Nymi With Evidian Functional Specifications

Connected Worker Platform
1.5.x - 1.14.x
2022-10-19

Contents

Introduction

This document provides a description of the interfaces, functions, and behaviour of the various software components in the Connected Worker Platform solution.

Nymi creates and maintains this document to provide customers with information about how the Nymi Solution is designed to address user specifications. The user-created User Requirements Specifications document describes the user specifications. The Nymi-defined acceptance criteria for functional requirements provide the source of information for the functional specifications. The Design/Configuration Specification document provides more information about the functional specifications outlined in this document.

Overview

The Nymi Solution provides enterprise customers with components that support the ability to lock and unlock a user terminal and perform authentication-related tasks in MES application by tapping the Nymi Band against a Bluetooth adapter or NFC reader, and components that support Smart Distancing and Contact Tracing.

Nymi Connected Worker Platform with Evidian Access Management Solution

The Nymi-Evidian solution extends the use of the Nymi Band. With Evidian Authentication Manager, a user can use their Nymi Band to lock and unlock a Windows desktop. With Evidian Single Sign On (SSO), a user can use their Nymi Band to perform MES authentication events. There are several supported deployment configurations in the Nymi-Evidian solution.

The Nymi Band supports two authentication methods in an Evidian environment:

- Wearable (NFC with Bluetooth)—During communications, tapping the Nymi Band on an NFC reader initiates the authentication, and then the Nymi Band is cryptographically authenticated over Bluetooth. This is the default authentication method.
- RFID-only—During communications, the Nymi Band is identified by using only the NFC UID without cryptographic authentication.

Nymi provides you with one or more *TokenManagerStructure.xml* files, based on your configuration needs. The *TokenManagerStructure.xml* file defines the supported authentication types and modules that implement the authentication modules. The contents of the TokenManagerStructure file are loaded on the EAM Controller and the default configuration is pushed by the EAM Controller to the EAM Clients. To override the default authentication method on a terminal, place a different version of the TokenManagerStructure file locally on the terminal.

The *TokenManagerStructure* file for the Nymi Band as a Wearable device differs from the *TokenManagerStructure* for the Nymi Band as an RFID-only device.

There are several supported deployment configurations in the Nymi-Evidian solution.

- Nymi Band configured as a wearable device
- Nymi Band configured as an RFID-only device
- Nymi Band configured as a mixed use device

Note: This document is specific to an Evidian configuration that uses Active Directory Lightweight Directory Services to provide data storage and retrieval support for directory-enabled applications.

Coexistence of Nymi-direct integrations and Evidian integrations

The Connected Worker Platform now supports the co-existence of Nymi-direct integration, and Evidian integration, within the same environment.

Nymi-direct integration supports:

- Nymi-enabled Application (NEAs) that make use of the Nymi SDK to perform application logons and electron signatures.
- Operating systems and applications that support the FIDO2 standard, to perform OS logon / unlock, application logon, and electronic signature.

Evidian integration supports:

