



Nymi Connected Worker Platform

Product Change Log

This document summarizes the key changes and feature enhancements for customers to consider when upgrading from Nymi Enterprise Edition (NEE) or the Nymi Connected Worker Platform (CWP).

Nymi's product accumulates features and improvements so later releases contain those that were added earlier.

Revision History

Date	Version	Release Notes
April 25, 2023	2.0	Refresh document Add changes for CWP 1.5.6 and CWP 1.6.1.



NEE 3.3.1

Nymi implemented Nymi Band Application and firmware changes in Nymi Enterprise Edition 3.3.1 to improve the enrollment and authentication experience. To improve the quality of the fingerprint template that the Nymi Band creates during enrollment, the following changes were made:

- Updating the fingerprint sensor library and detection algorithm.
- Increasing the number of fingerprint images captured during enrollment from 3 images to 5 images.
- Enhancing messaging and images in the Nymi Band Application to provide best practices and visual guidance to the user.

To improve the user experience during authentication, the Nymi Band:

- Provides users with an easy way to determine if an authentication is due to a fingerprint mismatch. If authentication fails due to a fingerprint mismatch, the Nymi Band vibrates and displays the Retry message approximately 1 second after the user places their finger on the fingerprint sensor.
- Provides the user with the ability to quickly retry an authentication failure that resulted from a fingerprint mismatch.
- Refines the fingerprint template on subsequent authentications. Nymi recommends that users perform 10 authentications immediately after enrollment to improve the quality of the template.

Note: To implement these improvements, after you update the Nymi Band firmware, you must re-enroll the Nymi Band. The *Nymi Enterprise Edition Administration Guide* provides more information.

NEE 3.3.2

Enrollment Improvements

Nymi implemented firmware changes in Nymi Enterprise Edition 3.3.2 to improve the enrollment experience. In Nymi Enterprise Edition 3.3.1 and earlier releases, during the enrollment process, the Nymi Band might display a fault code if the user presses Start on the Capture Fingerprint screen, and then places their finger on the sensor while the Nymi Band displays the Add User message instead of waiting until the Touch Sensor message appears. When this happens, the user must restart the Nymi Band and an NES Administrator must log in to the NES Administrator Console and delete the user association to the Nymi Band. The user can repeat the enrollment process with the same Nymi Band. The Nymi Enterprise Edition 3.3.2 firmware prevents the fault code from appearing on the Nymi Band if user places their finger on the sensor before the Nymi Band prompts them to do so.

CWP 1.1

Authentication and Enrollment Improvements

Several improvements have been made to the authentication and enrollment systems as part of CWP 1.1. The authentication algorithm has been improved to reduce the failure rate associated with fingerprint matching. The enrollment process has additional training material implemented in the Nymi Band Application, and the Liveness Detection feature is now enabled by a global configuration in the Nymi Enterprise Server policies.

FIDO2 Certification



The Nymi Band 3.0 has officially received FIDO2 certification from the FIDO Alliance. For additional information on the FIDO2 standard and benefits to your organization, contact your Nymi Solution Consultant.

Improved resistance to brute force authentication attacks

The Nymi Band 3.0 firmware now includes greater resistance to attempted brute force attacks. Repeated authentication failures will trigger a timed lockout preventing further authentication attempts. Each subsequent lockout increases in duration.

PIV Disabled

The PIV smartcard functionality is disabled in this release.

BLE Tap

This release introduces the option for the user to indicate intent by tapping their Nymi Band on the BLE adapter. This functionality eliminates the need for an NFC reader in environments where Nymi Bluetooth is used. For more information on this feature, see the *Nymi Administration Guide*.

Important:

- BLE tap is not supported in Evidian.
- BLE tap is not supported for FIDO2 / WebAuthn transactions

Nymi Lock Control

Nymi Lock Control is a Windows application that provides the following features:

- Login to a Windows PC via Nymi Band
- Unlock a locked Windows PC via Nymi Band
- Keep a Windows PC unlocked when the user is in close proximity to the PC
- “Walk-away Lock” - automatically locks a Windows PC when the user moves out of close proximity to the PC

For more information about Nymi Lock Control, see the *Nymi Administration Guide*.

CWP 1.1.1

Enrollment Improvements

Nymi implemented firmware changes in Connected Worker Platform 1.1.1 to improve the enrollment experience.

