Overview Guide

Nymi Connected Worker Platform
v1.0
2023-09-21

Contents

Preface

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

Purpose

This document provides overview information about the Connected Worker Platform (CWP) solution, such as component overview, deployment options, and supporting documentation information.

Audience

This guide provides information to CWP Administrators. An CWP Administrator is the person in the enterprise that manages the Connected Worker Platform for their work place.

Third-party Licenses

This product comprises subject matter which was obtained under an open source licenses. For details about Third-party Licenses, see the Nymi Connected Worker Platform—Third Party Licenses Document which is included in the release package.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	September 21, 2023	First release of this document for the CWP 1.13.0 release.

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

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

Nymi Connected Worker Platform Environment

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

The Connected Worker Platform consists of both hardware and software components. The Nymi Band is a wearable device that allows wireless communication between users and digital systems. On-device biometrics ensure the identity of the user while integrated sensors convey information about the individual and their environment. Combined with supporting software, Connected Worker Platform addresses numerous use cases. These include, but are not limited to:

- Physical Access
- Passwordless Windows Logon
- Automatic Terminal Locking
- Secure Printing
- Manufacturing Execution System (MES) Signing

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.
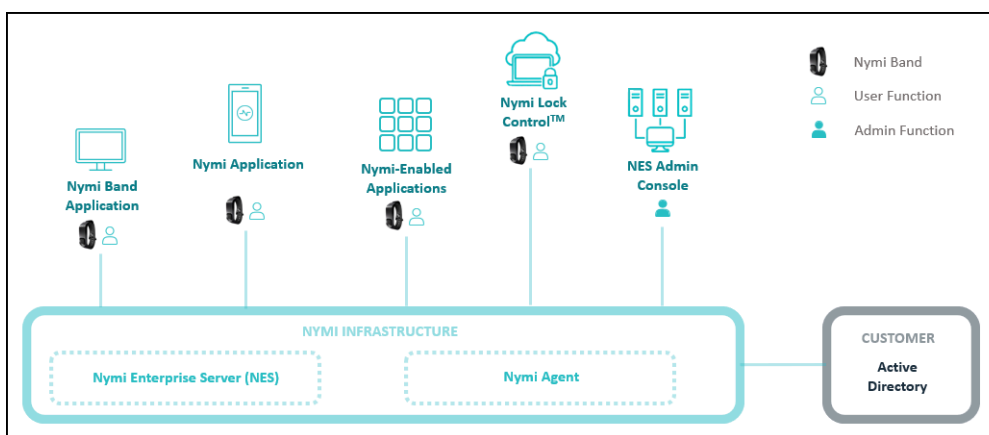

Figure 1: Nymi Connected Worker Platform Core Components

The Connected Worker Platform solution can be used as a stand-alone solution or integrated into third-party applications, devices, or services.

Nymi Band

The Connected Worker Platform features the Nymi Band – a wearable that combines multi-factor authentication with embedded sensors. Fingerprint biometrics, ECG liveness detection and on-body detection give strong identity assurance of the individual user. Near-Field Communications (NFC) and Bluetooth Low Energy (BLE) technology are incorporated into the Nymi Band to allow for wireless communication between the user and digital systems. The Nymi Band is IP66 and IP67 rated to ensure it will perform in challenging environments.

The Nymi Band communicates securely with an NEA that is built using the Nymi API over BLE and NFC protocols. The Nymi Band provides persistent authentication through on-body detection technology.

A Nymi Band user taps the Nymi Band against the NFC Reader or, if `BLE Tap Intent` is enabled, the BLED112 adapter (USB dongle) to indicate the intent to perform an operation. For example, a user can tap an authenticated Nymi Band on an NFC Reader that is attached to an user terminal to unlock their session on the machine.

Bluetooth Communication

The Nymi Band uses Bluetooth Low Energy (BLE) to interact with the Nymi Bluetooth Endpoint service. The Nymi Band BLE communication does not rely on Bluetooth security. All security is implemented using strong, standard-based cryptography.

Note:

BLE communication with a Windows terminal requires a BLE radio antenna. The BLE radio antenna is present on a BLE adapter.

Refer to the Nymi Connected Worker Platform—Deployment Guide for detailed system requirements. Refer to the Nymi Connected Worker Platform—Administration Guide for instructions on enabling BLE Tap Intent.

Near Field Communication

The Nymi Band supports a number of features over Near Field Communication (NFC). The Nymi Band also supports the *tap-to-authenticate* use case, in which the NFC Universal Identifier (UID) is transmitted over NFC to identify a Nymi Band, and the authentication is performed securely over BLE.

