Nymi Connected Worker Platform Release Notes

CWP 1.3.0

2022-May-17 v1.0

Contents

Table 1: Revision History

Version	Date	Revision History
01	May 17, 2022	First release of document

Nymi Connected Worker Platform 1.3

Nymi's Connected Worker Platform (CWP) connects people with technology through safe, simple, and secure solutions. The Connected Worker Platform supports numerous use cases and digital systems and combines point solutions into a single offering.

The goal of the Connected Worker Platform is to simplify the connection of workers to the digital space found in modern organizations. When the barriers to secure digital work are removed, workers can focus on what they do best.

The CWP 1.3 release is the very first CWP release that is validated for use in an GxP environment.

Nymi Connected Worker Platform components

CWP 1.3.0 includes the following component versions:
- Nymi Band™ 3.0
- Firmware version of Nymi Band 3.0– 4.2.9.5
- Nymi Band Application–4.0.2.3
- Nymi Lock Control–3.4.2.10
- Nymi Enterprise Server–4.2.0.3
- Nymi Enterprise Server Auto Deployment Scripts– 1.2.3
- Nymi SDK –5.11.0.8
- CWP backend components – 1.2.1.12
- Nymi Data Exchange Service Edge Agent -1.1.0.2

Nymi Documentation Package

For information on the documentation available for the CWP 1.3.0 release, see Appendix 1.

NFC Reader Support

NFC reader support is not tested under the CWP 1.3.0 release. For NFC readers supported in the previous CWP releases see Appendix 2.

New In This Release

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.

Table 2: Backwards Compatibility Table

			Nymi Infrastructure									
			NEE 2.x	NEE 2.5	NEE 2.6	NEE 3.0	NEE 3.1	NEE 3.2	NEE 3.3	CWP 1.1.x	CWP 1.2.x	CWP 1.3.0
Nymi Band Firmware	Nymi Band 2.0	NEE 2.x	•	•	•							
		NEE 2.5	•	•	•							
		NEE 2.6	•	•	•							
	Nymi Band 3.0	NEE 3.0				•						
		NEE 3.1		•	•		•					
		NEE 3.2		•	•			•	•			
		NEE 3.3		•	•			•	•			
		CWP 1.1.x								•		
		CWP 1.2									•	•
		CWP 1.2.1									•	•

Legend:

•   Compatible   ☐   Not compatible (empty box)

Upgrading to CWP 1.3.0

Table 3: Upgradability Table

Release versions	Upgradability

NEE 3.2.X to CWP 1.3.0
 	
NEE 3.3.X to CWP 1.3.0
	NES:
	  - direct upgrade
	NBA:
	  - direct upgrade
	  - can be upgraded after NES upgrade
	Firmware:
	  - direct upgrade
	  - **re-enroll required after upgrade**
	  - can be upgrade after NES and NBA upgrade

CWP 1.1.X to CWP 1.3.0
 	
CWP 1.2.X to CWP 1.3.0
	NES:
	  - direct upgrade
	NBA:
	  - direct upgrade
	Firmware:
	  - direct upgrade

The change implemented in CWP prevents Nymi Band running CWP 1.3.0 firmware to work properly with NEE 3.3.x SDK, specifically the Nymi Bluetooth Endpoint. To ensure the CWP function as expected, all CWP components have to be upgrade.

Known Issues and Limitations

Table 4: Known Issues in CWP 1.3

The following section lists known issues as of the CWP 1.3 release.

Issue Number	Description
SDK5-1955	**Issue:** Silent installation of SDK does not install Bluegiga driver.