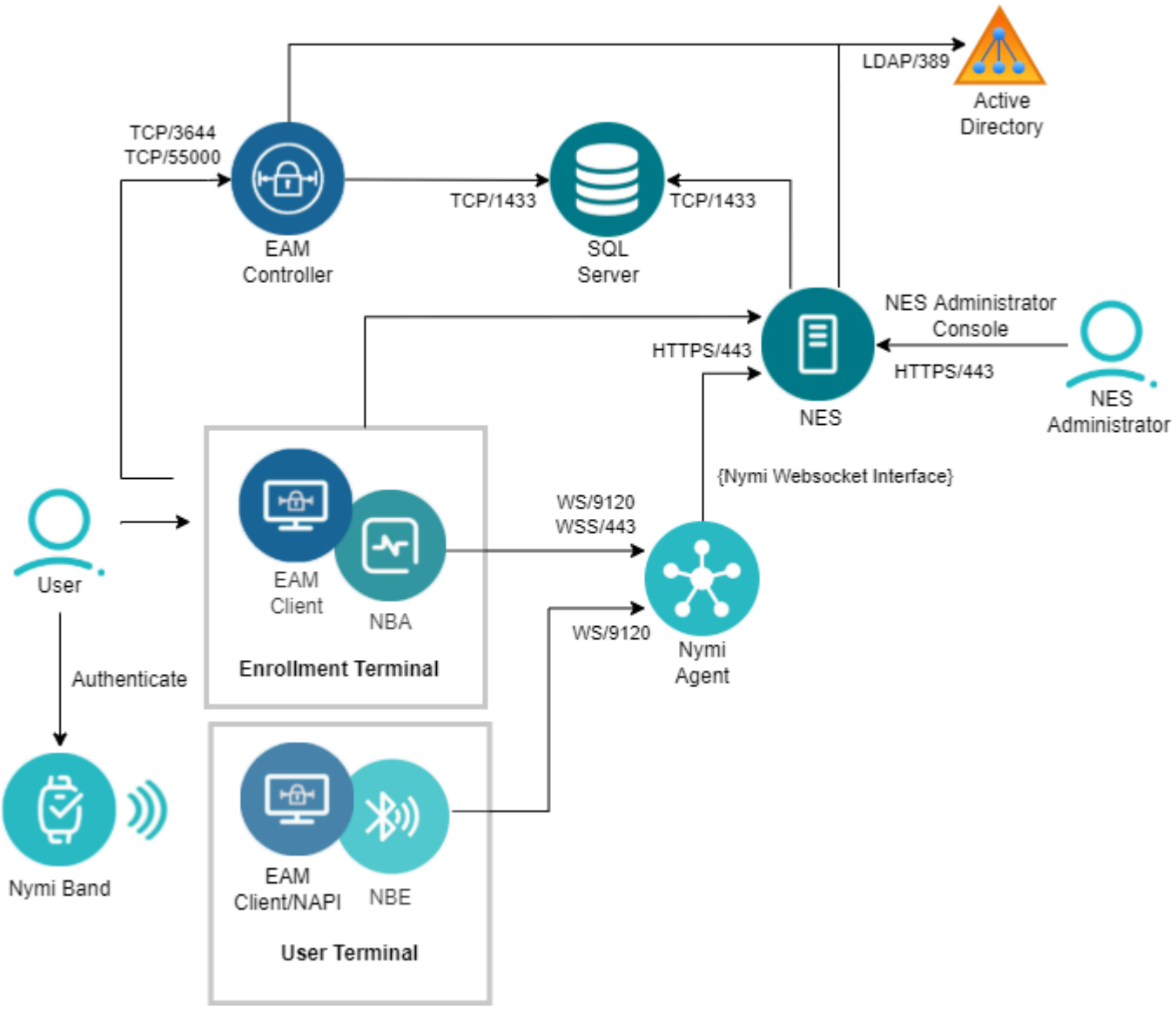
- Evidian-integrated applications, which leverage Evidian Single Sign-on (SSO) support to perform application logins and/or electronic signatures.
- Evidian Windows logon, which makes use of Evidian to perform Windows session logon, unlock, and relock when the user is away from the Windows terminal.

In these Evidian integration scenarios, Nymi Bands are integrated with the EAM Client and EAM Controller.

You can configure Connected Worker Platform to support either Nymi-direct integration only (default), or to support both Nymi-direct integration and Evidian integration simultaneously.

Nymi-Evidian Architecture - Wearable Device

The following image represents the components in a Nymi-Evidian solution where the Nymi Band is used as a wearable device.



Enrollment Terminal

The Windows 10 machine where users enroll their Nymi Band.

User Terminal

The workstation on which you install Nymi components and the Evidian Access Manager (EAM) client.

Nymi Band Application

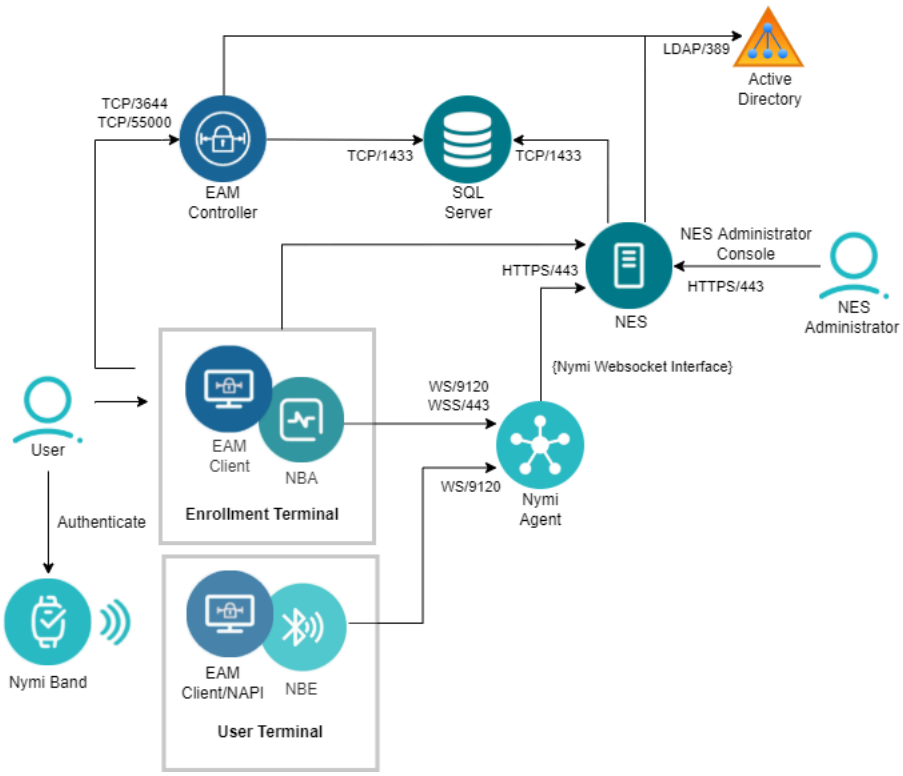
A native Windows application that is used to register biometric, employee ID, and Nymi Band with the enterprise. The Evidian version of the Nymi Band Application integrates directly to the Evidian ecosystem and facilitates communication between NES and the Nymi Bands. The Nymi Connected Worker Platform—Administration