Nymi Application

Nymi-supplied native iOS application that provides iOS devices with the ability to perform authentication tasks with a Nymi Band in a web-based and native iOS Nymi-enabled Application.

Nymi Band Application

Nymi Band Application is a Windows desktop application that enables end users to enroll their Nymi Band. Enrollment is the process of associating a new user's identity with a Nymi Band. The Nymi Band Application orchestrates user authentication, Nymi Band authentication, enrollment of fingerprint and other authentication credentials, and provides the necessary information to NES and/or the EAM Console for storage to support subsequent management and operation of Nymi Bands.

During enrollment, it is possible to configure the Nymi Band Application to create a corporate credential authenticator in addition to the fingerprint authenticator. With a corporate credential authenticator, a user can use their corporate username and password to authenticate to the Nymi Band instead of their fingerprint.

Nymi Lock Control

Nymi Lock Control is an application that provides users with the ability to manage access to a terminal, without typing a username and password. Nymi Lock Control verifies user access through Active Directory.

When you install Nymi Lock Control on a user terminal, the following functionality is supported:

- Unlocking or logging into a terminal by tapping an authenticated Nymi Band on an NFC reader that is attached to the terminal.
- Unlocking or logging into a terminal by placing an authenticated Nymi Band within the range of the Bluetooth adapter, and clicking the `Submit` button on the `Nymi Credential Provider Login` screen.
- Automatically unlocking or logging into a terminal by being placing an authenticated Nymi Band within range of the Bluetooth adapter and tapping their keyboard.
- Locking the user terminal when the authenticated user is not within the Bluetooth range of the terminal or when the user removes their Nymi Band.
- Preventing a user terminal from locking by keeping an authenticated Nymi Band within Bluetooth range.

Note: Nymi Lock Control is a single domain solution and does not support cross-domain access. All terminals must be on the same domain as the Nymi Enterprise Server host.

Nymi Enterprise Server

The Nymi Enterprise Server (NES) is the server component of the Connected Worker Platform and is responsible for the deployment, operations, and management of Nymi Bands and other Nymi software components. Primarily, it enables storage and retrieval of information

that is necessary for Nymi Band usage and management. Managing security policies, issuing authentication tokens to Nymi-enabled Applications (NEAs) and allowing user authentication between Active Directory and the Nymi Band are all functions of NES.

NES can be configured as a single instance or in a multi-server deployment.

NES makes use of Microsoft Internet Information Service (IIS) and Microsoft SQL Server, and is compatible with Microsoft Windows Server 2016 and Microsoft Windows Server 2019.

NES has a series of responsibilities:

- Manage the association between the Nymi Band and the corporate credentials
- Manage the enrollment of Nymi components into the ecosystem (for example, registers Nymi Bands, or Nymi-enabled Applications or Nymi Band Application)
- Manage the policies of the Nymi Band ecosystem (for example, when Nymi Bands are required to be authenticated through biometrics)

Nymi Enterprise Server Sub-components

NES manages centralized functionalities that are required for the deployment, operations and management of the Nymi Bands and other Nymi software components. NES has several sub-components that manage different areas of functionality.

Nymi Administration Console: Provides Nymi Band management options and NES security policy configuration.

Enrollment Service: Issues authentication tokens to NEAs by using the Nymi Token Service (NTS).

Authentication Service: Provides authentication functions for enterprise users and machines.

Directory and Policy Service: Allows storage and retrieval of information that is necessary for usage and management of the Nymi Bands and other Nymi software components.

Nymi Third Party Components

Nymi Enterprise Server(NES) interacts with Microsoft SQL and Microsoft IIS.

- Microsoft SQL—NES stores user, Nymi Band and policy configuration information in a SQL database. The SQL database can reside on the same server as NES or on a server in the same domain as the NES server.
- Microsoft IIS—The NES installation creates a web instance in IIS with the following web services:
  - `instance_name`_ES for the Enrollment Service.
  - `instance_name`_AS for the Authentication Service.
  - `instance_name`_DS for the Directory and Policy Service.

  The IIS server can reside on the same server as NES or on a server in the same domain as the NES server.

Nymi SDK Components

Nymi SDK delivers an API through one of the following mechanisms:

- Nymi API(NAPI)—A Windows Dynamically Linkable Library(DLL) named *nymi_api.dll* that developers include in a Windows application that supports a locally linked library.
- NBE_iOS_Framework—A framework to build web-based or native NEAs that are accessed by iOS devices.

