IT/OT Planning Guide

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

Contents

Preface

Nymi™ provides periodic revisions to the Nymi Connected Worker Platform. Therefore, some functionality that is described in this document might not apply to all currently supported Nymi products. The *Connected Worker Platform Release Notes* provide the most up to date information.

Purpose

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

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.

Audience

This guide provides information to Solution Consultants and NES Administrators. A NES Administrator is the person in the enterprise that manages the Connected Worker Platform for their workplace.

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.

Related documentation

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

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

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

Glossary

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

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 *Nymi Band Application(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

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

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-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

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

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

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 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

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

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.

IT/OT Overview

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.

Organizations use multiple identity domains to secure and segregate technologies. For example, organizations can have an *IT* in an AD forest with applications and systems that perform monitoring and process-related activities and one or more *OT* 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 *NBA Terminal*, which you configure to access the NES in the same identity domain.

Starting with Connected Worker Platform(CWP) 1.18.0, Nymi provides new functionality in NES policies to support IT/OT configurations natively without the need to run configuration scripts or perform SQL database synchronization.

The following figure provides an example of an Nymi IT/OT Solution deployment.

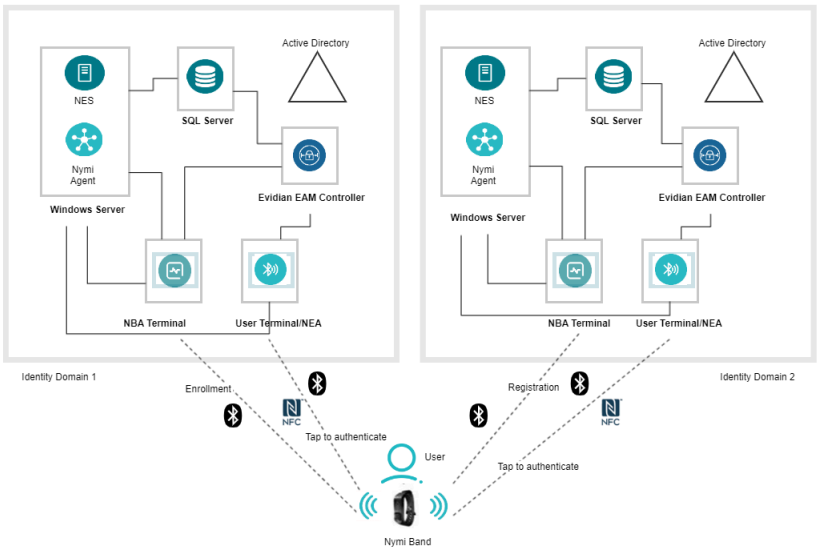

Figure 1: Nymi IT/OT Solution Overview

In the Nymi IT/OT Solution:

- The NES and Evidian EAM Controller in each identity domain is independent and is not connected to the NES and Evidian EAM Controller in other identity domains.
- The NES and Evidian EAM Controller databases in each identity domain are independent; therefore, you must query all databases for audit information.
- The *NBA Terminal* can support enrollment of the Nymi Bands only, registration of the Nymi Bands only, or both enrollment and registration of Nymi Bands in the identity domain.

  Note: The Group Policy configuration of the NES that the *NBA Terminal* connects to defines which functions the user can perform when they log into the *NBA Terminal*
- You can use SQL Server or SQL Server Express.

IT/OT Planning

The Nymi IT/OT Solution is 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.

In an Nymi IT/OT Solution deployment you must review the existing architecture and decide:

- How to configure the NES group policy in each identity domain. CWP 1.18.0 and later includes a group policy option that determined how users interact with the NES in an identity domain. Available options are enrollment only, registration only, and enrollment and registration.
- Which identity domain a user accesses to completes their initial enrollment.

  Note: A user must enroll to a Nymi Band before they register in additional identity domains.
- What are the policy management needs of the customer and how to achieve the objectives.

You can deploy the Nymi IT/OT Solution in various configurations to meet the needs of an organization. The following sections describe two of the most common deployment scenarios. Each scenario can have different configurations and these different configurations have different considerations. If the following table does not descrive your deployment requirements, consult with a Nymi Solution Consultant.

Single *Nymi IT/OT* deployment that is used by one or more sites

Configuration and requirements	Enrollment / registration order	Policy management method	Enrollment / registration policy option value
All Nymi Band users use their Nymi Band to perform authentication tasks in one of the identity domains (ID1). Some or all the Nymi Band users use their Nymi Band to perform authentication tasks in another identity domain (ID2). No special policy requirements.	Enroll all Nymi Band in ID1. Register the Nymi Bands in the ID2, as required.	Configure the policy settings in the NES in ID1.	ID1: Select **`Enrollment only`**. ID2: Select **`Registration only`**.

Configuration and requirements	Enrollment / registration order	Policy management method	Enrollment / registration policy option value
Some Nymi Band users use their Nymi Band to perform authentication tasks in one domain only (ID 1 or ID 2). Some users use their Nymi Bands in multiple domains (ID1 and ID2). A domain where all users use their Nymi Band to perform authentication tasks does not exist. No special policy requirements.	For single-domain Nymi Band users, instruct the user to enroll their Nymi Band in the appropriate domain. For multi-domain Nymi Band users, the CWP Administrator decides which domain that the users access for Nymi Band enrollment and which domain to use for Nymi Band registration.	Configure individual user policy and group policy settings in the NES on both domains according to the needs of the users, but ensure that the group policy settings always match for both NES.	Select **`Enrollment and Registration`** for both NES. **Note:** You can disallow registration in one of the domains,depending on your preferred order of enrollment and registration.
All Nymi Band users that use their Nymi Band to perform authentication tasks in an identity domain (ID1) have special policy requirements, such as no haptic feedback. Some users use their Nymi Bands in another identity domain (ID2).	For user that use their Nymi Band in ID2 only, instruct the user to enroll their Nymi Band on the enrollment terminal in ID2. For multi-domain Nymi Band users that use their Nymi Band in ID1 and ID2, instruct the users to enroll their Nymi Bands on the enrollment terminal in ID1 and register their Nymi Band in ID2.	Configure individual user policy and group policy settings in the NES on both domains according to the needs of the users.	ID1: Select **`Enrollment only`**. ID2: Select **`Enrollment and Registration`**.