	Guide provides more information about the Nymi Band Application.
Enterprise Access Management Client	The client-side Evidian software that provides users with a single sign-on (SSO) experience at the user terminal.
Nymi Enterprise Server	Management software for the Nymi Bands within the Nymi ecosystem. Nymi Enterprise Server (NES) ensures the validity of the hardware in the system. NES includes the NES Administrator Console, a web application that administrators can use to manage the Nymi Bands within the ecosystem.
Evidian Enterprise Access Management Controller	Evidian Enterprise Access Management (EAM) Controller allows centralization of User Access policy definition and audit events. Includes Evidian Enterprise SSO software that provides agile single sign-on (SSO). The EAM Console application provides the interface to perform management activities.
Corporate Directory	An Active Directory server that provides authentication services.
NFC Reader	Captures the NFC UID of the Nymi Band, which is used when an operator performs and SSO authentication event.
BLED112 Dongle	Nymi Band uses Bluetooth Low Energy (BLE) to interact with external components and services. Nymi Band BLE communication does not rely on Bluetooth security. All security is implemented using strong, standard-based cryptography. A BLE adapter (BLED112) is required on the enrollment terminal and user terminals.

Nymi-Evidian Architecture

In the configuration, two TokenManagerStructure files are used. Upload the RFID-only file to the EAM Controller and then copy the Wearable file to the enrollment terminal

The following image represents the components in a Nymi-Evidian solution where the Nymi Band is used as an RFID-only device.



Enrollment Terminal

The Windows 10 machine where users enroll their Nymi Band.

User Terminal

The workstation on which you install Nymi components and the Evidian Access Manager (EAM) client.

Nymi Band Application

A native Windows application that is used to register biometric, employee ID, and Nymi Band with the enterprise. The Evidian version of the Nymi Band Application integrates directly to the Evidian ecosystem and facilitates communication between NES and the Nymi Bands. The Nymi Connected Worker Platform—Administration Guide provides more information about the Nymi Band Application.

Enterprise Access Management Client

Also known as the Evidian Client. The client-side Evidian software that provides users with a single sign-on (SSO) experience at the user terminal.

Nymi Enterprise Server

Management software for the Nymi Bands within the Nymi ecosystem. Nymi Enterprise Server (NES) ensures the validity of the hardware in the system. NES includes the NES Administrator Console, a web application that administrators

	can use to manage the Nymi Bands within the ecosystem. NES includes: • Enrollment Service - Authenticates, validates, and authorizes certificate requests from requesters, such as the Nymi Band Application and Nymi-enabled Application(NEAs. • Directory and Policy Service - Maintains the NES database, and provides the IIS web service that allows the NES Administrator Console to access the NES database. • Authentication Service - Provides authentication and authorization support for domain users and computers. The service currently uses an Active Directory (LDAP) interface.
Evidian Enterprise Access Management Controller	Evidian Enterprise Access Management (EAM Controller) allows centralization of User Access policy definition and audit events. Includes Evidian Enterprise SSO software that provides agile single sign-on (SSO). The EAM Console application provides the interface to perform management activities.
Corporate Directory	A server such as Windows domain controller that provides authentication services, such as Active Directory.
NFC Reader	Captures the NFC ID of the Nymi Band, which is used when an operator performs an SSO authentication event.
BLE112 Dongle	Nymi Band uses Blue Tooth Low Energy (BLE) to interact with external components and services. Nymi Band BLE communication does not rely on Blue tooth security. All security is implemented using strong, standard-based cryptography. A BLE adapter (BLED112) is required on the enrollment terminal.

Components in a iOS Only Environment

The Connected Worker Platform(CWP) enables users to use Nymi Bands and administrators to manage Nymi Bands and CWP components in an enterprise setting.

CWP is comprised of Nymi-specific components and enterprise components, as shown in the following figure.