The Nymi SDK includes the Nymi Runtime, an application that facilitates communication between an NEA and Nymi Bands. The Nymi Runtime consists of two components that you can install together or separately:

- Nymi Agent— Provides BLE management, manages operations and message routing. Facilitates communication between NEAs and the Nymi Band, and maintains knowledge of the Nymi Band presence and authenticated states.

  You can install Nymi Agent on each workstation or install Nymi Agent in a central location, and then specify the location of the Nymi Agent in an Nymi Bluetooth Endpoint Daemon (NBEd) configuration file(*nbe.toml*).
- Nymi Bluetooth Endpoint— Provides an interface between the Bluetooth Adapter (BLE) and the Nymi Agent. You deploy Nymi Bluetooth Endpoint Daemon (NBEd) on individual workstations to provide local BLE communication with Nymi Bands through the Nymi-provided BLE Adapter. . For iOS devices, the Nymi Application includes the Nymi Bluetooth Endpoint

Nymi WebAPI
The Nymi WebAPI allows developers to utilize the websocket functionality of the Nymi SDK in a web-based or native application. The Nymi WebAPI architecture is part of the Nymi SDK and enabled in a Nymi Agent configuration file.

SDK Documentation and Sample Code

Nymi provides developers with Sample code to assist them in integrating the SDK with their application

The following sample applications are included in the SDK package:

- Nymi API C Interface:The sample application is located within the package at: *nymi-sdk/C/ sdkSamples/SDK_Sample*.
- Nymi API for Linux: The sample application is located within the package at: *nymi-sdk/linux/ examples/python*.
- Nymi WebAPI (Windows): The sample application is located within the package at: *nymi-sdk/webapi/sdkSamples/SDK_Sample*.
- Nymi WebAPI (iOS) includes two sample applications:

- Nymi Test App—A sample application that demonstrates to iOS developers how to integrate the SDK into their native iOS application, which is located within the package at: *nymi-sdk/ios/sampleApps/NymiTestApp*.
- Nymi Sample Browser App—A sample browser application that demonstrates to iOS developers how to integrate the SDK into their web-based applications and interact with the Nymi Application to support the completion of e-signatures on an iOS device, which is located within the package at: *nymi-sdk/iOS/sampleApps/browserApp*.

SDK Documentation

Nymi provides documentation for each interface which provides information about how to use the functionality that is available in the Nymi API that is part of Connected Worker Platform.

Nymi-Enabled Applications

Nymi provides an SDK that allows developers to build Nymi-enabled Application (NEAs). When the NEA is integrated with Connected Worker Platform, the solution can perform tasks such as application login, and electronic signatures.

NEAs can be a web application or native application that makes use of the Nymi Band's security functions.

Nymi Band Management Console

The Nymi Band Management Console is a web-based interface that provides administrators with the ability to manage and schedule firmware updates from a central location, and auditors with the ability to download information about Nymi Bands in *CSV* format for analysis. The Nymi Band Management Console stores information about Nymi Band firmware updates in a SQL database and uses a Docker container to store firmware images.

Domain Environment

The Connected Worker Platform is designed for seamless integration into enterprise Active Directory (AD) environments.

The Connected Worker Platform integration with AD is limited to performing authentication of users and computers, lookup of user status and group membership. The Connected Worker Platform does not write to AD. The Connected Worker Platform integration uses AD for the following purposes:

- For user authentication by the Nymi Band Application, to enable user management of Nymi Bands (e.g., Nymi Band enrollment).
- For user authentication and authorization during access to NES Administrator Console.
- For verification of user status (for example, to determine if a is user account still active in AD) during an assert identity operation.
- For client authentication when the NAPI DLL needs to access NES for privileged operations.

Nymi Enterprise Server Deployment Options

Nymi offers a number of standard configurations. Before you begin deploying the Connected Worker Platform solution, it is important to first determine how Nymi software fits into your environment.

See the following sections for more information:

- **Nymi Enterprise Server Deployments** for information about single server deployments or deployments using NES and Evidian Access Management (EAM).
- **Nymi Software Development Kit Deployments** for information about Nymi Software Development Kit deployments.

