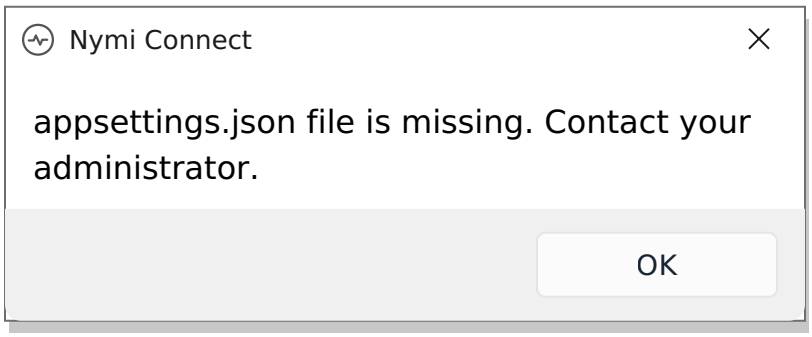


Figure 13. The appsettings.json file missing message box

When a user logs in to Windows, or manually starts or restarts Nymi Connect, an error dialog box appears with the message `appsettings.json file is missing. Contact your administrator.` The tray icon changes to the disconnected state. The `appsettings.json` file is missing.

Restore the `appsettings.json` file from a backup or reinstall Nymi Connect, then restart the application.

7.2.1.9 Configuration Error (Data Structure) in appsettings.json

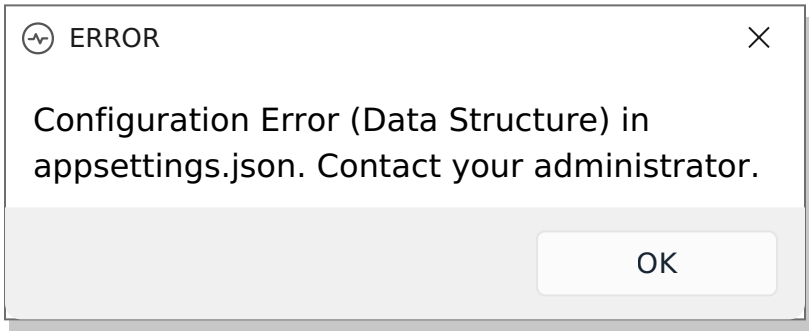


Figure 14. The appsettings.json configuration error message box

When a user logs in to Windows, or manually starts or restarts Nymi Connect, an error dialog box appears with the message `Configuration Error (Data Structure) in appsettings.json. Contact your administrator.` The tray icon changes to the disconnected state. There is a syntax error in the `appsettings.json` file.

Correct the `appsettings.json` file, and then restart Nymi Connect. Common configuration considerations include:

- Ensure the file contains valid JSON syntax.
- Each line should end with a comma (`,`) except for the last line before a closing `}`.
- Verify that all required settings are populated.
- Check the NCW Client app log for the specific error.

7.2.1.10 log4net.config File is Missing

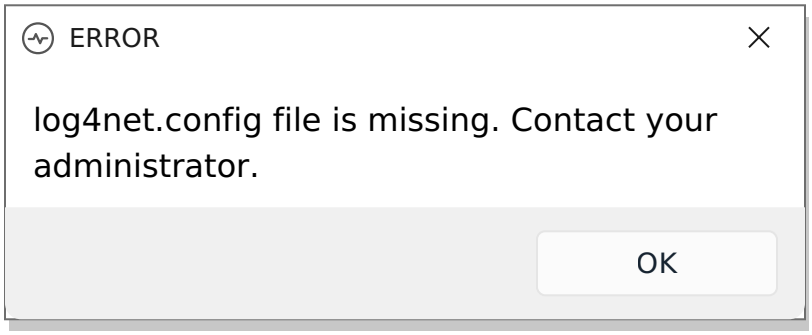


Figure 15. The log4net.config file missing message box

Nymi Connect shows the error `log4net.config file is missing. Contact your administrator.` in a message box, and the tray icon shows the error state. The `log4net.config` logging configuration file is not found in the installation directory.

Reinstall Nymi Connect or restore the `log4net.config` file from a known good installation, then restart the application.

7.2.1.11 Configuration Error in log4net.config

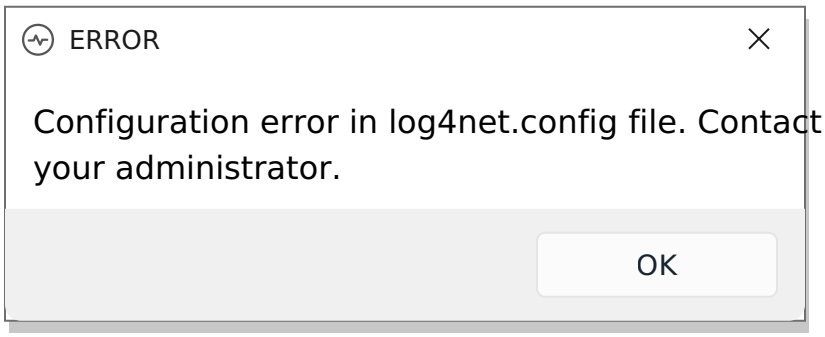


Figure 16. The log4net.config configuration error message box

Nymi Connect shows the error `Configuration error in log4net.config file. Contact your administrator.` in a message box, and the tray icon shows the error state. The `log4net.config` file is present but contains invalid XML syntax.