	Workaround: Run the standalone Bluegiga driver installer included in the SDK release package.
NEM-2803	**Issue:** Authentication related settings changes to the new default settings after upgrading to CWP 1.3.0. **Workaround:** Verify the group policy settings are desirable after upgrading to CWP 1.3.0.
NEM-2760	**Issue:** In the *Search* window, if you search with the none (group policy), not all users appear. **Workaround:** None. The *Search* results window only displays users that are in the NES database. Users appear in the NES database when an administrator has searched for them and viewed their properties or when a user has been enrolled to Nymi Band.
DOC-739	**Issue:** Not all CWP uses cases support multi-domain configurations. **Workaround:** None. Web Attestation and the Contact Tracing Dashboard use cases require user accounts to reside in the same domain as the infrastructure.

Table 5: Known Issues in CWP 1.2.1

The following section lists known issues as of the CWP 1.2.1 release.

Issue Number	Description
SDK5-1880	**Issue:** The Lock Control may not function properly through a remote session if the Window or Windows Server is not installed on C:\ drive **Workaround:** Make sure the Windows and Windows Server is installed on C:\ drive.
CWP-2095	**Issue:** When cache expiry settings are changed by an administrator, settings will take effect after the current expiry period if over. If an administrator checks the settings within the cache expiry time, they will appear unchanged. **Workaround:** Administrator should wait for the change to be implemented, typically 5 minutes, and the system will recover itself; or disable cache.

Table 6: Known Issues in CWP 1.2.0

The following section lists known issues as of the CWP 1.2.0 release.

Issue Number	Description
CWP-1931	**Issue**: When the user is signed into Health Check App across multiple device or in multiple browsers. Signing out in one session does not automatedly sign out all the other sessions. **Workaround**: Ensure the user signs out across all devices or close all browsers.
CWP-2018	**Issue**: The contact tracing information for a Nymi Band cannot be displayed when the Nymi Band is deleted in NES **Workaround**: First look up the MAC address of the deleted Nymi Band from the NES database, Nymi Band audit record. Then in the CT database, look up the contact events registered to that MAC address.
DCS-253	**Issue**: When viewed on certain browsers, the Contact Tracing Dashboard's Most Contact Employees graph does not zoom properly. **Workaround**: Return the browser to 100% zoom.
LC-797	**Issue**: Unlocking the PC by NFC tap fails if the network connection to NES is unavailable. **Workaround**: Unlocking the PC by typing in username then hit enter key or by tapping the Nymi Band on the Bluetooth adapter (if BLE tap is enabled).
LC-827	**Issue**: The Lock Control does not contain the same SDK as the SDK released in CWP 1.2.0. The functionality of the Lock Control is not impacted. When updating from an earlier version, the SDK might not be automatically updated. **Workaround**: For new install or update, first install the Nymi SDK, then run the Lock Control installer.
NEM-2738	**Issue**: When updating the NES, at the Review Settings tab the installer may give a database login error. **Workaround**: Navigate to the Database tab and click the Test button. Then go back to Review Settings tab and click Test.
NEM-2744	**Issue**: The NES command prompt install tool fails when encryption is set to "None".

	Workaround: Deploy or update NES either use NES installer executable or the NES auto deploy script.
NEM-2546	**Issue**: When the user selects the Contact Support option from the Lock Control tray icon, a zip file of logs is generated but the location of the zip is not provided. **Workaround**: See the documentation for the location of the zip file.
NEM-2747	**Issue**: When updating the NBA to CWP 1.2.0, the installer does automatically update the SDK to the latest version. Without updating the SDK, user might encounter errors during enrollment. **Workaround**: Before upgrading the NBA, uninstall SDK that exists on the terminal.
SKD5-1803	**Issue**: Nymi runtime fails to install when installing to a non-default location. **Workaround**: Install the Nymi runtime at its default location: "C:\Program Files\Nymi"
SDK5-1839	**Issue**: Occasionally, CWP data is not retrieved by the edge agent while the Nymi Band is on charger. **Workaround**: The data will be retrieved when the Nymi Band is authenticated.
SDK5-1854 SDK5-1855	**Issue**: nbed cannot be upgraded or uninstalled from some models of thin clients. **Workaround**: Uninstall the nbed by reset the thin client. To upgrade the nbed, reset the thin client to a standard image and then install the newer version of nbed.

