Nymi With Evidian Functional Specifications

Connected Worker Platform

1.3

2022-06-01

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.

Connected Worker Platform Components in a Local Configuration

The Connected Worker Platform enables administrators and users to manage Nymi Bands in an enterprise setting. The Connected Worker Platform is comprised of Nymi-specific components and enterprise components, as shown in the following figure.

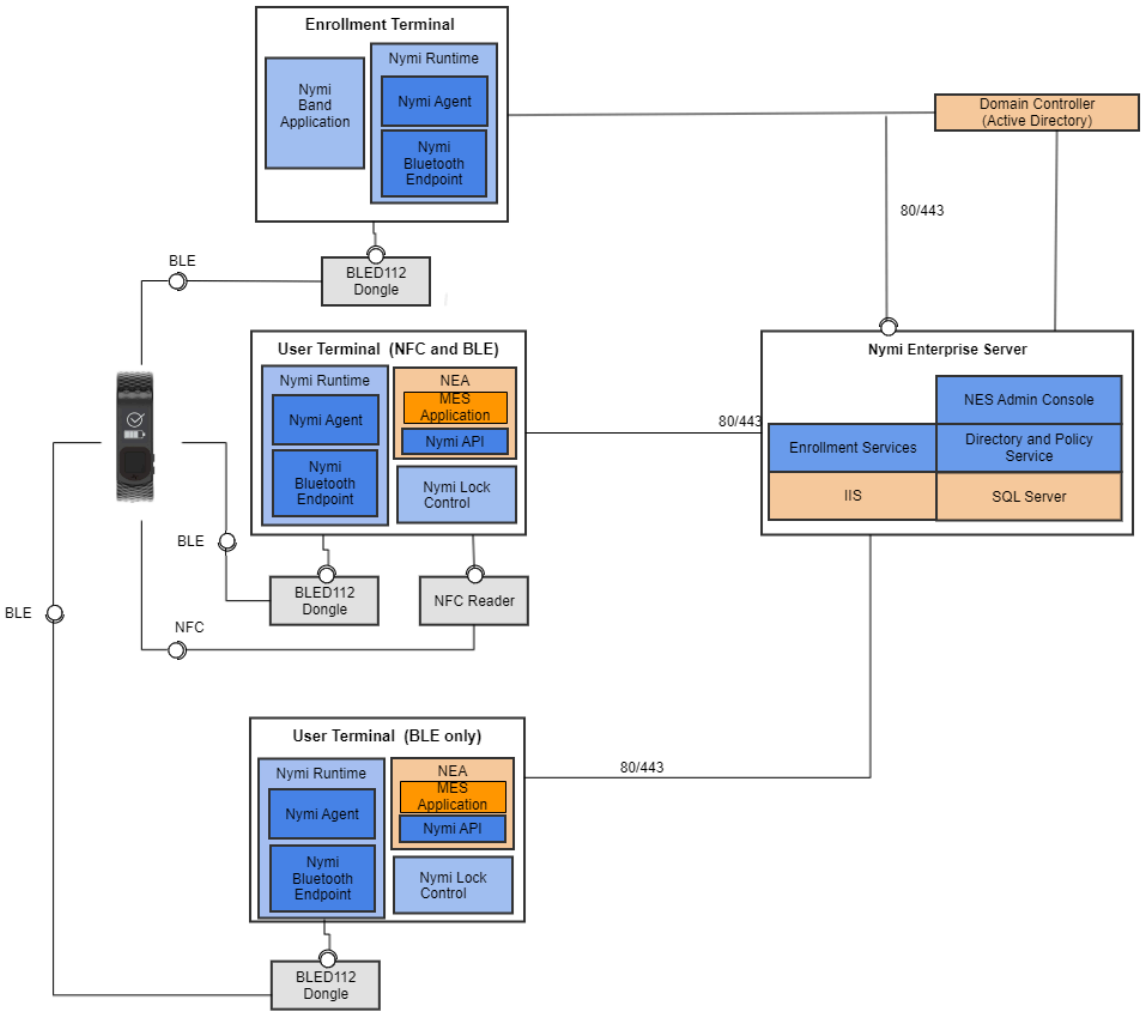

Figure 1: Connected Worker Platform components and connection ports

The Connected Worker Platform consists of the following components..

