nymi™

Overview Guide

Nymi Enterprise Edition
v3.0
2020-12-18

Contents

Preface

This document is part of the Nymi Enterprise Edition documentation suite.

Purpose

This document provides overview information about the Nymi Enterprise Edition solution, such as component overview, deployment options and supporting documentation information.

Audience

This guide provides information to NES Administrators. An NES Administrator is the person in the enterprise that manages Nymi Enterprise Edition for their workplace.

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 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
3.0	December 18, 2020	Update of this document for `Nymi Enterprise Edition` 3.3.0, which includes: • correcting typographical errors
2.0	September 18, 2020	Update of this document for the `Nymi Enterprise Edition` 3.2.0 release.
1.0	April 15, 2020	This guide is reissued due to document version update. There are no content changes since NEE 2.6.0.

Nymi Enterprise Edition Environment

The Nymi Enterprise Edition environment contains several core components:

- Nymi Band
- Nymi Enterprise Server (NES)
- Nymi Band Application
- Nymi SDK (which includes Nymi Runtime and Nymi_api.dll (NAPI DLL) file)
- BLE Adapter and NFC reader

Note: The Nymi-enabled Application (NEA) displays in the diagram, but is not a Nymi component. It is created using Nymi components.
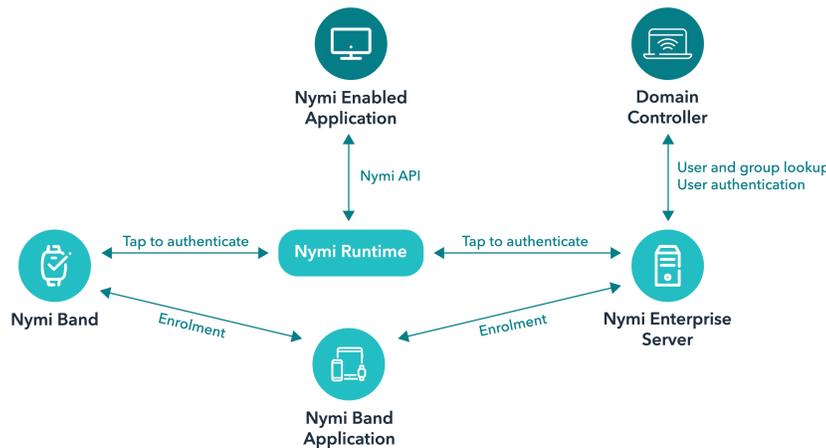
Figure 1: Nymi Enterprise Edition Core Components

The Nymi Enterprise Edition solution can be used as a stand-alone solution or integrated into third-party applications, devices, or services.

Nymi Band

The Nymi Enterprise Edition solution 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 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 and 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 (NBA) 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 NBA 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 (NES)

The Nymi Enterprise Server (NES) is the server component of the `Nymi Enterprise Edition` solution 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 2012 R2 or Microsoft Windows Server 2016 that 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.

SQL Server: Licensed SQL Server installation is required for production.

IIS Server: NES uses Microsoft Internet Information Service (IIS) to access web services.

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 SDK Components

Nymi SDK is composed of the `Nymi Runtime` and Nymi API (NAPI).

Nymi Runtime

`Nymi Runtime`—Facilitates communication between an NEA and Nymi Bands. The `Nymi Runtime` consists of the `Nymi Agent` and the Nymi Bluetooth Endpoint.

- The `Nymi Agent` facilitates communication between NEAs and the Nymi Bands, and maintains knowledge of Nymi Band presence and authentication states.
- The `Nymi Bluetooth Endpoint` is a service that is deployed on individual workstations to provide local BLE communications with Nymi Bands through the Nymi-provided bluetooth adapter.

Nymi Agent - Local and Centralized

Install the `Nymi Agent` in one of the following ways:

Local: Deploy a local `Nymi Agent` when an NEA that is using the `Nymi API C Interface` (via the NAPI DLL component) is running locally. In this scenario, the `Nymi Agent` runs on the same machine as the `Nymi Bluetooth Endpoint`, the BLE Adapter and the NFC reader).

Centralized: Deploy a centralized `Nymi Agent` in the following situations:

• When the NEA runs on a different machine from the NBE, BLE adapter, and NFC reader. For example, the NEA may run on a centralized Citrix / RDP server, while the NBE, BLE adapter and NFC reader are on terminals running Citrix / RDP clients.
• When the NEA uses the `Nymi API WebSocket Interface`.