In Connected Worker Platform 1.1, during the enrollment process, the Nymi Band might display a fault code if the user presses Start on the Capture Fingerprint screen, and then places their finger on the sensor while the Nymi Band displays the Add User message instead of waiting until the Touch Sensor message appears. When this happens, the user must restart the Nymi Band and an NES Administrator must log in to the NES Administration Console and delete the user association to the Nymi Band. The user can repeat the enrollment process with the same Nymi Band.

The Connected Worker Platform 1.1.1 firmware prevents the fault code from appearing on the Nymi Band if the user places their finger on the sensor before the Nymi Band prompts them to do so.



Nymi Lock Control

Nymi made changes to Nymi Lock Control to improve the user experience when the user terminal does not have a network connection to NES. In Connected Worker Platform 1.1, when a user performs a tap to unlock the desktop, but the user terminal does not have a network connection to NES, Nymi Lock Control waits for 60 seconds before displaying an error message to the user and allowing the user to reattempt the unlock. Connected Worker Platform 1.1.1, optimizes the unlocking behaviour when the network connection is not available, to quickly provide an appropriate error message to the user, and allow them to reattempt the unlock sooner. The improvement is observed under a specific circumstance where Nymi Credential provider blocks the Windows showing the log in screen.

CWP 1.1.2

Improvements to the Storage of the Truststore Password

Nymi implemented changes in Connected Worker Platform 1.1.2 to improve the security of the solution by introducing changes that support the encryption the truststore password that is used by the Contact Tracing Collection Agent.

Expanded Thin Client Support

Nymi implemented changes to have broader thin client compatibility. The Nymi Connected Worker Platform 1.1.2 now supports thin clients connecting to a virtual desktop that use a frame-buffer protocol, such as VMware Blast, PC over IP, or VNC.

CWP 1.1.3

Expanded thin client support

Nymi implemented changes to have broader thin client compatibility. The Nymi Connected Worker Platform 1.1.3 now supports a wider range of thin clients connecting to a virtual desktop that use a frame-buffer protocol, such as VMware Blast, PC over IP, or VNC.

Stability improvement to the NES authentication

Nymi implemented changes in Connected Worker Platform 1.1.3 to improve the stability of NES authentication. The authentication token obtained after a successful authentication are valid for a defined period.

CWP 1.2

Contact Tracing Update

The Contact Tracing solution has been updated to stay current with the latest CDC contact tracing guideline. Close contact events are reported if two Nymi Bands are in proximity for a cumulative total of 15 minutes or more over a 24-hour period.

The contact tracing dashboard received updates to improve usability and to help the Health and Safety



staff perform contact tracing more easily. NOTE: This is an optional feature.

Increased Scalability

This release increases the capacity of the infrastructure to support 3,000 active employees. For more information about these features, see the *Nymi Overview Guide*.

CWP 1.3

Individual User Policy

CWP 1.3 provides a finer grained control over how user can authenticate to their Nymi Band. By creating individual user policy, the authentication experience of any user can be customized. This feature allow user to authenticate to their Nymi Band by using fingerprint, by using corporate credential, or by using both fingerprint and Electrocardiogram (ECG). To take advantage of the individual user policies, created and assign policies to users in Nymi Enterprise Server (NES). Then advise the user to sign into the Nymi Band Application (NBA) with an authenticated Nymi Band to allow the new policy to be applied to the Nymi Band. NOTE: When upgrading the Nymi Band firmware to CWP 1.3, the Nymi Band maintains the previously configured policy settings. To update the policy settings, sign into the NBA with an authenticated Nymi Band.

Improved Authentication User Experience

CWP 1.3 enhances the biometric authentication experience. By default, any Nymi Band enrolled with CWP 1.3 enjoys a significantly quicker authentication taking less than one second. For organizations that require a stricter control over biometrics authentication, the Liveness Detection can be enabled through NES. NOTE: When upgrading NES to CWP 1.3, global policies will be updated with the new configuration options in their default (disabled) state.

Update SQL Server Express Package

This release includes the SQL Server Express 2017 application. New installations of the Nymi Enterprise Server (NES) provide you with the option of installing SQL Server Express 2017 if you do not have an existing SQL Server on which to install the NES database. NES upgrades continue to use the existing SQL Server version. SQL Express 2017 provides support for TLS 1.2, a requirement for the SD/CT database.

