Nymi Connected Worker Platform
Release Notes

CWP 1.1.3

V2.0

Contents

Release Notes Revision History

Nymi Connected Worker Platform 1.1.x

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.

Nymi Connected Worker Platform components

CWP 1.1.3 includes the following component versions:

1. Nymi Band™ 3.0
2. Firmware version of Nymi Band 3.0— 4.2.5.8
3. Nymi Band Application—4.0.2.5
4. Nymi Enterprise Server—4.0.1.3
5. Nymi SDK—5.8.2.5
6. Nymi Lock Control – 3.3.3.4
7. Contact Tracing Collection Agent –1.1.3.4

Nymi Documentation Package

For information on the documentation available for the CWP 1.1.3 release, see Appendix 1.

NFC Reader Support

For information on NFC readers tested against the Connected Worker Platform 1.1.3 release, see Appendix 2.

New In This Release

This section summarizes the new features in this release.

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.

Backwards Compatibility

This section summarizes the backwards compatibility.

Release Compatibility with CWP 1.1.x

This release is compatible with CWP 1.1.x. One exception is when updating the NES to the current release, a manual change to the web.config file is required. After completing the steps to use the configuration wizard to upgrade the NES and before launching the NES Administration Console, as outlined the CWP Administration Guide, perform the following the steps.

1. Ignore the error message in the NES configuration wizard and close the window.
2. Navigate to `C:\inetpub\wwwroot\<NES_instance_name>\NEnrollment` and locate the `web.config` file.
3. Open the `web.confg` file in a text editor as an administrator and make the following edits.
   a. Under the `<configuration>` section, add the following string.
      ```
      <configSections>
      <section name="entityFramework"
      type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSe
      ction, EntityFramework, Version=6.0.0.0, Culture=neutral,
      PublicKeyToken=b77a5c561934e089" requirePermission="false" />
      </configSections>
      ```
   b. Under the `<appSettings>` section, make sure the following string is present
      `<add key="SqlConnectionString" value="<Data Source=SqlConnectionSringValue>"/>`, modify the value to match the `SqlConnectionStringValue` of the current NES instance.
   c. **Note:** The `SqlConnectionStringValue` can be found in the following file `C:\inetpub\wwwroot\NES_instance_name\NES\web.config`. This is an example of a `SqlConnectionStringValue`:
      `Data Source=.\SQLEXPRESS;Initial Catalog=Nymi.nes;Integrated Security=True;MultipleActiveResultSets=True`
4. Add the following strings after the `</runtime>` line
   ```
   <entityFramework>
    <defaultConnectionFactory
   type="System.Data.Entity.Infrastructure.SqlConnectionFactory,
   EntityFramework"/> <providers> <provider
   ```

```
invariantName="System.Data.SqlClient"
type="System.Data.Entity.SqlServer.SqlProviderServices,
EntityFramework.SqlServer"/> </providers> </entityFramework>
```

5. Save the `web.config` file.

Release Compatibility with Nymi Band 2.0

Nymi Band 2.0 is not supported with CWP 1.1.x

Release Compatibility with Nymi Band 3.0

CWP 1.1.x introduces breaking changes in Nymi Band firmware. CWP 1.1.2 firmware is not compatible with existing Nymi Enterprise Edition Releases.

Nymi Enterprise Edition Infrastructure Compatibility

CWP 1.1 is a new product offering from Nymi. CWP introduces a new generation of the Nymi SDK. There is no compatibility of Nymi infrastructure components between NEE and CWP releases.

Known Issues

The following known issue are reported in the CWP 1.1.x release.

Table 2: Known Issues CWP 1.1.x

Issue Number	Description
NEM-2713	**Issue:** Upgrading to CWP 1.1.3 NES requires manually modifying a web.config file **Workaround**: Take the Nymi Bands off the charger one at a time and the contact events will be retrieved by CTCA. For detailed instructions refer to the Upgrading NES section in the CWP Administration Guide.

Issue Number	Description
LC-816	**Issue:** The use of the Nymi Band and Nymi Lock Control to log into or unlock a remote session is only supported with the following protocols: • Microsoft Remote Desktop • Citrix, when Network Level Authentication (NLA) is disabled.
CWP-1157	**Issue:** If multiple Nymi Bands are placed on the charger simultaneously, the Contact Tracing Collection Agent (CTCA) may not retrieve the contact events from all Nymi Bands. **Workaround**: Take the Nymi Bands off the charger one at a time and the contact events will be retrieved by CTCA.
CWP-1081	**Issue:** If a user re-enrolls to a different Nymi Band, any contact data associated with their new Nymi Band will not appear on the dashboard for up to 24 hours. **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.

Issue Number	Description
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. The login format for the dashboard is: username@domain
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.
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.
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.

© 2021 Nymi Inc.   Nymi Connected Worker Platform 1.1.3 Release Notes   **8/17**

Issue Number	Description
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
NEM-2270	**Issue:** In some cases, after logging in to the NES Administrator 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 sync. **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 Administrator Console, and restart enrollment.
NPM-363	**Issue:** By design, the Nymi Band firmware will not record a Proximity Event during the time that the Contact Tracing 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, if 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 behavior 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.