Nymi API C Interface (NAPI DLL)

The Nymi API (NAPI) DLL provides NEAs access to Nymi Band functionalities by using the `Nymi API C Interface`. It also manages NEA certificates and allows secure communications with Nymi Bands by using the Nymi Security Protocol.

Nymi API Websocket Interface

The `Nymi API WebSocket Interface` provides Nymi developers with a simplified way to utilize the functionality of the Nymi SDK, over a WebSocket connection. The `Nymi API WebSocket Interface` allows developers to write web applications that access services available from the `Nymi Enterprise Edition` solution. You can configure and enable the `Nymi API WebSocket Interface` in a centralized Nymi Agent environment.

Nymi API for Linux

The Nymi API for Linux provides NEAs access to Nymi Band functionalities by using the `Nymi API for Linux`. It also manages NEA certificates and allows secure communications with Nymi Bands using the Nymi Security Protocol. Install the Nymi Agent locally (similar to the NBA) or remotely (for example, when the NEA runs on ThinManager).

SDK Documentation and Sample Code

Nymi provides sample code for each SDK. The sample code is 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 API WebSocket Interface`: The sample application is located within the package at: nymi-sdk/webapi/sdkSamples/SDK_Sample.

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 Nymi Enterprise Edition.

Nymi-Enabled Applications

Nymi provides an SDK that allows teams to build Nymi-enabled Applications (NEAs), which consists of customer enterprise components. When the NEA is integrated with Nymi Enterprise Edition, the solution can perform tasks such as Windows terminal login / unlock, application login, and electronic signatures.

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

Domain Environment

Nymi Enterprise Edition is designed for seamless integration into enterprise Active Directory (AD) environments.

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

- For user authentication by the NBA, 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 NEE 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

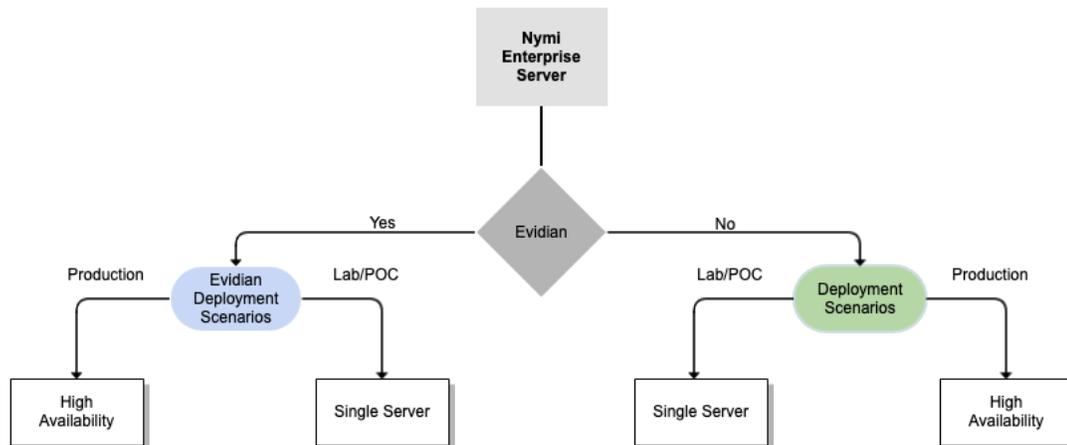Nymi Enterprise Edition can be deployed in the following configurations:

Figure 2: Nymi Enterprise Server Deployments

Deployment Decisions

Table 2: Deployment Options

Deployment Decision	Deployments Details	Nymi Documentation
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 Enterprise Edition with Evidian Installation and Configuration Guide*
NES is deployed in an Evidian environment in a production environment	Multiple servers configured for High Availability production environment	*Nymi Enterprise Edition with Evidian Installation and Configuration Guide*, *Nymi Deployment Guide*