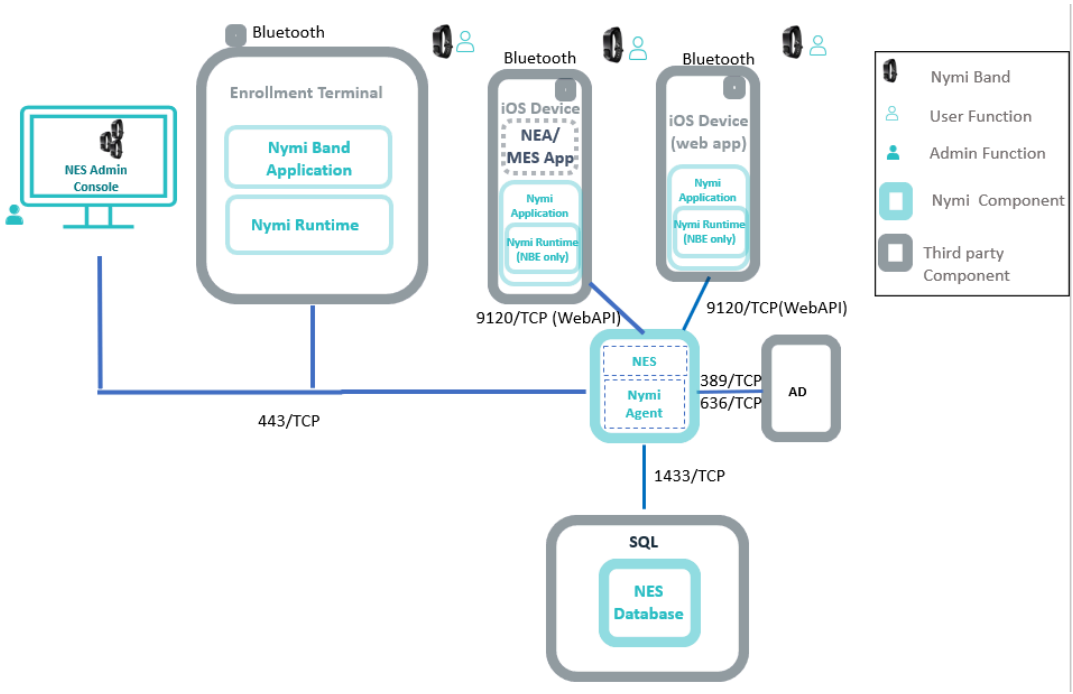


Figure 1: CWP components and firewall connection ports

The CWP consists of the following components.

Table 1: CWP Components

Component	Description
Enrollment Terminal	Windows 10 endpoint that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal and is used to enroll a new user and link them to their Nymi Band. The Nymi Band Application requires the Nymi Runtime application, which the Nymi Band Application automatically installs. The Nymi Band Application communicates with the Nymi Band through the Nymi-supplied Bluetooth adapter, which you plug into a USB port on the enrollment terminal.
Nymi Runtime	A Windows application that you install on the enrollment terminal and user terminals. Nymi Runtime includes the Nymi Agent and Nymi Bluetooth Endpoint components. Nymi Runtime supports communication between NES, the Nymi Band, NEAs, the Nymi Band Application and Nymi Lock Control.

Component	Description
User Terminal	Windows 10 endpoint on which you install Nymi components that allow users to perform authentication tasks with the Nymi Band. Use a supported Web Browser to connect to the POMSnet interface. To support authentication operations with the Nymi Band, plug an NFC reader and Bluetooth adapter into available USB ports on the user terminal. Starting with POMSnet Aquila 2022.1.0, the Bluetooth adapter is optional.
Nymi Band	A wearable device that is activated by the assigned user's biometrics. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled. See the Nymi Band section in this guide for more information.
Nymi-enabled Application	Developers can create corporate applications that integrate with Connected Worker Platform by using the Nymi WebAPI component of the Nymi API. These applications are called Nymi-enabled Applications (NEAs) and include Manufacturing Execution Systems (MES), Single Sign-On (SSO), and Human Machine Interface (HMI) applications. An NEA communicates with the Nymi Runtime components.
Nymi Lock Control	A Windows application that allows the user to unlock their terminal without entering their username and password, and automatically lock the user terminal when they walk away.
iOS Device	An iPad endpoint that users use to: • Perform authentication tasks in a web-based Nymi-enabled Application(NEA). • Perform authentication tasks in a native iOS NEA.
Nymi Application	Required on the iOS devices to perform authentication tasks. Nymi Application is a Nymi-supplied native iOS application that: • Embeds the Nymi Bluetooth Endpoint application, which provides an interface between the native Bluetooth Adapter (BLE) and the Nymi Agent. • Detects an intent to perform an authentication task with a Nymi Band (a tap) and passes the request to the NEA.

Component	Description
Nymi Enterprise Server (NES)	• A management server and collection of services that provides the NES Administrator Console and coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates. Includes the following services: • Enrollment Service (ES)—Authenticates, validates, and authorizes certificate requests from requesters, such as the Nymi Band Application and NEAs. • Directory and Policy Services (DPS)—Maintains the NES database, which contains a list of Active Directory (AD) users and the Nymi Bands that are associated with each user. Provides IIS web services, which allows the NES Administrator Console access to the NES database. • Authentication Service (AS)—Provides authentication and authorization support for domain users and computers. AS uses adapters to interface with external directory and database systems, such as an AD adapter to interface with Active Directory.
SQL Server	Database that contains table that store information about NES configuration and Nymi Bands. For Proof of Concept (POC) and pre-production environments, you can use the Nymi-provided SQL Server Express software. For production environments Nymi recommends that you use SQL server.
Domain Controller (DC)	Windows server with Active Directory.