Correct the invalid XML in the `log4net.config` file, then restart Nymi Connect.

7.2.1.12 Nymi Connect Cannot Initialize

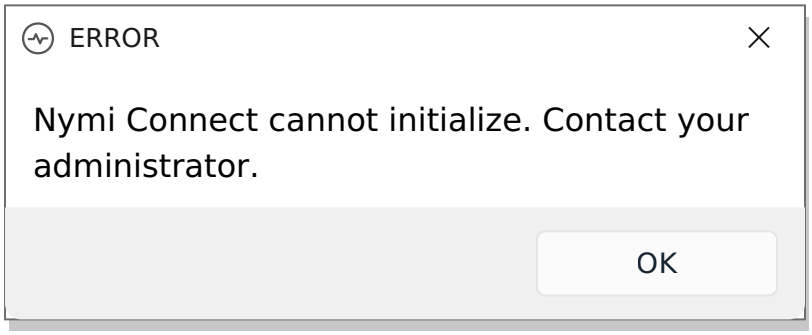


Figure 17. The Nymi Connect cannot initialize message box

Nymi Connect shows the error `Nymi Connect cannot initialize. Contact your administrator.` in a message box, and the tray icon shows the error state. An unexpected error occurred during application startup that does not fall into the categories above.

Check the NCW Client app log at `C:\Nymi\NymiConnectClient\Logs\{USERNAME}\App\` for the root cause exception. If the problem is unresolved, contact Nymi Support with the log files.

7.2.1.13 Nymi Connect is Already Running

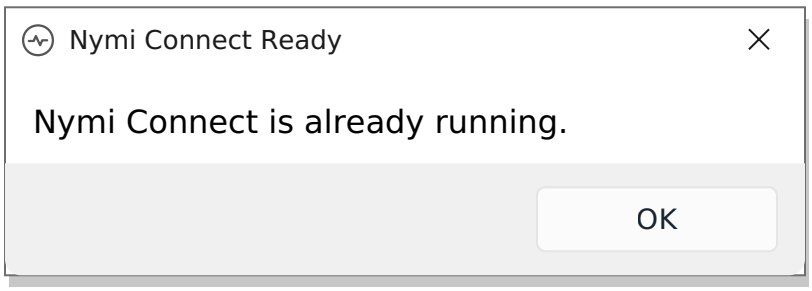


Figure 18. The Nymi Connect is already running message box

This error appears when a user starts Nymi Connect. Only one instance of Nymi Connect can run in each user session.

Click **OK**. View the System Tray and confirm that Nymi Connect is not already started. If no icon is visible, open Task Manager, end any existing `nymi_connect.exe` process, and then relaunch Nymi Connect.

7.2.2 CWP Mode Provisioning Problems

These errors can appear while a device is being provisioned in CWP Mode, or later if its registration with NES stops being valid. Unlike other Nymi Connect alerts, these errors carry an error code: the alert shows the error's title and instruction, with **Details** that you open to see the code, the detailed message, and a **Copy details** button. The alert stays until you close it, and a persistent error also marks the tray icon with a red cross until Nymi Connect is ready. See Provisioning CWP Mode.

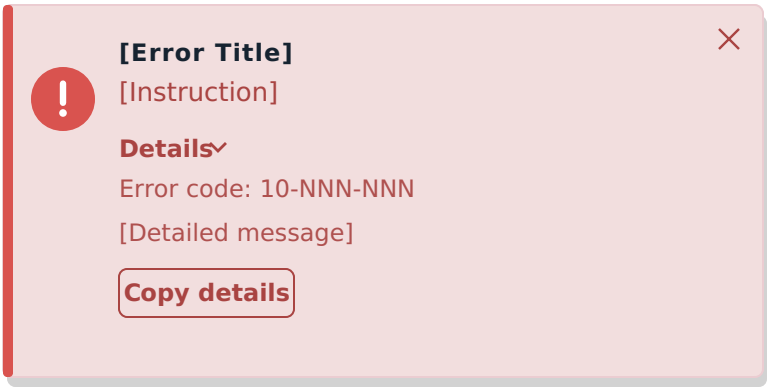


Figure 19. An error alert for a CWP Mode error, with Details open to show the code and detailed message

The entries below give each error by its code; use the code to identify the problem and to report it to your administrator.