Deployment Decision	Deployments Details	Nymi Documentation
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 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 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 Nymi Enterprise Server (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 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 NEE 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 Nymi Enterprise Server (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 Availabiltiy support, refer to the *Nymi 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.
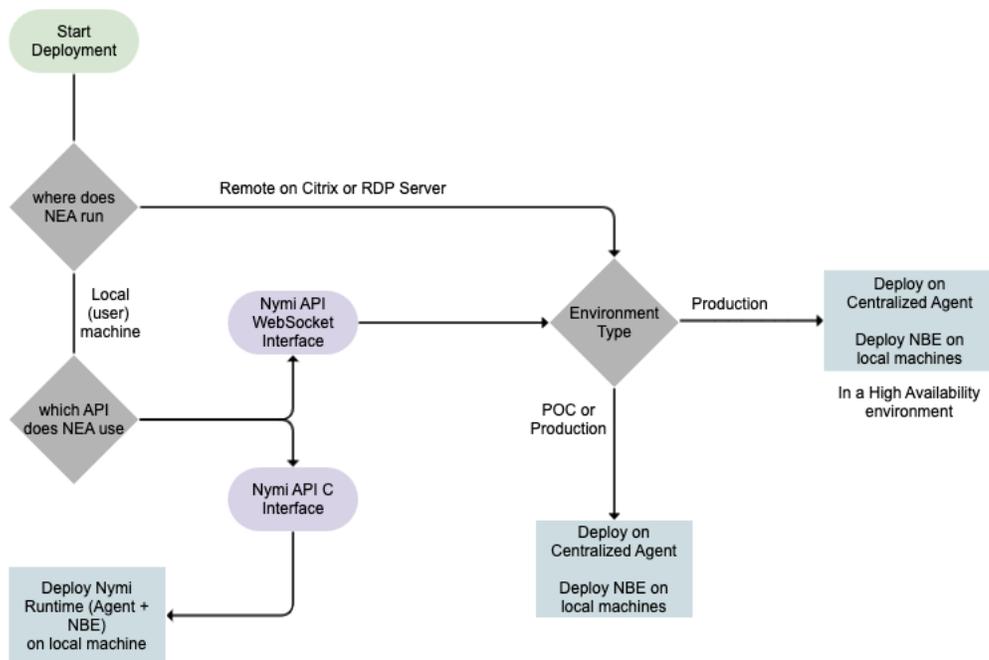
Figure 3: Nymi SDK Deployments

Deployment Decisions

Table 3: SDK Deployment Decisions

Deployments Details	NEE Documentation
On a local user terminal.	*Nymi API WebSocket Interface 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 API WebSocket Interface 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 API WebSocket Interface Guide*
Deploy `Nymi Runtime` (`Nymi Agent` + `Nymi Bluetooth Endpoint`) on the user terminal.	*Nymi API C Interface Guide* and *Nymi API for Linux 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 API WebSocket Interface` to provide the functionality of the Nymi SDK over a WebSocket connection. In the deployment, consider the following information:

- Extend existing NEE deployments by adding web clients that utilize the `Nymi API WebSocket Interface` 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 Nymi Enterprise Edition solution. Each guide contains information that is specific to a component or group of components included in the Nymi Enterprise Edition solution. 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. Additional documentation is available to support customers and deployments by asking your Nymi Customer Success representative for details.

Deployment Guide

This document provides an overview of the components and the steps that are required to deploy the Nymi Enterprise Server. This installation uses the Nymi Token Services to install certificates that enable communication between components.

This document provides information about deploying Nymi Enterprise Edition in a Citrix or RDP environment.

Administration Guide

This document provides information about how to use the Nymi Enterprise Server Administrator Console (NES Administrator Console) to manage a Nymi Enterprise Edition system. This document describes how to set up, use and manage the Nymi Band, and how to use the Nymi Band Application.

This document provides instructions on deploying the Nymi Band Application and Nymi Runtime components.

Troubleshooting Guide

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

Nymi API for C Interface Guide

This document provides information about how to use the functionality that is available in the Nymi API that is part of Nymi Enterprise Edition.

Nymi API for Linux Interface Guide

This document provides information about how to use the functionality that is available in the Nymi API that is part of Nymi Enterprise Edition.

Nymi API for WebSocket Interface Guide

This document provides information about how to use the functionality that is available in the Nymi API that is part of Nymi Enterprise Edition.

Nymi FIDO2 Implementation Guide

The Nymi FIDO2 feature offers a fast and secure way of logging into a Microsoft Account without entering credentials such as a username and password. The Nymi Band combines key elements of the FIDO2 specification to create a secure, convenient and private solution for logging into a Microsoft Account with continuous Nymi biometric authentication.

Nymi Enterprise Edition with Evidian Installation and Configuration Guide

The Nymi Enterprise Edition and Evidian Installation and Configuration Guide provides information about installing the Evidian components and configuration options based on your deployment. Alternative deployment options and configuration information are included in this guide.

Nymi Enterprise Edition Release Notes

The Nymi Enterprise Edition Release Notes contains information about Nymi Enterprise Edition and is part of the Nymi Enterprise Edition documentation suite.

Nymi Enteprise Edition Security White Paper

Security whitepaper describing the security architecture of the Nymi Enterprise Edition solution.

Nymi Third Party Licenses

The Nymi Enterprise Edition solution comprises subject matter which was obtained under an open source license, this document provides license information for third party licenses.

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