Component	Description
Centralized Nymi Agent	Required for iOS devices. 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. The Nymi Agent is installed in a central location on a single machine or a cluster of two or more machines that is accessible to all user terminals, for example on the NES server. To enable Nymi WebAPI communications between the Nymi Agent and the Nymi Bluetooth Endpoint, you must configure a *nymi_agent.toml* file. For web-based and native iOS NEAs that are accessed by an iOS device, the NEA defines the Nymi Agent host and communication port number. The *Nymi SDK for WebSocket Developer's Guide* provides more information.

Use Case and Workflow

A user with an authenticated Nymi Band can perform an action that requires an authentication task, such as an e-signature in a web-based Nymi-enabled Application(NEA)

A typical worflow for a Nymi Band user is as follows:

- Nymi Band user authenticates to their Nymi Band.
- Nymi Band user connects to a web-based NEA on their iOS device and performs an activity that requires an e-signature.
- NEA launches the Nymi Application.
- Nymi Application appears on the iOS device screen and prompts the user to perform a Nymi Band tap to complete the authentication task.
- User taps their Nymi Band on the bluetooth adapter on the iOS device.
- Nymi Application communicates with the Nymi Band through the integrated bluetooth adapter on the iOS device.
- Nymi Application communicates with the web-based NEA to complete the authentication task after the user successfully completes the Nymi Band tap.

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.

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 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 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 SDK

The Nymi SDK serves two purposes:

- Provides access to the Nymi API which enables developers to create NEAs.
- Provides Nymi Runtime (including the Nymi Agent and Nymi Bluetooth Endpoint) that communicates with Nymi Bands.

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.

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 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 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 theNymi 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.

Functions

The following functions represent high level description is broken down into individual functions including performance, safety and security, functions which are configurable, traceability to requirements in the URS and failure conditions, actions, logfiles and diagnostics.

Functions in the Nymi solution include configurations, NES enrollment and the Nymi SDK.

Configurations

The following table summarizes the functional specifications and related user specifications for configuration requirements.

Table 2: Functional specifications for configuration

URS #	User Specification	FS #	Functional Specification
URS-029	The Solution shall be configured so that there is no single point of failure.	FS-CFG-02	Create a document that describes the steps to deploy Nymi Agent so that it can achieve 99.9% availability

Connected Worker Platform Pre-requisite Requirements

The host on which you deploy the NES software must meet the following minimum software and hardware requirements.

NES Requirements

The following sections define the hardware and software requirements to consider before you deploy NES.

Hardware Requirements

The NES hardware requirements differ based on the nature of user operations, load and other software that is deployed on the same server. The following section lists the recommendations for minimum hardware requirements.

- 1-5000 users:
  - 4 Core CPU
  - 8GB RAM
  - 20GB free disk space

- 5000-10000 users:
  - 4 Core CPU
  - 16GB RAM
  - 40GB free disk space

Software Requirements

NES has the following software requirements.

- Microsoft Windows Server 2016 or 2019

  Note: Ensure that the NES host is not a Domain Controller (DC).
- Microsoft IIS
- Microsoft .NET Framework 4.8

  Note: The NES installation package includes Microsoft .NET Framework 4.8, and installs the software if required.

Software requirements
Hardware requirements

Minimum Requirements for the Enrollment Terminal

The section summarizes the minimum software and hardware requirements for the enrollment terminal,

Software Requirements

- Windows 10, 64-bit
- Windows 7, 64-bit
- Nymi Band Application

  Note: It is recommended to use 125% scaling and 1920 x 1080 screen resolution for the terminal hosting the Nymi Band Application.

Hardware Requirements

- 4GB RAM
- 5GB free disk space
- 2 core CPU (recommended)
- 1 USB 2.0 port
- Nymi-supplied bluetooth adapter

Nymi Lock Control Considerations

Review the following information about Nymi Lock Control

- Nymi Lock Control is a single domain solution. All terminals must be on the same domain as the Nymi Enterprise Server host, not across separate domains.

- Nymi Lock Control users can lock the desktop of a user terminal and the desktop of a Microsoft Remote Desktop Connection and Citrix when Network Level Authentication (NLA) is disabled.
- Each user terminal requires a connected Bluetooth Low Energy (BLE) radio antenna, such as a Bluegiga BLE adapter..

User Terminal Requirements

User terminals are endpoints that can perform different functions in the environment, including enrollment, MES authentication tasks, andand desktop locking and unlocking with Nymi Lock Control. User terminals include thick clients and thin clients.

Hardware and Software Requirements

All thick client user terminals require connectivity to the server on which you install Nymi Enterprise Server(NES). The following table summarizes the supported operating systems and the hardware device requirements for each user terminal use case.

Note: You can configure and use a user terminal for multiple use cases.