7.2.2.1 Nymi Connect isn’t set up on this device

Nymi Connect shows `Nymi Connect isn't set up on this device` when it could not register with NES, or could not finish configuring CWP Mode. The detailed message identifies the cause.

Client registration failed: client registration token has expired (10-030-001)	Generate a new token in NES and provision the device again.
Client registration failed: client registration token is revoked (10-030-002)	The token was revoked in NES. Generate a new token and provision the device again.

Client registration failed: client registration token has reached its usage limit (10-030-003)	Increase the token’s client limit, or generate a new token, and provision the device again.
Client registration failed: client registration token is not recognized (10-030-004)	Confirm that the token file came from this NES, then provision the device with a valid token.
Cannot authenticate with Nymi Enterprise Server: invalid client (10-030-008)	The client’s registration is no longer valid in NES. Provision the device again with a valid token.
Client registration failed: the client registration token is invalid (10-030-010)	Confirm the token file is complete and unmodified, then provision the device again.
Nymi Connect is not configured (10-060-001)	The device has not been provisioned. Provision the device with a Client Registration Token.
No client credentials or CRT were found (10-060-007)	Provide a new Client Registration Token and provision the device.

> **Note:** To create, view, revoke, or confirm tokens and clients in the NES Administrator Console, see the Nymi Connected Worker Platform—Administration Guide.

7.2.2.2 Nymi Connect can’t use this configuration

Nymi Connect found a configuration file but could not use it. The detailed message identifies the cause.

Configuration data was rejected (10-060-006)	Confirm that you placed the intended token file, then provision the device again.
Configuration data was rejected: data is malformed (10-060-008)	The `nymi.ncconf` file is not valid. Generate the token again, save a fresh `nymi.ncconf` file, and provision the device again.
Configuration data was rejected: one or more settings contain an invalid value (10-060-009)	Generate the token again, save a fresh `nymi.ncconf` file, and provision the device again.

7.2.2.3 Nymi Connect encountered an error on the server

Nymi Connect shows `Nymi Connect encountered an error on the server` when NES reports an internal error during registration.

Client registration failed: internal error in Nymi Enterprise Server (10-030-005)	NES reported an internal error while registering the device. Try again later. If this continues, contact your administrator.

7.2.3 Tap-to-Fill Problems

These problems appear when a user taps their Nymi Band to fill in a login or e-signature window.

7.2.3.1 Nymi Connect Does Not Detect Nymi Band Tap

A user performs a Nymi Band tap in the username and password window, but Nymi Connect does not detect the tap operation. The cause is one of the following.

Nymi Connect cannot communicate with the Nymi Agent	Refer to Nymi Connect Cannot Communicate with the Nymi Agent for resolution.
Nymi Connect cannot communicate with the Nymi Bluetooth Endpoint	Refer to Nymi Bluetooth Endpoint Service is not Running for resolution.
Nymi Bluetooth Adapter is missing	Refer to Nymi Bluetooth Adapter is Missing for resolution.
NFC reader issue	(When NFC tap is used) The NFC reader is not connected to the user terminal, is not recognized by the system, or is malfunctioning. 1. Verify that the NFC reader is plugged into a USB port on the user terminal. 2. Check Device Manager to confirm the NFC reader is recognized and drivers are installed. 3. Try a different USB port. 4. Replace the NFC reader if it is malfunctioning. 5. If the NFC reader is connected and recognized, try performing a BLE tap instead to confirm that the issue is specific to NFC.

Bluetooth adapter issue	(When BLE tap is used) The Bluetooth adapter is not connected to the user terminal, is not recognized by the system, or is malfunctioning. 1. Verify that the Bluetooth adapter is plugged into a USB port on the user terminal. 2. Check Device Manager to confirm the Bluetooth adapter is recognized and drivers are installed. 3. Try a different USB port. 4. Replace the Bluetooth adapter if it is malfunctioning. 5. If the Bluetooth adapter is connected and recognized, try performing an NFC tap instead to confirm that the issue is specific to Bluetooth.
Disconnecting an RDP or Citrix session and reconnecting from a different user terminal	If the user disconnects from an RDP or Citrix session without logging out of the session, and then launches RDP or Citrix again from a different user terminal, the existing, disconnected session is reused. Nymi Connect expects the user to be at the original user terminal, so it cannot detect Nymi Band taps at the new user terminal. Instruct the user to log out of the RDP or Citrix session, and then start a new session.
Application is on the suppressed list	The application that has focus at the time of the Nymi Band tap is configured in the `suppressed` list in `appsettings.json`. When a process is suppressed, Nymi Connect takes no action — no credential injection, no notification, and no error message. 1. If the application should not be suppressed, remove it from the `suppressed` list in `C:\Nymi\NymiConnectClient\appsettings.json` and restart Nymi Connect. 2. If the application is intentionally suppressed, use an alternative authentication method for that application.