Nymi Enterprise Server Deployments

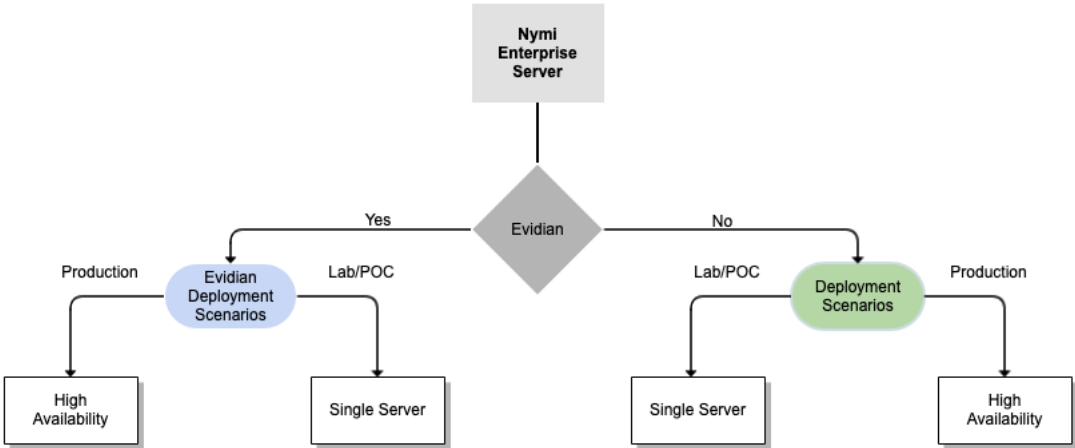The Connected Worker Platform can be deployed in the following configurations:

Figure 2: Nymi Enterprise Server Deployments

Deployment Decisions

Table 2: Deployment Options

Deployment Decision	Deployments Details	NymiDocumentation
NES is deployed in an Evidian environment in a lab or proof of concept (POC) environment	A single server deployed in a lab or POC environment	Nymi Connected Worker Platform with Evidian Guide
NES is deployed in an Evidian environment in a production environment	Multiple servers configured for High Availability production environment	Nymi Connected Worker Platform with Evidian Guide, Nymi Connected Worker Platform—Deployment Guide
NES is deployed in a lab or proof of concept (POC) environment without Evidian	A single server deployed in a lab or POC environment	Nymi Connected Worker Platform—Deployment Guide
NES is deployed in a production environment without Evidian	Multiple servers configured for High Availability in a production environment	*NES Failover High Availability Overview* section of the Nymi Connected Worker Platform—Deployment Guide

NES Single Server with Evidian

The NES Single Server with Evidian deployment provides you with a single sign-on solution. In this environment, the Nymi Band can interact with legacy applications that cannot otherwise be modified. The following software is required:

- Microsoft Windows server with the NES software
- Evidian Access Management (EAM) Controller software

NES with Evidian supporting High Availability

The NES with Evidian supporting High Availability deployment utilizes multiple NES and EAM Controller instances to support high availability for production deployments. This deployment uses a centralized Nymi Agent.

NES Single Server

The NES Single Server is a lightweight deployment that uses a standalone server to provide full Nymi enterprise services to the Nymi Bands and NEAs. Use the Single Server deployment when you're deploying the Connected Worker Platform in a lab or proof-of-concept environment, where high availability is not a concern.

- In this configuration you install NES, SQL Database, and IIS on the same server

NES Supporting High Availability

You can deploy NES in a High Availability (HA) configuration that uses DNS failover. This configuration is useful for maintaining NES availability by deploying multiple servers. When an NES server failure occurs, the DNS switches to a second NES node to avoid prolonged periods of downtime. For details about High Availability support, refer to the Nymi Connected Worker Platform—Deployment Guide.

Nymi SDK Component Deployments

This section describes the Nymi-supported SDK component deployments.

Nymi offers a number of SDK component deployment configurations that enable you to create NEAs depending upon the configuration of the Nymi solution and your environment.
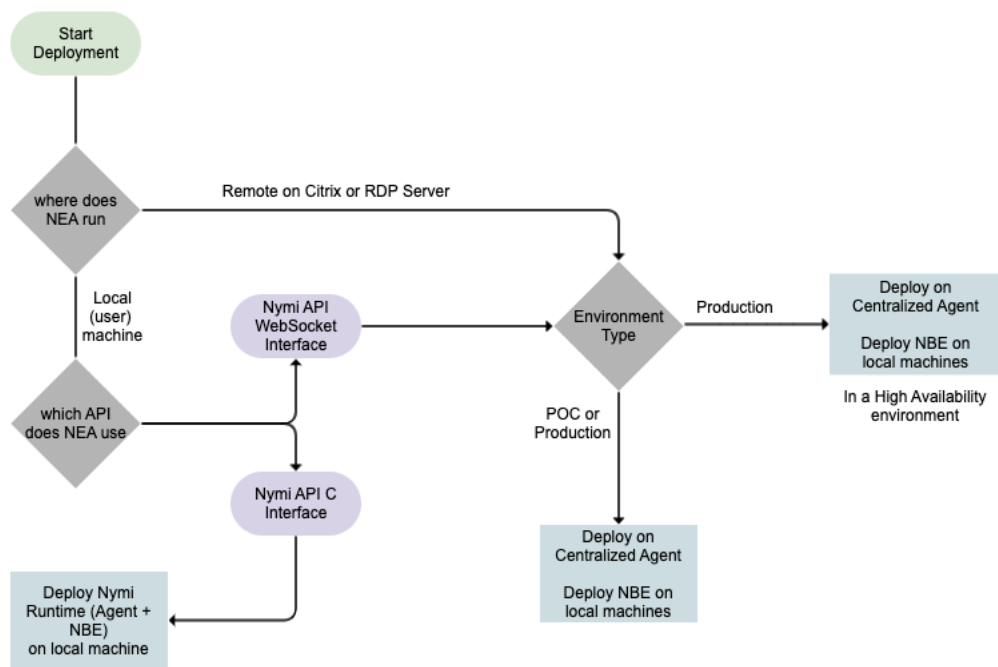
Figure 3: Nymi SDK Deployments

