# Connected Worker Platform

## New Features and Enhancements

*Document Version 5.1*

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<br>Add changes for CWP 1.5.6 and CWP 1.6.1. |
| June 20, 2023 | 3.0 | Add changes for CWP1.7, 1.8, and 1.9 |
| September 21, 2023 | 4.0 | Add changes for CWP 1.13.0 |
| October 12, 2023 | 5.0 | Add changes for CWP1.14 |
| November 08, 2023 | 5.1 | Add changes for CWP1.13.x and CWP1.14.x patch releases |

## 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 (NEE) 3.3.2 to improve the enrollment experience. In NEE 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 NEE 3.3.2 firmware prevents the fault code from appearing on the Nymi Band if user places their finger 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 the 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 certificates 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 the 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.

# CWP 1.7.0

## Nymi Band in Hazardous Environments

CWP 1.7.0 introduced a new setting to disable all haptic feedback on the Nymi Band. The haptic feedback can be disabled to all Nymi Bands or to selected set of Nymi Bands through Nymi Enterprise Server Admin Console. With haptic feedback disabled, the Nymi Band can be safely used in hazardous environments where an explosion can occur if there is an ignition source. There are different regulations that apply to equipment used in these areas.  At the time of the release, the Nymi Band is compliant with ANSI/ISA-12.12.03-2011 standard, which regulates portable electronic equipment, such as Nymi Band.

For customers adopting a different specification regulating the electronic equipment used in hazardous environments, a site-specific assessment will be required before deploying the Nymi Band.

## Nymi Enterprise Server Security Improvements

We take security very seriously at Nymi and are committed to ensuring the safety and integrity of our customers' data.  The present release addresses a few vulnerabilities in the Nymi Enterprise Server.

## CWP 1.8.0

### Nymi Band Fingerprint Enrollment Improvement

When setting up the Nymi Band, user is required to enroll their fingerprint for biometric authentications. At the end of the enrollment, the Nymi Band generates a fingerprint template of the enrolled finger. This release introduced changes to the fingerprint enrollment procedure to improve the quality of the fingerprint template, thus boosting the biometric authentication success rate. During the fingerprint enrollment, the Nymi Band captures more images of the enrolling fingerprint and verifies whether the fingerprint supplied meets the biometric authentication requirements. If a user is having trouble enrolling the fingerprint, the Nymi Band will alert the user to contact the administrator for support. Note that the changes do not affect the fingerprint enrollment and matching algorithm. As a result, there is no impact on the security and privacy of the solution.

### Nymi Enterprise Biometric Authentication Improvement

When a user encounters repeated issues with biometric authentication to the Nymi Band, the Nymi Band provides the user with guidance on what to do to troubleshoot the issues. The Nymi Band also displays the causes of the biometric authentication failure, due to fingerprint matching, liveness detection, or both. With the additional information and guidance, the user can make corrective actions, such as cleaning their finger, and authenticate to the Nymi Band without any issue.

## CWP 1.8.1

### Improve Nymi Band e-signature performance in Evidian integration

Nymi-Evidian integration has a large customer base. This integration allows the Nymi Band user to create e-signatures with Evidian. In the effort to continuously improve the operational efficiency and usability to Nymi Band customers, Nymi is working with Evidian in improving reliability, speed, and flexibility in the solution. The changes introduced in the present release is applicable to the Nymi-Evidian integration in the wearable mode, brings three major benefits to the customer:

1- Eliminates the dependency on Nymi Enterprise Server (NES) connection during e-signature creation in Evidian. This improves the reliability of the solution: NES is no longer required in the frequent and high traffic e-signature related transactions.
2- By eliminating the round-trip to NES, the transaction speed for an e-signature creation in Evidian is greatly improved, significantly so in a remote desktop set up (e.g. Citrix).
3- Support the BLE tap to create e-signatures. User can tap the Nymi Band on the Bluetooth adaptor instead of NFC reader, simplifying the peripheral requirement to implement the Nymi-Evidian solution.

## CWP 1.9.0

### NES Deployment Improvement

The release added support for putting NES webservices into different app pools during installation. This change simplifies the NES deployment since Service Principal Names no longer need to be configured in Active Directory for Kerberos authentication.

### NES Security Improvement

This release patched up a few security vulnerabilities in NES making the solution more secure.

## CWP 1.9.1

### Fix NES Admin Console User Authentication Issue

Fix to the NES admin console user sign in issue, if user belongs to too many AD groups.

## CWP 1.11.0

### Nymi Band Fault Handling Improvement

Nymi Band will attempt to recover from faults. Only displays fault message if it is not recoverable.

## CWP 1.12.2

### Secure e-signature over Webapi

CWP1.12.2 introduces a new and more secure method to create e-signature using Nymi Band. The new protocol eliminates the security shortcomings in the lookup operation.

## CWP 1.13.0

### Native app integration with Nymi Application

CWP 1.13.0 introduces a new protocol for native iOS applications to communicate with the Nymi Application. This enables native iOS applications to delegate communication with the Nymi Band via wireless protocols to the Nymi Application instead of implementing the protocols themselves. This expands the usability of Nymi CWP in environments with iOS devices in a secure manner, while allowing developers of native iOS apps to integrate with Nymi efficiently.