Use Cases	Supported Operating System/ Browser	Hardware
Enrollment	• Windows 10, 64-bit, minimum build version 1607 • Windows 7, 64-bit **Note:** Nymi recommends that you use 125% scaling and 1920 x 1080 screen resolution for the terminal hosting the Nymi Band Application	• 4GB RAM • 5GB free disk space • 2 core CPU (recommended) • 1 USB 2.0 port • Nymi-supplied bluetooth adapter
Authentication tasks with a Nymi Band in a MES application(Nymi-enabled Applications(NEAs) on Windows, HP ThinPro, and IGEL	• Windows 10 x86-64, including on Citrix, RDP, and VMWare Horizon, minimum build version 1607 • HP ThinPro x86-64, including on VMWare Horizon • IGEL OS v10, including IGEL Thin Client on Citrix Tested web browsers for web-based NEAs: • Firefox 70 and later • Chrome 78 and later • Internet Explorer 11 and later • Microsoft Edge 44.18362.387.0	• Nymi-supplied Bluetooth adapter • NFC reader (optional)

Use Cases	Supported Operating System/ Browser	Hardware
Authentication tasks with a Nymi Band in an NEA on an iOS device	• iOS version 13 and later • Safari 15.7 (web-based NEA only)	Integrated Bluetooth adapter
Locking and Unlocking the Desktop	• Windows 10 x86-64, including on Citrix, RDP, and VMWare Horizon. Minimum build version 1607 • HP ThinPro x86-64, including on VMWare Horizon	• Nymi-supplied Bluetooth adapter • NFC reader (optional)

Windows N Edition Requirements

Windows N Edition does not include media features by default. The Nymi Band Application includes embedded video that cannot display without the media feature pack.

To obtain the media feature pack, perform one of the following actions:

- For Windows 10, version 1909 and later, navigate to **`Start > Settings > Apps & features > Optional features`**. Click **`Add a feature`**. From the list of available optional features, select **`Media Feature Pack`**.
- For Windows 10 versions that are earlier than 1909, download and install the media feature pack from https://www.microsoft.com/en-us/software-download/mediafeaturepackMicrosoft.
- For Windows 11, navigate to **`Start > Settings > Apps > Optional features`**. Next to **`Add an optional feature`**, select **`View features`**, and then form the list of optional features, select the Media Feature Pack.

The Nymi Band

General functional specifications for the Nymi Band are summarized in the following table.

Table 3: Nymi Band functional specifications

URS #	User Specification	FS #	Functional Specification
URS-030	An alternative method of authentication for the user shall be available for the operator if the wearable biometric is unavailable.	FS-NB-015	Connected Worker Platform allows authentication to the Nymi Band by biometrics or an external authenticator, such as Active Directory.
URS-013	All passwords which are stored by the Solution are encrypted.	FS-NB-016	Connected Worker Platform solution ensures that the Nymi Band user is valid in Active Directory. Passwords are not stored in the NES database.

URS #	User Specification	FS #	Functional Specification
URS-006 URS-017	The wearable biometric device functions under personal protective equipment (PPE) suitable for Class A/B, Class C and Class D environments. The solution shall recognize the wearable biometric: • On an NFC reader if 3 cm of plexiglass is between the NFC reader and the Nymi Band. • On the Nymi-supplied blue tooth adapter when PPE is between the blue tooth adapter and the Nymi Band.	FS-NB-019	The Nymi Band: • NFC antennae supports a read-range that allows detection by an NFC reader through protective clothing and plexiglass coverings. • Bluetooth antennae supports a read-range that allows detection by the Bluegiga Bluetooth adapter through protective clothing.

Battery life

Functional specifications for the Nymi Band battery life are summarized in the following table.

Table 4: Functional specifications for battery life

URS #	User Specification	FS #	Functional Specification
URS-007	The wearable biometric authentication device function shall function for the duration of an Operator shift (8-10hrs) on a single charge.	FS-BAT-001	The Nymi Band supports a 3-day battery life, assuming 10-hour shifts, 900 taps total (300 per shift) with one shift per day.
URS-009	The wearable biometric authentication device shall have means for charging.	FS-BAT-005	Nymi Band contains a rechargeable battery and Nymi performs standard benchmark battery life tests that can be used to provide estimations to customers and compare battery life between different firmware releases.

Physical characteristics

Functional specifications for the physical characteristics of the Nymi Band are summarized in the following table.

Table 5: Functional specifications for physical characteristics

URS #	User Specification	FS #	Functional Specification
URS-026	Operators shall be able to visually check the authentication status of the wearable biometric device. (authenticated or de-authenticated)	FS-PHY-007	The Nymi Band has a display which provides information to the user.

NES enrollment

NES uses Nymi Token Service (NTS) to manage certificates for enrollment. The following table summarizes the functional specifications and related user specifications for NES enrollment.

