Overview Guide

Nymi Connected Worker Platform 1.19.0
v1.0
2024-11-08

Contents

Preface

This document is part of the Connected Worker Platform(CWP) 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. A CWP Administrator is the person in the enterprise that manages the Connected Worker Platform for their organization.

Third-party Licenses

The Nymi solution uses subject matter that was obtained under 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	November 08, 2024	First release of this document for the CWP 1.19.0 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

The Nymi 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 converging point solutions into a single offering.

CWP 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, CWP 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
- Nymi IT/OT Solution

The goal of the CWP 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. You can use the CWP solution as a stand-alone solution or you can integrate the solution into third-party applications, devices, or services.

The following figure shows the core CWP components.

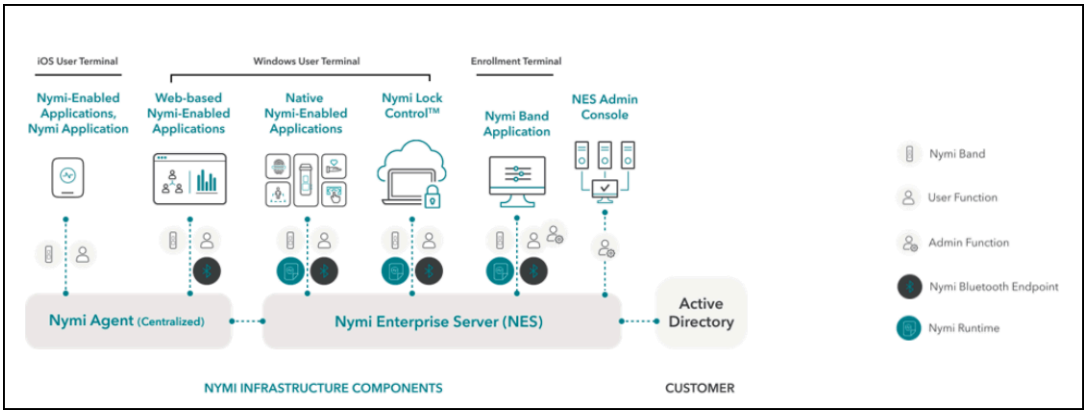

Figure 1: Nymi Connected Worker Platform Core Components

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 over BLE and NFC protocols with a Nymi-enabled Application(NEA) that is built using the Nymi API. 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.

User Terminal

A computer that users access to complete authentication tasks in a Nymi-enabled Application(NEA) with a Nymi Band tap.

CWP supports Windows, iOS, and Linux user terminals that are thick or thin clients.

On thin clients and iOS clients, you must configure each user terminal to access the Nymi Agent component from a centralized location.

For thick clients, you can configure the user terminal to use a local installation of the Nymi Agent component or connect to a centralized Nymi Agent. You cannot configure the user terminal to simultaneously connect to both a local and centralized Nymi Agent.

Nymi-enabled Applications

Nymi provides an SDK that allows developers to build Nymi-enabled Application(NEAs). When you integrate an NEA with Connected Worker Platform, the users can use a Nymi Band to perform authentication tasks such as physical access, application login, and electronic signatures.

Third parties can develop an NEAs as web application or native application that makes use of the Nymi Band's security functions.

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 Lock Control

Nymi Lock Control is a Nymi-enabled Application that you can install on Windows user terminals to provide users with the ability to manage access to the user terminal with a Nymi Band instead of typing their username and password. Nymi Lock Control verifies user access through Active Directory.

Nymi Lock Control provides users with the following functionality:

- Unlock the desktop or log in to a user terminal by tapping an authenticated Nymi Band on an NFC reader or the Nymi-supplied Bluetooth adapter that is attached to the terminal.
- Lock the desktop when the authenticated user is not within the Bluetooth range of the terminal or when the user removes their Nymi Band.
- Prevent a desktop lock while an authenticated Nymi Band stays within Bluetooth range.

Note: Nymi Lock Control is a single domain solution and does not support cross-domain access. Ensure that all user terminals reside on the same domain as the Nymi Enterprise Server host.

Enrollment Terminal

Windows computer where users access the Nymi Band Application to perform an enrollment, which associates a user with a Nymi Band.

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 Evidian EAM Management 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 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.