Table 7: Known Issues in CWP 1.1.x

The following known issues were reported in the CWP 1.1.x releases.

Issue Number	Description
DCS-260	**Issue:** log4j CVE-2021-44228 vulnerability
CWP-1157	**Issue**: If multiple Nymi Bands are placed on the charger simultaneously, the Contact Tracing Collection Agent (CTCA) may not retrieve the contract events from all the Nymi Bands.

Issue Number	Description
	Workaround: Take the Nymi band off the charger and the contact events will be retrieved by CTCA.
CWP-1081	**Issue**: If a user re-enrolls to a different Nymi Band, then any new contact data they collect will not show up for 24 hours in the dashboard. **Workaround**: Wait 24 hours for the data to update, or restart the CTCA.
CWP-1059	**Issue**: On the Contact Tracing dashboard, when searching for contact events by contact date, not all events may be returned for a specified day. **Workaround**: Add one day to the end of the date range specified in order to ensure that all data is returned.
CWP-1024, CWP-1012	**Issue:** In a multi-domain environment, the Contact Tracing dashboard only shows data from users in one domain. **Workaround**: Ensure that all users of the Contact Tracing feature are in the same domain.
CWP-1017	**Issue:** The Contact Tracing Collection Agent (CTCA) may take a long time to initialize the API. This is a benign issue as no data is lost.
CWP-1015	**Issue:** Multi-instance functionality for CTCA is not currently supported. If multiple instances of the CTCA are started, errors will occur and only one of the instances will function correctly.
CWP-1014	**Issue:** The Contact Tracing dashboard label for Contact Time, erroneously indicates that time is shown in UTC time zone. The time is shown is the local time of the web browser. This is a cosmetic issue that does not affect data.
CWP-1008	**Issue:** The format of the login name for the Contact Tracing dashboard is different from the format required by other Nymi product logins. **Workaround**: Ensure the login name is entered in the appropriate format: <usename>@example.domain.name
CWP-1004	**Issue:** There is no input validation on user-specified queries for the Employee Timeline graph on the Contact Tracing dashboard. If an invalid query is entered, a blank graph is returned.

Issue Number	Description
CWP-1000	**Issue:** On the Contact Tracing dashboard, the Update button for the Most Contacted Employee Details does not update the view. **Workaround**: Refresh the page to update the view.
CWP-926	**Issue:** The contact tracing dashboard does not indicate when the display is blank because there is no data in the database. This is a cosmetic issue and does not affect functionality.
CWP-691	**Issue:** Spurious warning messages about *ctca.properties* appear in the log when the configuration is correct. These warnings can be safely ignored. (This issue is only applicable for CWP 1.1.x)
CWP-570	**Issue:** On the Contact Tracing dashboard, the list of user contact events in the User Timeline is not paginated. **Workaround**: If too many results are returned, filter the search query to narrow the results.
CWP-569	**Issue:** On the Contact Tracing dashboard, the axis labels for Unique Contact Count stack on top of each other, making the text illegible. This is a cosmetic issue that does not affect the data.
NEM-2660	**Issue:** On Windows Server 2019, the SQL Express 2012 installer included in the NES installer may fail. **Workaround**: Install SQL Express 2017 in Basic mode before running the NES installer on Windows Server 2019.
NEM-2651	**Issue:** The *NesSupportTool.exe* is not able to extract and create a log zip file on Windows Server 2019.
NEM-2632	**Issue:** The *.ninst* file generated by NES is not self-documented. Contact Nymi Support for any *.ninst* file related questions.
NEM-2553	**Issue:** Running the NES install.exe program for a second time causes a disabled NES Installer Maintenance dialog to appear. **Workaround**: None. This dialog does not require user intervention.