Deployment Decisions

Table 3: SDK Deployment Decisions

Deployments Details	Connected Worker Platform Documentation
On a local user terminal.	Nymi SDK for WebSocket Developer's Guide
Remotely on a Citrix or RDP Server: If the deployment is for a POC or prilot environment, then deploy on a centralized Nymi Agent. Install the Nymi Bluetooth Endpoint on each user terminal.	Nymi SDK for WebSocket Developer's Guide
Remotely on a Citrix or RDP Server: If the deployment is for a production environment, then deploy in a high availability environment with a centralized Nymi Agent. Install the Nymi Bluetooth Endpoint on each user terminal.	Nymi SDK for WebSocket Developer's Guide
Deploy Nymi Runtime (Nymi Agent + Nymi Bluetooth Endpoint) on the user terminal.	Nymi SDK for WebSocket Developer's GuideNymi SDK for Linux Developer's Guide

Centralized Nymi Agent Deployment

A centralized Nymi Agent deployment in either a single server deployment or with high availability enables developers to use the Nymi WebAPI to provide the functionality of the Nymi SDK over a WebSocket connection. In the deployment, consider the following information:

- Extend existing Connected Worker Platform deployments by adding web clients that utilize the Nymi WebAPI Service without requiring re-deployment of any pre-existing Nymi components.
- Install the Nymi Bluetooth Endpoint on the same user terminal that is running the remote client software.
- Configure the NEA to have knowledge of the remote session address, so that it can connect to the Nymi Agent.

Local Nymi Runtime Deployment

Deploy the Nymi Runtime (Nymi Agent and Nymi Bluetooth Endpoint) on a local machine to support the NEA that uses the Nymi API C Interface. Alternatively, use the Nymi API C Interface in a NEA that runs on a Citrix or RDP server. This configuration requires a centralized Nymi Agent.

- Nymi Bluetooth Endpoint establishes and secures the bluetooth connection to the Nymi Band.
- Nymi Runtime is installed on the local machine or on any machine where the NEA executes.

Nymi Documentation

Nymi provides a suite of documentation to help you understand concepts, processes and procedures associated with the Connected Worker Platform. Each guide contains information that is specific to a component or group of components included in the Connected Worker Platform. The following information provides a list of guides that are available from Nymi and a short description about the contents of each guide. Each Nymi release may contain all or a subset of the entire documentation set.

- **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 device.

- **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 with Evidian Installation and Configuration Guide**

  The Nymi Connected Worker Platform with Evidian Guides provides information about installing the Evidian components and configuration options based on your deployment. Separate guides are provided for Wearable, RFID-only, and mixed Wearable and RFID-only deployments.

- **Nymi Connected Worker Platform with Evidian Troubleshooting Guide**

  This document provides overview information about how to troubleshoot issues that you might experience when using the Nymi solution with Evidian.

- **Nymi SDK for C Developer's Guide**

  This document provides information about how to develop Nymi-enabled Applications by using the Nymi API(NAPI).

- **Nymi SDK for WebSocket Developer's Guide**

  This document provides information about how to understand and develop Nymi-enabled Applications (NEA) by utilizing the functionality of the Nymi SDK, over a WebSocket connection that is managed by a web-based or other application. Separate guides are provided for Windows and iOS application development.

- **Nymi Connected Worker Platform—Troubleshooting Guide**

This document provides information about how to troubleshoot issues and the error messages that you might experience with the NES Administrator Console, the Nymi Enterprise Server deployment, the Nymi Band, and the Nymi Band Application.

- **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.