Domain Environment

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

A CWP integration with AD is limited to performing authentication of users and computers, lookup of user status and group membership. CWP does not write to AD.

A CWP integration uses AD for the following purposes:

- For user authentication by the Nymi Band Application, to enable user management of Nymi Bands, such as 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.
- For client authentication when the Nymi-enabled Application(NEA) needs to access Nymi Enterprise Server(NES) for privileged operations.

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, which you plug into a USB port on the user terminal. . 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 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, deployments using NES and Evidian Access Management (EAM), and IT/OT deployments.
- **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:

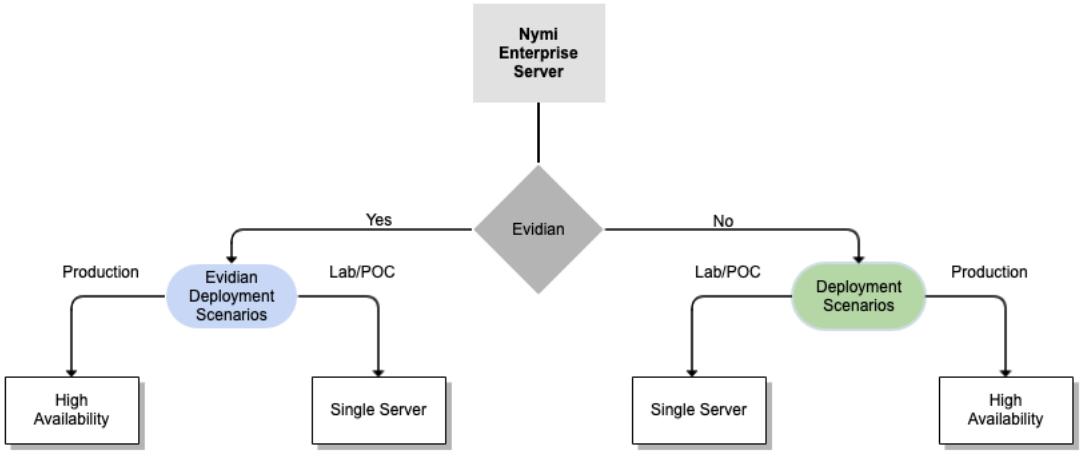

Figure 2: Nymi Enterprise Server Deployments

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 Evidian 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 IT/OT Solution

Organizations use multiple identity domains to secure and segregate technologies. For example, organizations can have an *Information Technology(IT) Identity Domain* in an AD forest with applications and systems that perform monitoring and process-related activities and one or more *Operational Technology(OT) Identity Domain* with applications and systems in other AD forests that perform operational-related activities.

The Nymi IT/OT Solution allows a Nymi Band user to enroll their Nymi Band in one identity domains and register their Nymi Band in other identity domains, which allows them to use their Nymi Band in all identity domains. Each user can have one separate account in up to three separate identity domains, and all accounts are associated with a single Nymi Band. The Nymi IT/OT Solution does not require a trust relationship or network connectivity between the identity domains.

In the Nymi IT/OT Solution, each identity domain has:

- One Nymi Enterprise Server(NES).
- One Evidian EAM Controller, if required.
- One centralized Nymi Agent, if required.
- At least one *Nymi Band Application(NBA)Terminal*, which you configure to access the NES in the same identity domain.

Review the glossary for information about *Registration* , *Enrollment* , the *NBA Terminal*, the *Registration Terminal*, the *Enrollment Terminal*, the *Registration Nymi Enterprise Server(NES)*, and the *Enrollment Nymi Enterprise Server(Enrollment NES)*.

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.