7.2.3.2 Nymi Connect Cannot Find a User Associated with This Nymi Band in NES

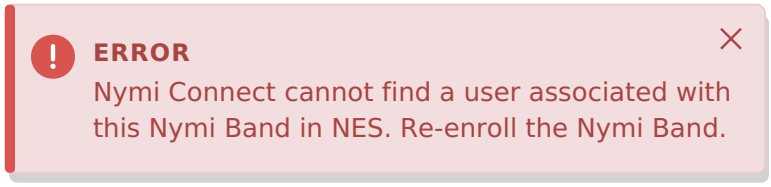


Figure 20. The Nymi Band not found in NES alert

This error appears when a user performs a Nymi Band tap. The tapped Nymi Band is not enrolled in NES, or its enrollment data has been deleted from the server.

1. Re-enroll the Nymi Band using the Nymi Band Application.
2. Verify the enrollment completed successfully.

7.2.3.3 Nymi Connect Has Detected a Nymi Band with an Incomplete Enrollment

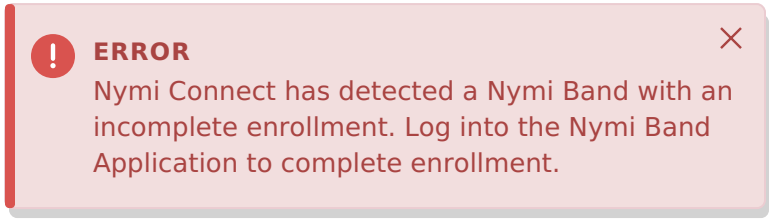


Figure 21. The incomplete enrollment alert

This error appears when a user performs a Nymi Band tap. The Nymi Band does not have the key needed for encrypting and decrypting the user password. This can occur when the Nymi Band enrollment did not complete, for example because the Nymi Band Application lost Bluetooth connectivity with the Nymi Band during enrollment.

1. Instruct the user to log in to the Nymi Band Application while they wear their authenticated Nymi Band and allow the enrollment to complete.
2. Instruct the user to perform the Nymi Band tap again.

7.2.3.4 Nymi Connect Cannot Detect the Username or Password Field

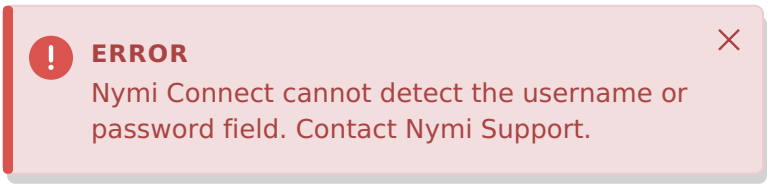


Figure 22. The Cannot Detect the Username or Password Field alert

This error appears when a user performs a Nymi Band tap. The cause is one of the following.

Username field is not selected	No text field is selected at the time of the Nymi Band tap. Instruct the user to click their mouse in the **username** field, and then perform the Nymi Band tap.
The active window is not a login or e-signature screen	The active window is not a login screen or an e-signature screen — a password field is not present. Instruct the user to navigate to the login or e-signature screen, click their mouse in the **username** field, and then perform the Nymi Band tap.
Interference from browser autofill	Autofill is enabled in the browser. When the user clicks on the username field, the browser may show autofill suggestions. If the user moves the mouse at this point, the username text box may no longer be in focus. Instruct the user to click on the username field again, not move the mouse, and perform a Nymi Band tap again. Alternatively, disable autofill in the browser.

7.2.3.5 Active Window Changed During Sign-In

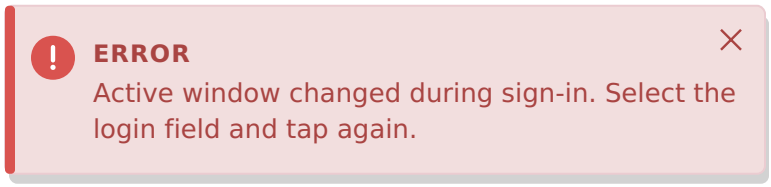


Figure 23. The Active Window Changed alert

This error appears when the active (foreground) window changes between the time the user taps their Nymi Band and the time Nymi Connect injects the credentials. The user or the system changed the active window during sign-in — for example, the user clicked another window or moved the mouse off the login field, or a system pop-up took focus. Nymi Connect injects credentials into the field that has focus, so it stops when the target window is no longer active.

Select the login (username) field again, and perform the Nymi Band tap again. Do not click elsewhere or move the mouse off the field after tapping until the credentials are injected.