## CWP 1.13.1

### Improve Nymi Runtime Language and Locale Support

The Nymi Runtime and all its components can be installed on a wider range of operating systems with various language and locale settings.

### Improve Nymi Enterprise Server Authentication Compatibility

Nymi Enterprise Server (NES) no longer has restrictions over the Active Directory (AD) Group membership or the AD Group name lengths. With this improvement, users who belong to a lot of AD Groups or AD Groups with long names can perform e-signatures in Evidian integration without slow down or experience crashes. Such users also can sign into the NES Admin Console without any issue.

### Key Resolved Issues in CWP 1.13.1

| Issue Number | Description |
|---|---|
| NEM-3009<br>NEM-3052 | Users who belong to lots of Active Directory Groups (AD) or groups with long group names can experience slow response in Evidian, Evidian crashing, or NES admin console authentication failures. |
| SDK5-2730 | Nymi Runtime installation can fail in non-English operating systems. |

# CWP 1.13.2

## Improve Nymi Runtime Installation stability

Nymi Runtime can be successfully installed consistently across all supported platforms.

## Key Resolved Issues in CWP 1.13.2

| Issue Number | Description |
|---|---|
| SDK5-2657 | Nymi Runtime installation stability issue. |

# CWP 1.14.0

## LEGIC Advant on Nymi Band

LEGIC Advant is a memory transponder chip for smartcards, keys and watches. It can be used for access control, time & attendance and cashless payments can be combined with third- party applications. Integrating the LEGIC Advant into the Nymi Band combines the biometric authentication offered by the Nymi Band with the security and flexibility of the LEGIC Advant. To take advantage of LEGIC on Nymi Band, LEGIC enabled Nymi Bands are required and the Nymi Bands must go through an encoding process. The LEGIC enabled Nymi Band also supports all existing Nymi Band use cases.

## NFC Reader Compatibility Improvement

Nymi Band now can work with a wider range of NFC readers and tablets. The following devices are now supported:  iDTronic NEO 2 desktop reader, Zebra ET80 tablet, and Getac F110 (G6) tablet.

## Key Resolved Issues in CWP 1.14.0

| Issue Number | Description |
|---|---|
| NF-4049 | Issue: Nymi Band cannot work with the following devices: Zebra ET80 tablet, Getac F110 (G6) tablet, IDTronic NEO 2 desktop reader |

# CWP 1.14.1

## Improve Data Accuracy in Nymi Enterprise Server

The Nymi Enterprise Server (NES) stores information associated with Nymi Band and Nymi Band activities. This release improves the accuracy across all data stored in the NES database. The database now uses Coordinated Universal Time (UTC) to represent event timestamps allowing deployments across multiple geographical regions to accurately track events. In addition, the audit data received an update to fix an issue with incorrect username.

## Fix Lock Control Debug Log Issue

Lock Control debug logs no longer contain any sensitive information.

## OpenSSL 3.0 Library Update

Nyim Runtime utilizes OpenSSL 3.0 library to take advantage of the up-to-date security standards. Nymi partners, who integrate with Nymi SDK on Linux based operating systems, should

update their applications to maintain compatibility with the latest CWP releases.

### Key Resolved Issues in CWP 1.14.1

| Issue Number | Description |
|---|---|
| LC-851 | Lock Control shows sensitive user information in debug logs |
| NEM-3035 | Incorrect user can be logged in NES audit data |
| NEM-3037 | Incorrect timestamp can be logged in NES database |

## CWP 1.14.2

### Nymi Application Compatibility and Scalability Enhancements

Nymi Application enables users to create e-signatures in Nymi-integrated iOS applications with their Nymi Bands. The enhancement introduce in this release improves the compatibility and scalability of the Nymi Application. Nymi integration partners benefit greatly from the compatibility enhancements making the integration work a lot easier. For the customers who deploys the Nymi Application on their iOS devices, Nymi expanded the support of configuring the Nymi Application using Mobile Device Management applications.

### Improve Nymi Runtime Language and Locale Support

The Nymi Runtime and all its components can be installed on a wider range of operating systems with various language and locale settings.

### Improve Nymi Enterprise Server Authentication Compatibility

Nymi Enterprise Server (NES) no longer has restrictions over Active Directory (AD) Group membership AD Group name lengths. With this improvement, users who belong to a lot of AD Groups or AD Groups with long names can perform e-signatures in Evidian integration without slow down or experience crashes. Such users also can sign into the NES Admin Console without any issue.

## Key Resolved Issues in CWP 1.14.2

| Issue Number | Description |
|---|---|
| NEM-3009<br>NEM-3052 | Users who belong to lots of Active Directory Groups (AD) or groups with long group names can experience slow response in Evidian, Evidian crashing, or NES admin console authentication failures. |
| SDK5-2730 | Nymi Runtime installation can fail in non-English operating systems. |
| SDK5-2657 | Nymi Runtime installation stability issue. |