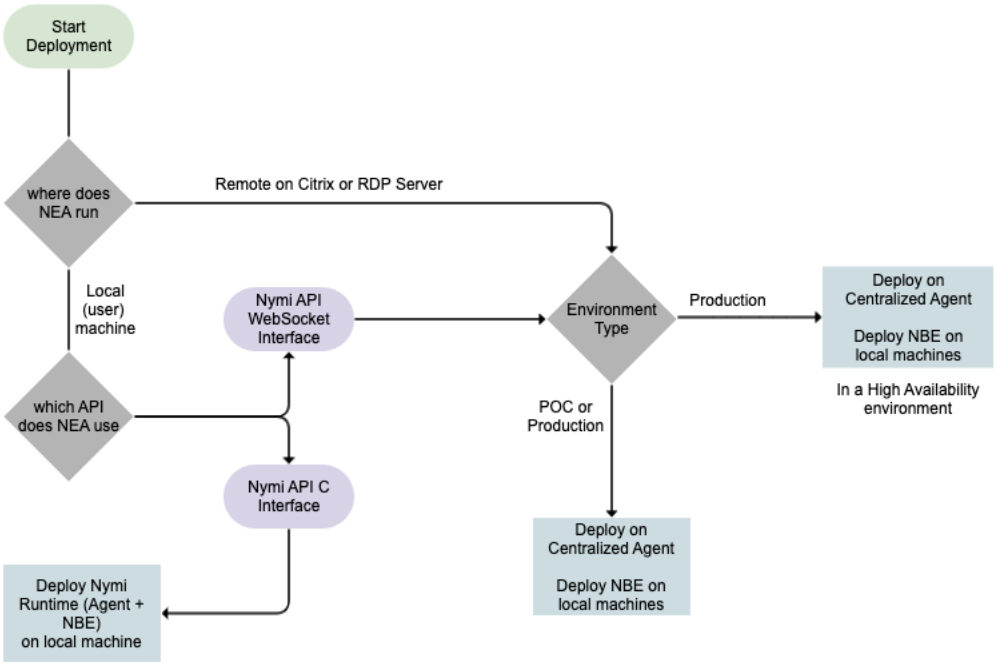

Figure 3: Nymi SDK Deployments

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 user terminal to support the NEA that uses the Nymi API C Interface. Alternatively, use theNymi 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.
- **Nymi IT/OT Solution Planning Guide**

  This guides contains information about how to plan for an implementation of the Nymi IT/OT Solution in Connected Worker Platform(CWP) 1.18.0 and later, including how to migrate from earlier Nymi IT/OT implementations.
- **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 Developer Guide—NymiAPI(Windows)**

  This document provides information about how to develop Nymi-enabled Applications by using the Nymi API(NAPI).
- **Nymi SDK Developer Guide—Webapi(Windows)**

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

- **Nymi SDK Developer Guide—Webapi(iOS)**

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

Glossary

The following is a list of terms that are used in this guide.

Authentication Station

Name give to the *NBA Terminal* where users access the Nymi Band Application to authenticate the Nymi Band by corporate credentials.

Alternate Terms: Nymi Band Application Terminal

Authentication Task

An activity that a user completes in a Nymi-Enabled Application(NEA) with a tap of their authenticated Nymi Band.

Band ID

A value on the Nymi Band that uniquely identifies the Nymi Band through the Bluetooth interface.

The Band ID for a Nymi Band changes with each enrollment.

Alternate Terms: MAC Address, BLE MAC Address

BasicLoginWithToken

A type of authentication method that a Nymi-Enabled Application(NEA) uses to connects to Nymi Enterprise Server(NES) the first time that a user accesses the NEA.

The NEA uses the HTTPS basic authentication mechanism to provide NES with the username and password for a Active Directory user account. If the authentication succeeds, NES provides the NEA with an authentication token that the NEA uses for subsequent NES access.

Biometric Authentication

A process that uses unique biological characteristics of a person to reliably verify their identity.

Biometric Authentication

Note: The Nymi Band uses a fingerprint template to identify a person.

Bluetooth Tap

The action of tapping an authenticated Nymi Band on Bluetooth Adapter to transmit the Band ID.

Bluetooth Tap(BLE Tap)

BLE Tap

Bluetooth Adapter

A Nymi-supplied bluetooth device that supports Bluetooth communications. When a user taps their authenticated Nymi Band on the Bluetooth adapter (BLE Adapter), the Bluetooth adapter reads the Band ID of the Nymi Band, to identify the user that is associated with the Nymi Band.

Bluetooth adapter(BLE Adapter)

BLE Adapter

Alternate Terms: Bluetooth dongle, Bluegiga Adapter, BLED112 Bluetooth Low Energy Dongle

Bluetooth Range

Distance between an authenticated Nymi Band and a *Bluetooth adapter(BLE Adapter)* that is plugged into a user terminal, enrollment terminal, or authentication station.