7.2.3.6 Sign-in Timed Out

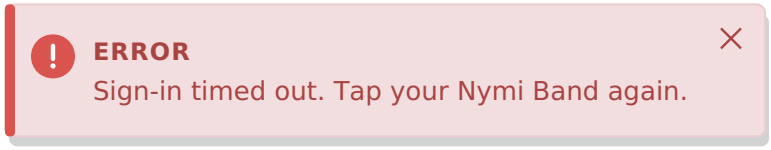


Figure 24. The Sign-in Timed Out alert

Nymi Connect shows `Sign-in timed out. Clear any text that was filled in, then tap your Nymi Band again.` when it cannot locate the password field within the allowed time after a Nymi Band tap. This is more likely on application screens that contain a large number of fields and other elements, which take longer for Nymi Connect to scan.

Select the login field and perform the Nymi Band tap again. A repeat attempt usually completes faster. If the timeout occurs consistently on the same screen, contact Nymi Support.

7.2.3.7 Nymi Connect Cannot Detect Fields in a Java Application

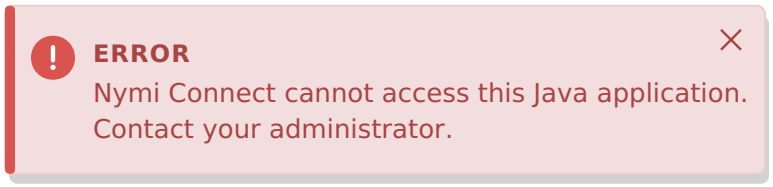


Figure 25. The Java Application Inaccessible alert

Nymi Connect shows `Nymi Connect cannot access this Java application. Contact your administrator.` when it cannot read the UI fields of a Java-based application: no credentials are injected after a Nymi Band tap. The cause is one of the following.

Java Access Bridge is not enabled	Java applications do not expose their fields to the Windows accessibility layer unless Java Access Bridge is enabled for the application's JRE. 1. Confirm Java Access Bridge is enabled for the JRE used by the application, as described in Enabling Support for Java-Based Applications. Nymi Connect records in its log when Java Access Bridge is not enabled. See Log File Locations. 2. Enable it for the JRE the application actually uses. On a machine with more than one JRE, it is easy to enable Java Access Bridge for a different JRE than the application runs on; use the check in the next cause to confirm which JRE the application loads. 3. Restart the Java application after enabling Java Access Bridge. The JVM loads the Access Bridge only at start-up, so the change does not take effect until the application is restarted. 4. Confirm the JRE actually includes Java Access Bridge. A custom or stripped-down runtime can omit it; check that `jabswitch` and the Access Bridge libraries are present in the JRE's `bin` folder. If they are missing, Java Access Bridge cannot be enabled for that runtime.

Another product has claimed the Java accessibility interface	Another product on the operating system (for example, Evidian EAM) has registered its own Java accessibility provider for the JVM. A JVM loads its accessibility provider from a single `assistive_technologies` setting, so the other product can displace the standard Access Bridge that Nymi Connect requires — even when Java Access Bridge appears to be enabled. Determine which accessibility provider the application's JVM actually loads, then remove the conflicting one.
	
	1. Identify the JRE the application uses (a system JRE, or a JRE bundled with the application). In a Command Prompt, list the Java installations on the PATH:
	
	`where java`
	
	A bundled JRE is usually not on the PATH. To find every `java.exe` on the machine, run the following in Windows PowerShell:
	
	`Get-ChildItem C:\ -Filter java.exe -Recurse -ErrorAction SilentlyContinue | Select-Object FullName`
	
	2. In the Command Prompt, change to the JRE's `bin` folder, for example:
	
	`cd "C:\ProgramData\<Vendor>\<App>\jre\bin"`
	
	3. Run the following command to check which accessibility provider the JVM resolves:
	
	`java -XshowSettings:properties -version 2>&1 | findstr /i "assistive JAVA_TOOL_OPTIONS"`
	
	A `Picked up JAVA_TOOL_OPTIONS:` line that contains `-Djavax.accessibility.assistive_technologies=` means an environment variable is forcing an accessibility provider into every

JVM. This setting overrides any `accessibility.properties` file. If `javax.accessibility.assistive_technologies` is listed with a value other than `com.sun.java.accessibility.AccessBridge`, a different (non-Nymi) provider is loaded.

4. Check the accessibility configuration files for a non-standard provider (a provider set through a file does not always appear in the previous step). Check the JRE-level (system-wide) file first, then the per-user file. Check the `assistive_technologies` line in `accessibility.properties`, which should read `com.sun.java.accessibility.AccessBridge`; a different class name indicates another product has claimed the accessibility interface. For Java 8 the file is at `<install-folder>\lib`; for Java 9 and later it is at `<install-folder>\conf`; the per-user file (`.accessibility.properties` in the user's home folder, if present) takes precedence over the JRE-level file in all versions.

If the checks show another provider, disable that product's Java accessibility function (see Resolving Conflicts with Other Java Accessibility Clients), then ensure Java Access Bridge is enabled for the JRE and restart the application.