Issue Number	Description
NEM-2270, NEM02280, NEM-2296	**Issue:** In some cases, after logging in to the NES Admin Console, the console page does not show that login succeeded. **Workaround**: Navigate to another page to confirm that login was successful.
NEM-1750	**Issue:** Any interruption in network connectivity during enrollment causes the system to become out of synch. **Workaround**: If network connectivity is lost during enrollment, perform a Delete User Data operation on the Nymi Band, disconnect the device from the user in the NES Admin Console, and restart enrollment.
NPM-363	**Issue:** By design, the Nymi Band firmware will not record a Proximity Event during the time that the Collection Agent is connected to download Proximity Events. In some rare cases, this can lead to a missed Contact Event.
SDK5-1729	**Issue:** While using Lock Control, **i**f a user moves their Nymi Band within 10cm of the BLE adapter, a login or unlock will occur even if that was not the user's intent. For example, this may occur if a user is reaching past the adapter to plug in a charger or access a USB hub. This is a benign issue and does not affect the behaviour of the system.
LC-785	**Issue:** When a user without an active Nymi Band registered in NES attempts an NFC tap to unlock or login, no error message is shown. This is a benign issue as the NFC tap is expected to fail when the Nymi Band is deactivated in NES.
NF-3748	**Issue:** In some rare instances, users may experience consecutive authentication failures due to the ECG measurement during Liveness Detection. **Workaround**: If required, Liveness Detection can be disabled. See NF-3733 for important considerations before using this workaround.
NF-3745	**Issue:** The fingerprint sensor does not respond to the user placing their finger on the sensor. Authentication times out. **Workaround**: In this scenario, authentication failure now occurs quickly, and the user can retry authentication with a high chance of success.
NF-3741	**Issue:** In some cases, the firmware update may take longer than 300 seconds.

Issue Number	Description
NF-3739	**Issue:** In some cases, the firmware updater program may not make use of all available BLE adapters. **Workaround**: If this issue occurs, stop and restart the updater.
NF-3738	**Issue**: In some rare instances, the fingerprint sensor may not respond while a user is attempting to register their fingerprint template. **Workaround**: Remove the Nymi Band from the wrist. Put the Nymi Band back on and restart the enrollment process.
NF-3733	**Issue:** When Liveness Detection is disabled in the NES Policy, it is possible for users to authenticate the Nymi Band on objects other than a human body if the correct fingerprint is provided. This is a known and expected side effect of disabling Liveness Detection. **Workaround**: Liveness Detection should be disabled only in environments where users are having difficulty authenticating due to liveness and no other remedy has resolved their issue.
NF-3724	**Issue:** In some rare cases, when using the firmware updater to update the firmware on a Nymi Band that is in Recovery mode, the update may fail on the first attempt. **Workaround**: No user intervention is required. The updater continues to retry the update until it is successful.
NF-3694, NF-3693, NF-3687	**Issue:** In some cases, when using the Nymi Band as a FIDO2 security key to sign into a Windows PC, the user may have to hold their Nymi Band over the NFC reader for up to 400ms. If this issue occurs, a full authentication may take up to 2000ms.

Table 8: Known Issues in NEE 3.3.0

The following known issues were reported in the NEE 3.3.0 release.

Issue Number	Description

NEM-2643	**Issue:** If the Nymi Band Application loses the network connection or if the app is closed during the fingerprint enrollment process, the Nymi Band and the application will become desynchronized, and enrollment is interrupted. **Workaround:** If this issue is encountered, the user must Delete User Data and start the enrollment process again.
NEM-2453	**Issue**: When upgrading NES from NEE 2.6.X to NEE 3.3.0, if the NES Admin Console is left open in a browser page, there can be deprecation in functionality. The logout button will not work. **Workaround**: Before performing an upgrade of NES, close all browsers with the NES Admin Console open.

Table 9: Known Issues for NEE 3.2.1

The following known issues were reported in the NEE 3.2.1 release.