When the distance between the Nymi Band and *BLE Adapter* allows continuous Bluetooth communications, the devices are "within range" of each other.

When the distance between the Nymi Band and *BLE Adapter* does not allow continuous Bluetooth communications, the devices are "out of range" of each other.

BLE Range

Configuration Specifications Document

Good Automated Manufacturing Practices(GAMP)-specific document that provides information about how to configure the Nymi solution to supports requirements that are defined in the *User Requirements Specifications(URS)* document.

Nymi provides the Configurations Specifications document.

Not all requirements in the *User Requirements Specifications Document* have a configuration specification.

Configuration Specifications(CS)

CS

Delete User Data

Operation that a user or administrator performs to remove the fingerprint template from the Nymi Band

Security wipe

Enrollment

A process where a user associates (binds) themselves to a Nymi Band, and the Nymi Band to their corporate identity.

The Nymi Band Application facilitates the enrollment process. The user to Nymi Band association is an interactive activity that results in the creation of a fingerprint template. The Nymi Band to corporate identity association is an activity that the Nymi Band Application performs after the fingerprint template creation.

Enrollment Terminal

Name give to the *NBA Terminal* where users access the Nymi Band Application to enroll their Nymi Band.

Note: In some Nymi IT/OT Solution configurations, users can also use the *NBA Terminal* to register their Nymi Bands.

Alternate Terms: Nymi Band Application Terminal

Enrollment Nymi Enterprise Server

Name give to the Nymi Enterprise Server(NES) in an IT/OT environment that has permission to enroll Nymi Band to users in an identity domain and manage all policies for the users.

Enrollment Nymi Enterprise Server(Enrollment NES)

Enrollment NES

Enterprise Access Management

A solution that allows administrators to control user accesses to workstations and applications, and allows end-users to automate their accesses to applications by performing single sign-on (SSO).

The Evidian Enterprise Access Management(EAM) solution integrates with the Nymi Solution to provide SSO with aNymi Band tap.

Enterprise Access Management(EAM)

EAM

Fingerprint Template

A mathematical representation of unique fingerprint features for the finger that a user places on the Nymi Band during the enrollment process.

The Nymi Band stores the fingerprint template in a protected memory space inside the microcontroller unit (MCU).

The fingerprint template is not a fingerprint image and the Nymi Band does not retain original fingerprint images.

False Acceptance Rate

An authentication measurement. The rate at which the Nymi Band fingerprint sensor matches a fingerprint that the associated user did not supply to create the fingerprint template, and authentication succeeds.

False Acceptance Rate(FAR)

FAR

False Rejection Rate

An authentication measurement. The rate at which the Nymi Band fingerprint sensor rejects a fingerprint on the finger that the associated user used to create the fingerprint template, and authentication fails.

False Rejection Rate(FRR)

FRR

Functional Specifications Document

GAMP-specific document that provides information about the functionality in the Nymi solution that supports each requirement that is defined in the *User Requirements Specifications Document* document.

Nymi provides the Functional Specifications document.

Functional Specifications(FS)

FS

Good Automated Manufacturing Practices

Set of guidelines for industries that use automation to follow, to maintain operational efficiency and reliability.

Good Automated Manufacturing Practices(GAMP)

GAMP

Note: Nymi provides sample GAMP templates that support validation of the Nymi solution in a GAMP environment.

Identity Domain

A collection of one or more Active Directory (AD) domains and/or forests.

Examples of identity domains include a single AD forest with a single domain, a single AD forest with multiple domains, or a collection of AD forests with a full two-way trust.

Identity Domain

Nymi IT/OT

A deployment architecture that allows one Nymi Band user to use a single Nymi Band to perform authentication tasks such as electronic signatures in up to three identity domains.

The user can have one distinct user account in each of the identity domains.

Information Technology Identity Domain

An identity domain that has non-manufacturing systems, which a Nymi Band user accesses to complete authentication tasks.

Information Technology(IT) Identity Domain

IT

Information Qualification

GAMP-specific document that defines test cases, test steps, and test results.

Customers perform the test cases in the Operational Qualification document to validate that the Nymi solution meets operations-specific requirements that are defined in the URS.