7.2.3.8 Nymi Connect is not Configured for This Application

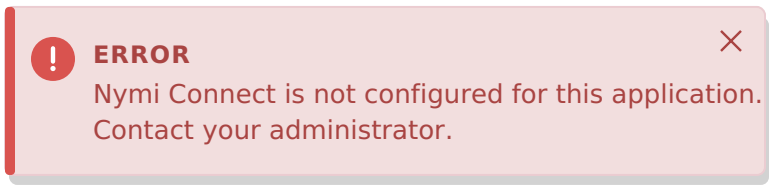


Figure 26. The Application Not Configured alert

This error appears when a user performs a Nymi Band tap. Nymi Connect has been configured with an explicit list of allowed applications, and the application that is active at the time of the Nymi Band tap is not on the list.

Before performing the Nymi Band tap, ensure that the target application is the active window. If the application should be allowed for use with Nymi Connect, contact your administrator to add it to the list.

7.2.3.9 Internal Error. Please Retry

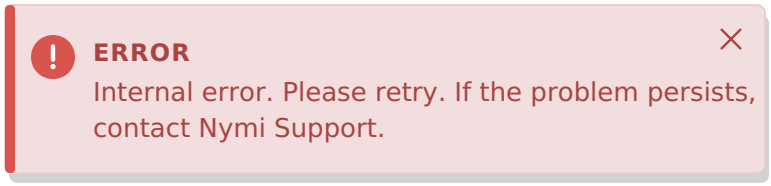


Figure 27. The Internal Error alert

Nymi Connect shows `Internal error. Please retry. If the problem persists, contact Nymi Support.` when decrypting the stored password returns an empty or invalid password after a Nymi Band tap.

1. Retry the Nymi Band tap.
2. If the error persists, check the NCW Client app log at `C:\Nymi\NymiConnectClient\Logs\{USERNAME}\App\ncc_{yyyyMMdd}.log`.
3. Contact Nymi Support with the log files if the problem is unresolved.

7.2.4 Password Problems

7.2.4.1 Password Injection Succeeds but Login or E-Signature Fails

The user performs a Nymi Band tap, and credentials are injected into the username and password fields. However, when the user clicks **Submit** or **Login**, the application rejects the credentials. The cause is one of the following.

Active Directory password has changed	The password stored in Nymi infrastructure does not match the user's current Active Directory password. This can occur after a recent password change. Nymi Connect typically displays the Password Update Form soon after the credential injection. 1. Complete the Password Update Form following the on-screen instructions. 2. In the login or e-signature window, select the username field, and perform another Nymi Band tap. Nymi Connect injects the username and the correct password.
Application requires additional fields	The target application requires fields beyond username and password (for example, a domain field or a database name) that Nymi Connect does not populate. Instruct the user to manually enter any additional required fields before or after the Nymi Band tap, and then click **Submit**.
The user is not authorized to perform the action	The correct username and password are provided by Nymi Connect, but the user is not authorized to perform the requested action. Nymi Connect is only responsible for injecting the username and password, and is not involved in any application-level authorization decisions. Contact the application administrator to resolve any authorization issues.