CWP 1.3.1

iGEL Stability Improvement

Improve Nymi Bluetooth Endpoint stability on iGel thin clients. The NBE restarts automatically if it receives corrupted data from iGEL avoiding being stuck in a deadlock. The end user can continue use their Nymi Band after the NBE restart. The iGel support is only available with SDK build 5.11.1+9-9

NES Bug Fixes

Fix defect associated with NES individual user policy and the NES automated deployment script.



CWP 1.3.2

Lock Control Security

This release enhances the security of Nymi Lock Control. This changes the default configuration to require a user's explicit intent with Nymi Band to unlock a computer.

CWP 1.3.2 was a customer-specific release with changes that were not made generally available.

CWP 1.3.3

Improve e-signature response time for non-persistent sessions

When performing e-signatures on a non-persistent session (such as through Citrix or Remote Desktop Protocol), new device token is required for every session. Nymi made improvements on how the device token is processed. As a result, the response time for completing e-signatures on such sessions is greatly reduced. This improvement further boosts the efficiency gains unlocked by adopting Nymi solution. This change is limited to deployments that make use of the device token. For deployments that do not use device token for authentication (such as webapi), the e-signature performance is unaffected.

Add support for mixed Evidian environment

An organization that has multiple sites can have variations of the CWP and Evidian integration. Some sites require a CWP and Evidian integration, whereas other sites do not require Evidian components. CWP 1.3.3 introduces improvements to allow Nymi Bands to be enrolled with or without the presence of an Evidian client on the terminal, providing more flexibility to how the CWP can be deployed.

Apply security patches to SDK

To continuously make CWP more secure, the present release enhances the security of the Nymi SDK. The OpenSSL security patch affects Linux only, i.e. NBE on thin clients. Windows SDK does not use OpenSSL.

CWP 1.3.4

Implemented bug fixes

The present release sees two issues fixed. Firstly, removing restrictions on updating NES instances. A NES instance can be updated without it being installed on C:\ drive. In addition, Relaxing .NET framework requirement for NBA. Both changes offer more flexibility and greater convenience in deploying or upgrading the CWP solution.

CWP 1.3.6



Implemented bug fixes

The present release addresses an issue with cached certificates on the Nymi Band. The Nymi Band stores certificates that are used to establish secure communication with the Nymi infrastructure. One certificate (NES L1 certificate) must remain on an enrolled Nymi Band, while other certificates that reside on the Nymi Band are cached to speed up operations. When the Nymi Band cache becomes full (after caching approximately 80 certificates), the Nymi Band deletes the contents of the cache. A defect in the cache clearing operation, inadvertently deletes the NES L1 certificate in addition to the cached certificates. When the L1 certificate is not on the Nymi Band, the user cannot perform BLE operations until the user re-enrolls the Nymi Band. The fix eliminates the unintended deletion of the NES L1 certificate.

The issue related to cached certificate occurs more frequently in Citrix / Remote Desktop environments with non-persistent user profiles, where a new certificate is required for each user session.

This issue does not impact users that access web-based applications to perform Nymi Band operations, or Evidian environments that use the Nymi Band in an RFID-only configuration.

CWP 1.5.6

Enable the Nymi SDK for web applications on the Apple iPad

CWP 1.5.6 adds support in the Nymi SDK for web applications that run on an iPad. Once a developer has integrated the Nymi SDK into their application, the Nymi Band can be used to verify the user's identity by tapping it on the iPad. The CWP 1.5.6 release sees the solution being suitable for use in GxP environment. The updated SDK introduces a new component, the Nymi Application, which is a native iOS app that handles communication with the Nymi Band.

Also in this release, the Nymi Calibration Application can help the administrator to determine the optimal location on an iOS device for tapping the Nymi Band and to come up with the appropriate setting for Nymi Application. The Nymi Calibration Application is still an experimental feature.

The Nymi Application will be available through the Apple App Store.

Lock Control Security

This release enhances the security of Nymi Lock Control. This changes the default configuration to require a user's explicit intent with Nymi Band to unlock a computer.

This was first introduced into CWP 1.3.2 as a fix for a specific customer. Nymi is making this improvement available to all customers.

CWP 1.6.1

Increased identity assurance

This release increases assurance in the assignment of a Nymi Band to a user. Some edge cases have been



identified where a user may be interrupted during the Nymi Band enrollment process and the process can be completed by a different user. In some of these cases, the Nymi Band will be associated with the wrong user.

The solution will be applied to all customers and will result in improved usability. A consequence of this change is that the Setup Code is no longer used during enrollment.