Table 6: Functional specifications for Enrollment

URS #	User Specifications	FS #	Functional Specification
URS-042	The solution provides assurance that the identity that is linked to the Nymi Band is the same as the user performs e-signatures with the Nymi Band.	FS-ENR-009	The enrollment process provides the user with a statement of usage and consent, and the enroll cannot proceed until the user acknowledges the statement.

Data

Data in which the system works are described and the following aspects should be addressed, access, allowed range of values for all inputs and outputs, required fields, data validation checks, data relationships, data capacity, retention time, data archiving, data integrity and security and data migration.

Data storage for NES

Table 7: Functional specifications for NES data storage

URS #	User Specification	FS #	Functional Specification
URS-011	The Solution supports the backup and restore of any internal database that is used in the Solution.	FS-DAT-002	Backup and restore procedures for database protection follow corporate policies.
URS-010 URS-012	The Solution stores biometric information in an encrypted format. Biometric information for authentication is not stored centrally.	FS-NB-012	The biometric information that is stored on the Nymi Band consists of a fingerprint template, which is securely stored locally on the micro-controller unit (MCU). The biometric information is permanently deleted when the user perform a delete user data operation on their Nymi Band. No biometric information is stored in the server and the fingerprint template never leaves the Nymi Band.

URS #	User Specification	FS #	Functional Specification
URS-027 URS-028	The Solution provides an administrator with the ability to view and print reports that provide information about additions and modifications of users and device associations. The Solution provides the ability to report on an authentication action, the user that performed the action, the date of the action and the time of the action, historically and in real time.	FS-SAF-005	The solution maintains an audit log of Nymi Band user assignments that: • Maintains a record of each change (create, update, delete) that is made to a system record, including the date and operator ID. • Is accessible to the enterprise that deployed the Connected Worker Platform solution, without support from Nymi. • Is stored in an intelligible, well-defined format, and be available at any time for review, even past the lifetime of NES. • Supports the addition of fields that you can add to the log later without affecting existing records (e g. a "reason for change" field could be added later). • Provides the existence of the audit log and a procedure for viewing its administrator. • Ensures that nothing in the Nymi system allows a user to change audit log records after the record has been generated. • Allows MES application to gather key information about the Nymi Band and the username to support the creation of an authentication audit trail.

Interfaces

Interfaces include application interfaces, NFC reader support, remote application support, and MES support.

Table 8: Functional specifications for interfaces

URS #	URS Specification	FS #	Functional Specification
URS-001	The Solution shall operate on standard IT infrastructure. (Windows Server 2016).	FS-CFG-01	The server-side components can be installed on bare metal within the customer's environment (Supported Operating Systems: Windows Server Windows Server 2016, Windows 2019)
URS-002	The Solution supports a deployment of server components in a virtualized environment.	FS-CFG-010	NES and the Nymi Agent are installable on a virtual machine that has connectivity with required components, such as a Domain Controller and AD server. The NES server and Nymi Agent must also have connectivity and access to the user terminals. The Nymi Agent can qualify as a server side component and you can deploy Nymi Agent on a VM. In the VDA environment, you can deploy a user terminal (with the Evidian client) on a virtual machine.
URS-003	The Solution integrates with single and multi-domain configurations in a single or multi-forest environment, with one-way or two-way trust.	FS-CFG-03	Connected Worker Platform shall be deployable in a way that allows a user's Nymi Band to be enrolled once and able to authenticate to systems in multiple domains.
URS-003	The Solution integrates with single and multi-domain configurations in a single or multi-forest environment, with one-way or two-way trust.	FS-CFG-04	NES shall require only one AD account for all domains for which there are trust relationships (requires two way trust between domains).

URS #	URS Specification	FS #	Functional Specification
URS-025	Operators shall be able to visually check battery charge on the wearable device.	FS-BAT-006	Users can accurately tell whether their Nymi Band's battery is Low, Medium, or High from the battery indicator on the screen.

Application interfaces

Connected Worker Platform provides IT Administrators with interface to manage the Nymi Band and NES.

The following table summarizes the functional specifications and related user specifications for application interfaces.

Table 9: Functional specifications for application interfaces

URS #	User Specification	FS #	Functional Requirement
URS-030	An alternative method of authentication for the user shall be available for the operator if the wearable biometric is unavailable.	FS-APP-001	The Nymi Band Application is a graphical user interface that allows users to enroll a Nymi Band and authenticate their Nymi Band using corporate credentials.
URS-019 URS-024	The Solution provides a self-service administrative interface to associate and disassociate a user with a biometric device. The Solution provides an administrator with the ability to view and modify Policies for the wearable authentication device.	FS-APP-002	The NES Administrator Console is a web-based application that allows administrators to manage NES policies and users. The EAM Console is provided to manage users and their Nymi Bands.
URS-039	The Solution provides a mechanism to associate Nymi Bands to a single user.	FS-APP-003	The solution provides the Nymi Band Application to assign a single user to a Nymi Band, and prevents another user from attempting to enroll the Nymi Band when the Nymi Band to user association exists in the NES database.