Mixed regional + site level deployment.

For example, there is a:

- Regional deployment for IT, where there is a single site identity domain (ID1) that works across multiple physical sites.
- Per-site deployment for OT, where each site(x) has its own OT identity domain (ID2x).

Each ID has its own Nymi Enterprise Server(NES). The assumption is that each user will use their Nymi Band in a single site ID2x only. Some users will enroll their Nymi Band in IT. Some users will enroll their Nymi Band in one site in ID2x. Some might have a Nymi Band association in ID1 and ID2x, where they enroll the Nymi Band in one ID and register in the other.

Configuration and requirements	Enrollment / registration order	Policy management	Enrollment / registration policy option value
All Nymi Band users use their Nymi Band to perform authentication tasks in one of the identity domains (ID1). Some or all the Nymi Band users use their Nymi Band to perform authentication tasks in another identity domain (ID2x).	Enroll all Nymi Bands in ID1. Register the Nymi Bands in ID2x, as required.	Configure the policy settings in the NES in ID1.	ID1: Select **`Enrollment only`**. ID2x: Select **`Registration only`**.
Some Nymi Band users use their Nymi Band to perform authentication tasks in one domain only (ID1 or ID2x). Other users use their Nymi Bands in two domains (ID1 and ID2x). A domain where all users use their Nymi Band to perform authentication tasks does not exist. No special policy requirements.	For single-domain Nymi Band users, instruct the user to enroll their Nymi Band in the appropriate domain. For multi-domain Nymi Band users, instruct the user to enroll their Nymi Band in the OT domain ID2x, and then register their Nymi Band in the ID domain ID1.	Configure group policy settings in the NES on both domains, but ensure that the group policy settings always match for both NES. For users who access both identity domains that require individual policies, define the policy on the Enrollment NES for the appropriate users. **Note:** Involve all Global administrators when you set the individual user policies for the ID1-only users.	ID1: Select **`Enrollment and Registration`**. ID2x: Select **`Enrollment Only`**.

Configuration and requirements	Enrollment / registration order	Policy management	Enrollment / registration policy option value
Some Nymi Band users use their Nymi Band to perform authentication tasks in one domain only (ID1 or ID2x). Other users use their Nymi Band in two domains (ID1 and one of the ID2x). All Nymi Band users that use their Nymi Band to perform authentication tasks in an OT identity domain (ID2x) have special policy requirements, such as no haptic feedback.	For users that use their Nymi Band in only one identity domain, instruct the user to enroll their Nymi Band on the enrollment terminal in that identity domain. For multi-domain Nymi Band users that use their Nymi Band in ID1 and one of the ID2x, instruct the users to enroll their Nymi Bands on the enrollment terminal in ID2x and register their Nymi Band in ID1.	Configure group policy settings in the NES all identity domains, but ensure that the group policy settings in ID2x reflect the special requirement, such as haptic feedback disabled. For users who access both identity domains that require individual policies, define the individual policy on the Enrollment NES for those users. **Note:** Involve all Global administrators when you set the individual user policies for the ID1-only users.	ID1: Select **`Enrollment and Registration`**. ID2x: Select **`Enrollment only`**.

Migrating to the Nymi IT/OT Solution

For customers that currently use a pre-CWP 1.18.x implementation of the Nymi IT/OT solution, review the recommended sequence of actions to migrate the implementation to CWP 1.18.0.

Note: In the following instructions, identity domain 1(ID1) is the source domain, and identity domain 2(ID2) is the destination domain of the IT-OT synchronization, which means that users enroll their Nymi Bands in ID1, and then register their Nymi Bands in ID2.

1. Stop IT-OT synchronization on the SQL Server in ID1.
2. Run the following SQL script on the ID2 (Target) database: ***DROP VIEW IF EXISTS [im].[UserCoreLookup];***
3. In ID2, perform the following actions:
   - Update all Connected Worker Platform(CWP) components except firmware to CWP 1.18.0 or later.
   - Update all Evidian components.
   - In the active NES Group policy, from the **`Enrollment / Registration`** list, select **`Registration only`**, or **`Enrollment and Registration`** as appropriate
   - In the active NES Group policy, from the **`Policy management for assigned Nymi Bands`** list, select **`Do not manage policy`**.
4. In ID1, perform the following actions:
   - Update all Connected Worker Platform(CWP) components except firmware to CWP 1.18.0 or later.
   - Update all Evidian components.
   - In the active NES Group policy, from the **`Enrollment / Registration`** list, select **`Enrollment only`**, or **`Enrollment and Registration`** as appropriate
   - In the active NES Group policy, from the **`Policy management for assigned Nymi Bands`** list, select **`Manage policy`**.
5. Verify the operation of the solution and then decommission IT-OT synchronization.
6. Upgrade firmware on all Nymi Bands to CWP 1.18.0 or later

Notes:

- After you complete the update and migration, the previously enrolled Nymi Bands continue to support only 2 identity domains. Nymi Bands that you enroll after the update support 3 identity domains.
- If necessary, you can only perform the update and migration in ID2 and not proceed with (or postpone) steps 4 and 5.

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