Issue Number	Description
SOL-365	**Issue**: During the import of the *fullchain.p12* file, no keys are found for the certificate during the NES installation. While *certlm.msc* displays a private key icon next to the NES L2 certificate, Windows is not able to access the private key. This results in a failure on the NES diagnostics page indicating that there was an error generating test certificates. **Workaround**: Delete the entire certificate chain and then re-import the fullchain.p12 (right click - import PFX) resulting in the cert chain AND key being successfully imported. If the IIS application pool identity used by NES is not "LOCAL SYSTEM", then move the NES L2 certificate to the Intermediate CA certificate store, and run "iisreset".
NEM-2302	**Issue**: Previously configured database logins are not saved in the generated .ninst file when loaded from a previous installation. **Workaround**: To generate a complete .ninst file, Export Settings immediately after completing a fresh installation of NES.

Issue Number	Description
NEM-2295	**Issue**: NES does not have sufficient Application Pool identity permissions to support the infrastructure (NEA certificate generation, look-ups, etc.). **Workaround**: Change the Application Pool identity setting to LocalSystem.
NEM-2249	**Issue**: In the NES GUI installer, the user is unable to edit Database login details after initial entry of details. **Workaround**: Use the original database user details entered for the new user/auditor, or close and restart the NES installer.
NEM-2439	**Issue:** Completing a NES installation with a specific user account specified for the Application Pool identity, where the user account which does not have Database privileges, results in database errors when running tests on the database page in the NES installer. **Workaround:** If a NES installation is completed by a user who does not have Database permissions, complete the installation without running tests on the Database page of the installer.
SDK5-1618	**Issue**: When upgrading the Nymi runtime from NEE 2.6 to NEE 3.2, the Nymi Websocket API stops working. **Resolution**: Replace the original nymi_agent.toml file with the nymi_agent.toml file from the NEE 3.2.1 package.
NEM-1954	**Issue**: To configure hardening on NES, configure the NES to use LocalSystem identity from the Application Pool Identity list. This can be changed on the IIS page in the NES installer.

Appendix 1: Documentation Package for CWP 1.3

Documentation for the Nymi Connected Worker Platform can be found in the release package delivered for CWP 1.3.

Core Documentation

The core documentation accompanies the standard CWP 1.3.0 package. These documentations provide crucial information on the CWP 1.3.0 release as well as instructions on deploying and maintain the solution.

To access all the secondary documents, visit: https://support.nymi.com/hc/en-us/articles/6337039121940-Connected-Worker-Platform-1-3-Product-Documentation

Secondary Documentation

The secondary documents offer additional support for the CWP 1.3 solution. These documents are not included in the CWP 1.3 package.

To access all the secondary documents, visit:
https://support.nymi.com/hc/en-us/sections/360012100892-Supplementary-Product-Documentation

Appendix 2: NFC Readers Tested for CWP 1.3.0

Nymi includes dedicated NFC reader compatibility testing as part of its release testing. The following table covers the specific NFC reader models tested for compatibility with CWP 1.3.0. Note that the level of ongoing testing is indicated as follows:

1. <u>Recommended Readers</u> - best performance; testing planned with every CWP release going forward from CWP 1.3.0.
2. <u>Supported Readers</u> - meet specific use cases but may not perform as well as a recommended reader; testing planned with every CWP release going forward from CWP 1.3.0.
3. <u>Verified Readers</u> - tested against a minimum of one NEE or CWP release; additional testing may be required to support additional releases; will be tested as part of the customer upgrade process.

Table 10: NFC Readers

NFC Reader Model	Status
HID Omnikey 5022	Recommended
ACS ACR122U	Verified with CWP 1.3.0
Systec CONNECT BOX	Verified with NEE 3.3.0
Elatec TWN4 LEGIC NFC USB	Verified with CWP 1.3.0
HID Omnikey 5127CK Mini	Verified with NEE 3.2.0
ACS ACR1252U	Verified with NEE 3.2.0
Identiv CLOUD/uTrust 3700 F	Verified with NEE 3.2.0
RFIdeas WAVE ID Nano SDK 13.56MHz CSN Black Vertical USB Reade	Verified with CWP 1.3.0