Known Issues in NEE 3.3

The following known issues are reported in the NEE 3.3 release.

Table 3: Known Issues NEE 3.3

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 Administrator 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 Administrator Console open.

Known Issues in NEE 3.2.1

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

Table 4: Known Issues NEE 3.2.1

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 NESdiagnostics 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".

Issue Number	Description
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.
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 1.1.3

Documentation for the Nymi Connected Worker Platform can be found in the release package delivered for CWP 1.1.2.

Core Documentation

The following documentation is provided with the standard CWP 1.1.2 package. This table identifies revisions to documentation since the last release package.

Table 5: Core Product Documentation

Document Title	Version	Reference	Modifications
Nymi Connected Worker Platform Release Notes 1.1.3	1.0	Nymi_Connected_Worker_Platform_Release_Notes_1.1.2_v 1.pdf	Release notes for CWP 1.1.3
Nymi Overview Guide	4.0	NymiOverviewGuide_V4.pdf	No modifications
Nymi Deployment Guide	5.0	NymiDeploymentGuide_V5.pdf	No modifications
Nymi Administration Guide	5.0	NymiAdministrationGuide_V5.pdf	No modifications

Document Title	Version	Reference	Modifications
Nymi Smart Distancing & Contact Tracing Installation & Configuration Guide	2.0	NymiSDCTInstallandConfig_v2.pdf	No modifications
Nymi Troubleshooting Guide	5.0	NymiTroubleshootingGuide_v5.pdf	No modifications
Nymi Band Regulatory Guide	2.1	Nymi BandRegulatoryInformationGuide_V2.1.pdf	No modifications
Nymi Connected Worker Platform Security White Paper	3.0	NymiCWP_Security_WhitePaper_v3.0.pdf	No modifications
Nymi Third Party Licenses	4.0	NymiThirdPartyLicenses_V4_20210427.pdf	No modifications
Nymi API WebSocket Interface Guide	3.0	Nymi API WebSocket InterfaceGuide_V3.pdf	No modifications
Nymi API C Interface Guide	3.0	Nymi API C InterfaceGuide_V3.pdf	No modifications
Nymi API for Linux Guide	3.0	Nymi API for LinuxGuide_V3.pdf	No modifications

Secondary Documentation

The following documents offer additional support for the CWP 1.1.x solution. These documents are not included in the CWP 1.1.x package. Contact your Customer Success representative for additional details.

Table 6: Table 6:Secondary Documentation

Document Title	Version	Description
Nymi Band 3.0 Bulk Charger Reference Design	1.0	A reference diagram for a bulk charging solution for Nymi Bands.
Nymi Band 3.0 Charging Recommendation Guide	1.4	Nymi has provided a Charging recommendation guide with recommendations for bulk charging stations.
Nymi Band 3.0 Material Composition	1.1	A reference document outlining the surface materials composing the Gen 3.0 Nymi Band.
Nymi Band 3.0 Reliability Specification	1.1	A reference document outlining the reliability specifications for the Gen 3.0 Nymi Band.
Nymi Band 3.0 Cleaning Guide	1.3	A reference document that provides recommendations on appropriate cleaning procedure for the Gen 3.0 Nymi Band.
Nymi Band 3.0 Strap Extenders	1.0	Nymi has provided a guide on the installation and use of strap extenders for users whom the band is too small to comfortably fit their wrist.
Nymi Feature Availability	2.1	A reference document that provides an overview of the availability of features across release versions.
CWP Storage and Transmission of Personal Data	2.0	This guide explains how personal data (or PII) is handled in the Nymi solution.
Nymi Band 2.0 and Nymi Band 3.0 Differences	1.1	A reference document that describes the differences between the Nymi Band 2.0 and 3.0 wearable device hardware.
Nymi Feature Availability	2.1	A reference document that describes availability of features with the Nymi Band across NEE and CWP versions.

Document Title	Version	Description
Connected Worker Platform FAQ	1.3	A reference document that answers common questions about the Connected Worker Platform.
Connected Worker Platform 1.1.0 Technical Specification	1.14	A reference document that describes the technical specifications of the Nymi Band and Connected Worker Platform solution.
Secure Fingerprint Template Storage on the Nymi Band	1.1	A reference document that explains how the Nymi Band maintains user privacy and security with fingerprint data.

Appendix 2: NFC Readers Tested for CWP 1.1.x

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 1.1.x. Note that the level of ongoing testing is indicated as follows:

1. Recommended Readers - best performance; testing planned with every CWP release going forward from CWP 1.1.0.
2. Supported Readers - meet specific use cases but may not perform as well as a recommended reader; testing planned with every CWP release going forward from CWP 1.1.0.
3. Verified Readers - 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 7: NFC Readers

NFC Reader Model	Status
HID Omnikey 5022	Recommended

ACS ACR122U	Verified with NEE 3.3.0
Systec CONNECT BOX	Verified with NEE 3.3.0
Elatec TWN4 LEGIC NFC USB	Verified with NEE 3.3.0
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