7.2.4.2 Password Validation Errors

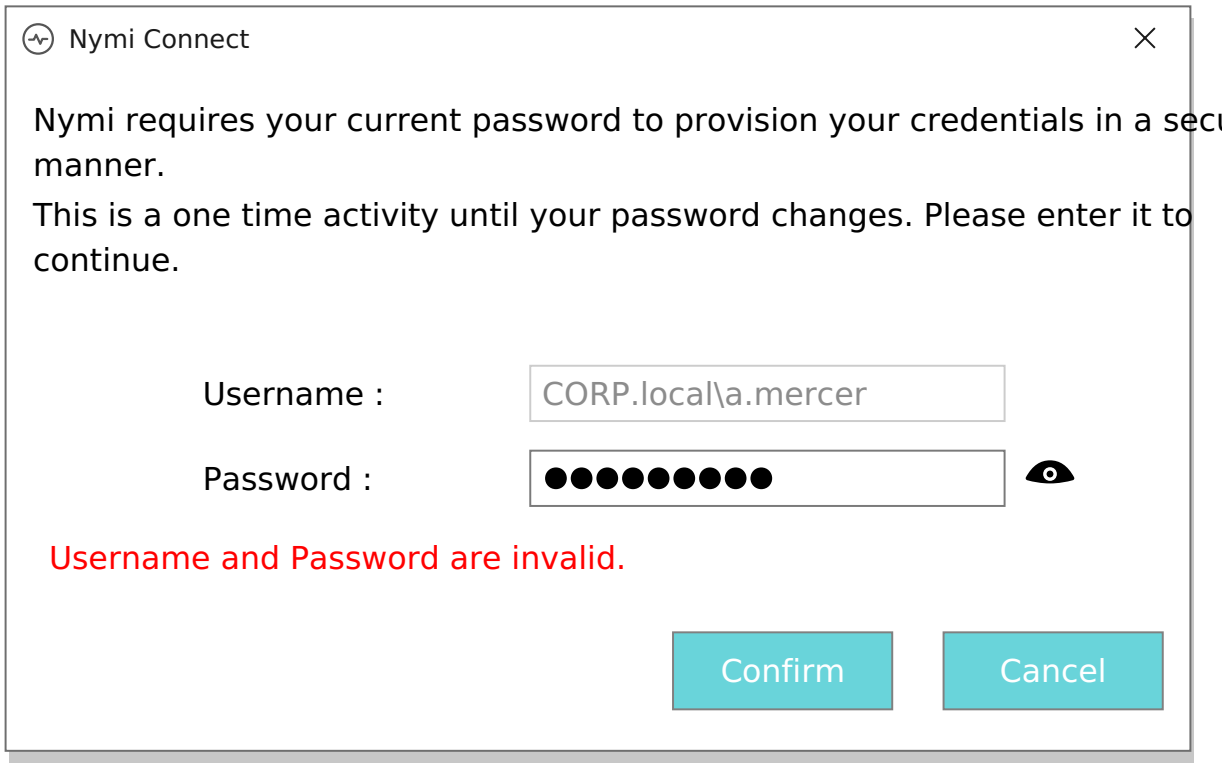


Figure 28. The Password Update Form showing a credential error

When a user types their username and password on the Nymi Connect password prompt and clicks **Confirm**, Nymi Connect validates the credentials against Active Directory. If validation fails, the prompt shows one of the following messages:

Message	Cause	Resolution
`Your user account is locked. Contact your administrator.`	The user's Active Directory account is locked, typically after too many failed login attempts.	Contact your administrator to unlock the account in Active Directory, then perform the Nymi Band tap again.
`Your password has expired. Change your password and then try again.`	The user's Active Directory password has expired.	Change the password in Active Directory, enter the new password in the Nymi Connect Password Update Form, then perform the Nymi Band tap again.
`Your user account has expired. Contact your administrator.`	The user's Active Directory account has expired.	Contact your administrator to renew the account in Active Directory.

Message	Cause	Resolution
`This account is disabled. Contact your administrator.`	The user's Active Directory account is disabled.	Contact your administrator to re-enable the account in Active Directory.
`This account does not exist. Contact your administrator.`	The user's account was not found in Active Directory.	Contact your administrator to verify that the account exists in Active Directory.
`Account status cannot be determined. Contact your administrator.`	Nymi Connect could not determine the status of the user's Active Directory account, which may indicate a connectivity issue with Active Directory.	Verify network connectivity to Active Directory. If the problem persists, contact your administrator.