Information Qualification(IQ)

IQ

Intent

A deliberate act where a user taps their Nymi Band on an NFC or Bluetooth device to associates the results of an event or action with the identity of the user.

Nymi Band Tap

Nymi Lock Control

Optional Nymi application that provides Windows login and unlock capabilities based on user presence.

Nymi Lock Control

Manufacturing Execution System

Third-party tool that monitors and tracks various stages of the manufacturing processes.

Manufacturing Execution System(MES)

Note: When you integrate the Nymi SDK within a Manufacturing Execution System, the Manufacturing Execution System becomes a Nymi-enabled Application, which allows you to complete tasks within the system that require a username and Password with a Nymi Band tap.

MES

NegotiateLoginWithToken

An API that a Nymi-Enabled Application(NEA) uses to obtain an authentication token from the Nymi Enterprise Server(NES).

The NEA uses the HTTPS negotiate authentication mechanism to provide NES with an Active Directory(AD) user account or computer account credentials for authentication. NES uses the provided credentials to establish that the account is valid and to determine access level authorization. If the account is valid, authentication succeeds and NES provides the NEA with an authentication token. The NEA uses the token to make subsequent calls to NES and complete authorized actions. Negotiate authentication uses either Kerberos or NTLM protocols for authentication.

Near Field Communications UID

A value on the Nymi Band that uniquely identifies the Nymi Band through the Near Field Communication(NFC) interface.

During the enrollment process, Nymi Enterprise Server (NES) associates the NFC UID with the user that logs into the Nymi Band Application.

NFC devices can read the identifier on an authenticated Nymi Band.

Near Field Communications UID(NFC UID)

NFC UID

Near Field Communications Tap

The action of tapping an authenticated Nymi Band on an Near Field Communications(NFC) reader to transmit the NFC ID.

Near Field Communications Tap(NFC Tap)

NFC Tap

NFC Reader

A device that supports Near Field Communications (NFC). When a user taps their authenticated Nymi Band on an NFC reader, the NFC reader reads the NFC UID of the Nymi Band, to identify the user that is associated with the Nymi Band.

Nymi API

Set of APIs published by Nymi in the Nymi SDK (Nymi SDK) that Developers can use to create a Nymi-Enabled Application (NEA).

Nymi API(NAPI)

NAPI

Nymi Application

A component of the Nymi solution that supports Nymi Band taps on the Bluetooth adapter to complete authentication tasks in iOS Nymi-Enabled Application (NEA).

Nymi Agent

Component of the Nymi Runtime that provides an interface between Nymi Enterprise Server(Nymi Enterprise Server) and the Nymi Bluetooth Endpoint component.

Nymi Band

A biometric device that a user wears on their wrist and uses to perform authentication tasks.

Nymi Band

Nymi Band Application

Nymi-provided Windows application that allows users enroll a Nymi Band and authenticate to a Nymi Band with corporate credentials.

Nymi Band Application(NBA)

NBA

Nymi Band Application Terminal

Name give to the computer where users access the Nymi Band Application to perform assignment activities on their Nymi Band.

The functions that a user can perform depends on the group and individual policy configuration of the Nymi Enterprise Server(NES).

Functions include:

- Nymi Band enrollment in NES and Evidian EAM Controller.
- Nymi Band registration in NES and Evidian EAM Controller.
- Authentication by corporate credentials.
- Assignment of Nymi Band label.
- Nymi Band self re-enrollment.
- Nymi Lock Control support.

Nymi Band Application(NBA)Terminal

NBA Terminal

Nymi Bluetooth Endpoint

Component of the Nymi Runtime that provides an interface between the Bluetooth Adapter and the Nymi Agentcomponent.

Nymi Bluetooth Endpoint(NBE)

NBE

Nymi-Enabled Application

A native or web-based application that utilizes the Nymi API C Interface to integrate the Nymi Solution.

The Nymi Band Application and Nymi Lock Control are Nymi-Enabled Applications(NEAs). Other applications that can utilize the Nymi API C Interface to become an NEA

include Single Sign-On (SSO), Manufacturing Execution Systems (MES), and Physical Access Systems (PACS).

Nymi-Enabled Application(NEA)

NEA

Nymi Enterprise Server

Component of the Nymi Solution that you install on a Windows server that acts as a management server and collection of services. Nymi Enterprise Server (NES) coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates.