Remote application support via RDP and Citrix

Connected Worker Platform allows users to access multi-user applications running on a remote RDP-based and Citrix-based environment solution and have multiple user sessions running on it by using an authenticated Nymi Band.

The following table summarizes the functional specifications and related user specifications for remote application support.

Table 10: Functional specifications for remote application support

URS #	User Specification	FS #	Functional Specification
URS-020 URS-021 URS-022	The Solution supports NFC taps to signal intent when the Authentication Module is configured to use NFC-only (RFID). The Solution supports remote desktop services such as RDP to access and authenticate a remote MES Solution. The Solution supports the use of thin clients to remotely access configuration applications and provide e-signatures over RDP and Citrix sessions.	FS-RDP-005	Administrators can install NEAs on Windows 10 thin clients running Citrix (compatibility requirement).

MES support

The Connected Worker Platform enables users to interface with MES applications by providing a Nymi API.

The following table summarizes the functional specifications and related user specifications for MES support.

Table 11: Functional specifications for MES support

URS #	User Specification	FS #	Functional Specification
URS-014 URS-023	The solution provides the capability to log into Windows and Enterprise Single Sign-On to on-boarded applications (including MES applications). The Solution only provides access to authorized users.	FS-MES-001	The Active Directory user status is queried for every user authentication provided by a Nymi Band to Windows and MES login.
URS-004 URS-015	The Solution provides secure communication with endpoints that require credential verification. The Solution provides a configurable login to the MES Applications with a pop-up windows for authentication.	FS-MES-006	Integrate the Nymi API into an MES to support the use of a Nymi Band for login. Integration with Evidian enables a popup window for sign off/ e-signature.
URS-016 URS-018	The Solution provides an automatic user logoff from the Windows session if s/he walks away from a logged in Windows session. Log off will trigger when the wearable biometric device is outside of the BLE range. The Solution provides an automatic user logoff from the Windows session if the operator removes the wearable authentication device/ the device is deauthenticated.	FS-MES-008	The System shall provide automatic user logoff from a Windows session if s/he walks away from a logged in Windows session or the Nymi Band deauthenticates.

Environment

Environment requirements outline that in which the system is to work including physical layout, physical conditions, physical security, power requirements and any special physical or logical requirements.

Table 12: Environment requirements

URS #	User Specification	FS #	Functional Specification
URS-005	The wearable biometric authentication device does not introduce any unacceptable risks to the health and safety risk of the person who wears the device.	FS-ENV-001	The Nymi Band maintains biocompatibility and chemical resistance.

URS-005	The wearable biometric authentication device does not introduce any unacceptable risks to the health and safety risk of the person who wears the device.	FS-ENV-002	• The Nymi Band is certified by:
			  • FCC (United States)
			  • CE (Europe)
			  • IC (Canada)
			• The Nymi Band is made of hypoallergenic material.

URS-008	The wearable biometric authentication device function shall be suitable for cleaning with isopropyl alcohol (IPA) 70% wipes or hydrogen peroxide.	FS-ENV-003	The Nymi Band can be sanitized with an alcohol wipe or spray and hydrogen peroxide.
URS-040	The wearable biometric authentication device shall be suitable for ANSI 12.12.03.2011 compliant environments.	FS-ENV-005	The solution provides a configurable option to disable haptic feedback on Nymi Bands to maintain compliance with the ANSI 12.12.03.2011 standard.

Glossary

Definitions/acronyms used throughout this document are defined below.

Table 13: Glossary

Acronym	Definition
AD	Active Directory. Directory service for domain networks.
AD LDS	Active Directory Lightweight Directory Services. Directory service for domain networks.
IAM	Identity Access Management
SSO	Single Sign-On
MES	Manufacturing Execution System
CWP	Connected Worker Platform
EAM	Enterprise Access Management
ESSO	Enterprise Single Sign on
RFID	Radio-frequency identification
Solution	All components that enable biometric authentication, including Nymi Enterprise Edition components , Evidian components and the MES.
Class A	Class A clean rooms are for high-risk operations (eg. filling zone, stopper bowls, open ampoules and vials and, making aseptic connections). Class A environments are sterile environments
Class B	Class B Clean rooms provide the background environment for grade A zone items needing aseptic preparation and filling.
Class D	Environments for less critical tasks in the manufacturing process.
21 CFR Part 11	Part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration regulations on electronic records and electronic signatures.

Copyright ©2023
Nymi Inc. All rights reserved.

Nymi Inc. (Nymi) believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

The information in this document is provided as-is and Nymi makes no representations or warranties of any kind. This document does not provide you with any legal rights to any intellectual property in any Nymi product. You may copy and use this document for your referential purposes.

This software or hardware is developed for general use in a variety of industries and Nymi assumes no liability as a result of their use or application. Nymi, Nymi Band, and other trademarks are the property of Nymi Inc. Other trademarks may be the property of their respective owners.

Published in Canada.
Nymi Inc.
Toronto, Ontario
www.nymi.com