7.2.4.3 Password Update Errors

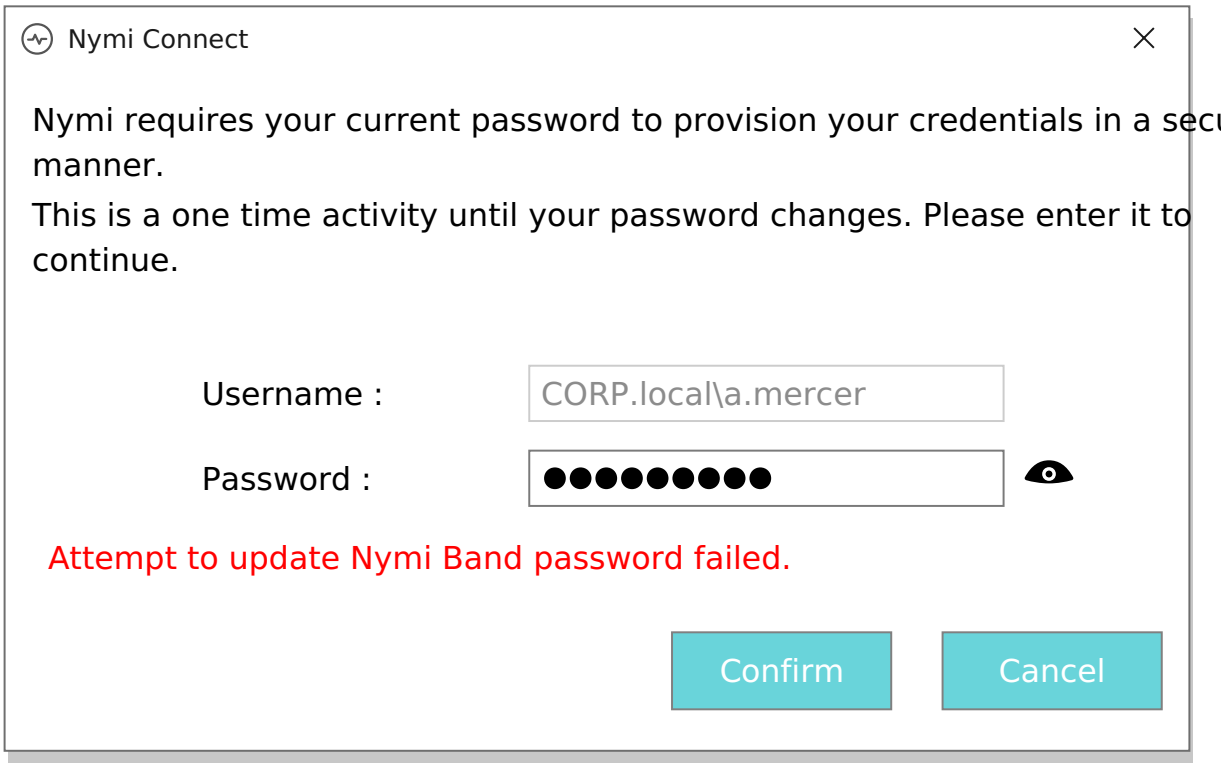


Figure 29. The Password Update Form after a failed update

When a user enters a password on the Password Update Form and clicks **Confirm**, the form may show one of the following messages:

Message	Cause	Resolution
`Password cannot be empty.`	The user clicked **Confirm** without entering a password.	Enter the current domain password in the field and click **Confirm**.
`Attempt to update Nymi Band password failed.`	The API calls to update the encrypted password on NES failed, which may be due to a network issue, an NES error, or a band communication problem.	Do the following: **a.** Check network connectivity to NES **b.** Verify the entered password is correct **c.** Retry the password update operation **d.** If the problem persists, check the NCW Client app log at `C:\Nymi\NymiConnectClient\Logs\{USERNAME}\App\ncc_{yyyyMMdd}.log`

7.2.5 Other Issues

7.2.5.1 Nymi Connect Detects Spurious Nymi Band Tap

Nymi Connect detects a Nymi Band tap when the user is not performing a Nymi Band tap, and displays a tap notification, often followed by an error notification such as Nymi Connect is not Configured for This Application or a request to reselect the username field. These spurious Nymi Band taps may be detected occasionally, or several of them may be detected in quick succession. The Bluetooth adapter or the NFC reader is placed too close to the user's wrist where the Nymi Band is worn.

1. Move the Bluetooth or NFC reader to a different location, further away from the user's wrist.
2. Use a different USB port.
3. Use a USB extension cable to move the NFC reader or the Bluetooth adapter further away from the user's wrist.

8 Upgrading Nymi Connect

Nymi Connect supports in-place upgrades. You do not need to uninstall the previous version before installing a new version. The upgrade process preserves existing configuration files and log files.

Note: Administrative privileges are required to perform an upgrade.

8.1 Upgrading with the Installation Wizard

1. Double-click the new version of the Nymi Connect installer.
2. Follow the installation wizard prompts. The installer detects the existing installation and performs an in-place upgrade.
3. After the upgrade completes, verify that the Nymi Connect icon appears in the system tray.

8.2 Upgrading Silently

1. Run a Command Prompt as administrator.
2. Type the following command, replacing `<version>` with the version in the installer's file name:

```
"Nymi Connect Installer-<version>.exe" /exenoui /q
```

Note: If you use management software to push the upgrade to user terminals, you will need to restart the user terminal to ensure that all components initialize correctly.

Note: Existing log files in the previous log location are not migrated to the new location. Previous logs remain accessible at the old path for reference.

Note: Nymi Connect requires Connected Worker Platform (CWP) 1.20.0 or later; the CWP Mode for component authentication requires CWP 1.20.1 or later. See Supported Connected Worker Platform Versions.

9 Uninstalling Nymi Connect

Perform the following actions to remove the Nymi Connect application.

9.1 Uninstalling with the Installation Wizard

1. From Add or Remove Programs, select **Nymi Connect**, and then click Uninstall.
2. When prompted, click **Uninstall**.
3. On the Modify Setup window, click **Uninstall**.
4. On the User Account Control window, click **Yes**.
5. On the **Uninstall Complete** window, click **Close**.

> **Note:** By default, the uninstaller removes `C:\Nymi\Configuration` and `%ProgramData%\Nymi\ncc`. To keep the device's registration data for a later reinstallation, select **Keep the CWP configuration and client registration for a later reinstallation** during the uninstall; the uninstaller then leaves these files on disk.

9.2 Uninstalling Silently

1. Run a Command Prompt as administrator.
2. Type the following command, replacing `<version>` with the version in the installer's file name:

   ```
   "Nymi Connect Installer-<version>.exe" /uninstall /quiet
   ```

   By default, this removes `C:\Nymi\Configuration` and `%ProgramData%\Nymi\ncc`. To keep the device's registration data for a later reinstallation, add `KeepSecureData=1`:

```
"Nymi Connect Installer-<version>.exe" /uninstall /quiet
KeepSecureData=1
```

Copyright ©2026 Nymi Inc. All rights reserved.

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

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

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

Published in Canada.

Nymi Inc.
Toronto, Ontario
www.nymi.com