Nymi Enterprise Sever(NES)

NES

See also: Registration NES, Enrollment NES

Operational Technology Identity Domain

An identity domain that has the manufacturing systems and MES applications, which a Nymi Band user accesses to complete authentication tasks.

Operational Technology(OT) Identity Domain

OT

Nymi Security Layer

Cross-platform library that provides security functions to the Nymi Band and Nymi API(Nymi API(NAPI, such as encryption and decryption, signing and signature verification, secure keystore, and message authentication.

Nymi Security Layer(NSL)

NSL

On-Body Detection

The ability of the Nymi Band to detect when it is worn on a human body, and any transitions on and off that body.

On-Body Sensors

The optical and capacitive sensors on the underside of the Nymi Band.

Operational Qualification Document

GAMP-specific document that defines test cases, test steps, and test results.

Customers perform the test cases in the Operational Qualification document to validate that the Nymi solution meets operations-specific requirements that are defined in the URS.

Operational Qualification(OQ)

OQ

Performance Qualification

GAMP-specific document that defines test cases, test steps, and test results.

Customers perform the test cases in the *Operational Qualification(OQ)* document to validate that the Nymi solution meets operations-specific requirements that are defined in the URS.

Performance Qualification(PS)

PQ

Presence Detection

A Nymi SDK and Nymi Lock Control feature that detects whether or not a Nymi Band is in Bluetooth range, and the authentication state of a Nymi Band.

Public-Key Cryptography Standards #11

Public-Key Cryptography Standard and the programming interface that the Nymi Solution uses to create and manipulate cryptographic tokens.

Public-Key Cryptography Standards #11(PKCS11)

PKCS11

Recovery Mode

A Nymi Band state where the firmware on the Nymi Band switches to recovery firmware.

Note: The recovery mode process also performs a delete user data operation. To downgrade the firmware version on a Nymi Band, you must first switch the Nymi Band to recovery mode.

Recovery Firmware

A limited feature-set version of standard Nymi Band firmware.

Note: Provides a fall-back mechanism or always known-good firmware on the Nymi Band in the event that the Nymi Band encounters problems with the standard firmware version. Nymi pre-loads recovery firmware on the Nymi Band that you cannot remove or change.

Registration

A process where a user associates (binds) their enrolled Nymi Band to additional corporate identities.

In an Nymi IT/OT Solution, when a user wears their authenticated Nymi Band and logs into the Nymi Band Application in a domain that differs from the enrollment domain, the Nymi Band Application performs the registration process passively.

Registration Nymi Enterprise Server

Name give to the Nymi Enterprise Server(NES) in an IT/OT environment that has permission to register Nymi Band to users when their enrollment occurred on an Enrollment NES. Registration NES can manage settings that influence the behaviour of Connected Worker Platform infrastructure and terminals, for example self re-enrollment, Nymi Lock Control settings and the

use of the Corporate Credentials Authenticator. A Registration NES cannot manage the settings that are applicable to a Nymi Band, such as haptic feedback and liveness detection.

Registration Nymi Enterprise Server(NES)

Registration NES

Registration Terminal

Name give to the computer in the Nymi IT/OT Solution where users access the Nymi Band Application to register their Nymi Band.

Note: In some Nymi IT/OT Solution configurations, users can also use the Nymi Band Application to enroll their Nymi Bands.

Alternate Terms: Nymi Band Application Terminal

Thick Client

A user terminal that is physical machine and hosts an *Manufacturing Execution System(MES)* application.

Thin Client

A user terminal that connects to a centralized server, such as RDP or Citrix to access an *MES* application.

Alternate terms: Remote Client, Remote User Terminal, Citrix Client, RDP Client

Token Management Structure

An Evidian-supplied file that defines the meta-data of the authentication method that supports the use of the Nymi Band for Enterprise Single Sign On (eSSO).

Token Management Structure(TMS)

TMS

User Terminal

Name give to the computer that users access to complete authentication tasks in a Nymi-Enabled Application(NEA) with a Nymi Band tap.

User Requirements Specifications Document

GAMP-specific document that defines the requirements that the Nymi Solution must meet before a customer can deploy the Nymi Solution in a production environment.

User Requirements Specifications(URS)

URS

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