Table 1: Connected Worker Platform Components

Component	Description
Enrollment Terminal	Windows 10 machine 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.
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`.
User Terminal	Windows 10 machine on which you install Nymi components that allow users to perform authentication tasks with the Nymi Band.
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 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 requires the Nymi Runtime software.
Nymi Lock Control	A Windows application that allows the user to unlock their terminal without entering their username and password.

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.
Domain Controller (DC)	Windows server with external directory and database systems, such as Active Directory.

Connected Worker Platform Deployment in Citrix Environment

The following figure provides an overview of the `Connected Worker Platform` components that are installed in a Citrix environment.

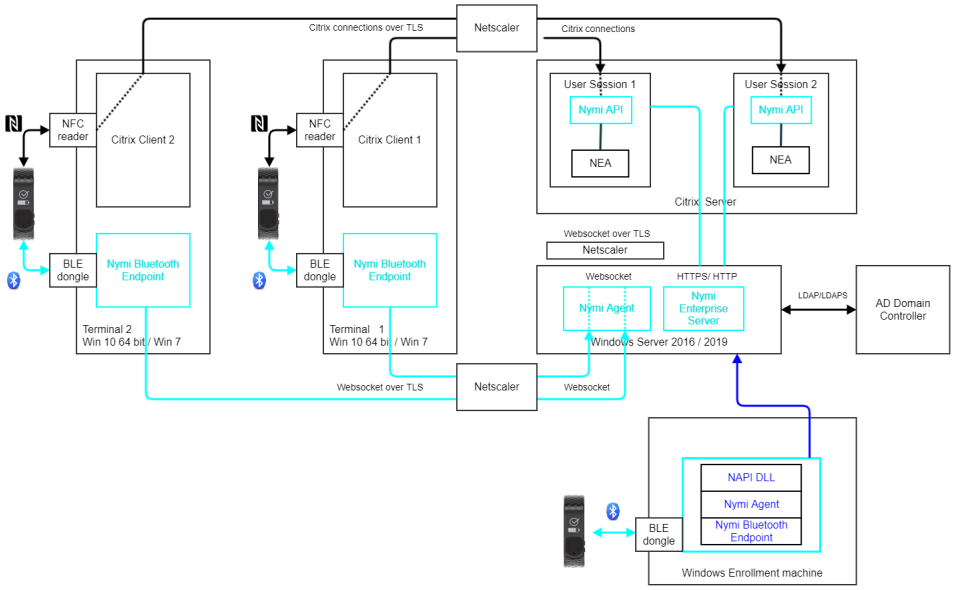

Figure 2: Connected Worker Platform components in a Citrix environment

In Citrix and RDP environments, the user launches an NEA that is installed on a remote session host. Different user sessions run their own NEA instance. In this configuration the NEA communicates with a centralized Nymi Agent, which is installed on a single machine or a cluster of two or more machines in the environment.

This figure shows the following configuration:

- The Nymi Bluetooth Endpoint is installed on each Citrix client. The Nymi Bluetooth Endpoint service on each Citrix client communicates with the Nymi Agent service, which is installed on a separate host, on websocket port 9120.
- The Nymi Agent is installed in an central location that is accessible to all user terminals, for example on the NES server.
- An *nbe.toml* file is installed on the Citrix client, and is configured with the location of the Nymi Agent.
- An NEA runs on the Citrix server and includes the *nymi_api* for communicating with Nymi Bands.

Connected Worker Platform Deployment in RDP Environment

The Connected Worker Platform support deployments in RDP Environments.

The following figure provides an overview of the Connected Worker Platform components that are installed in an RDP environment.

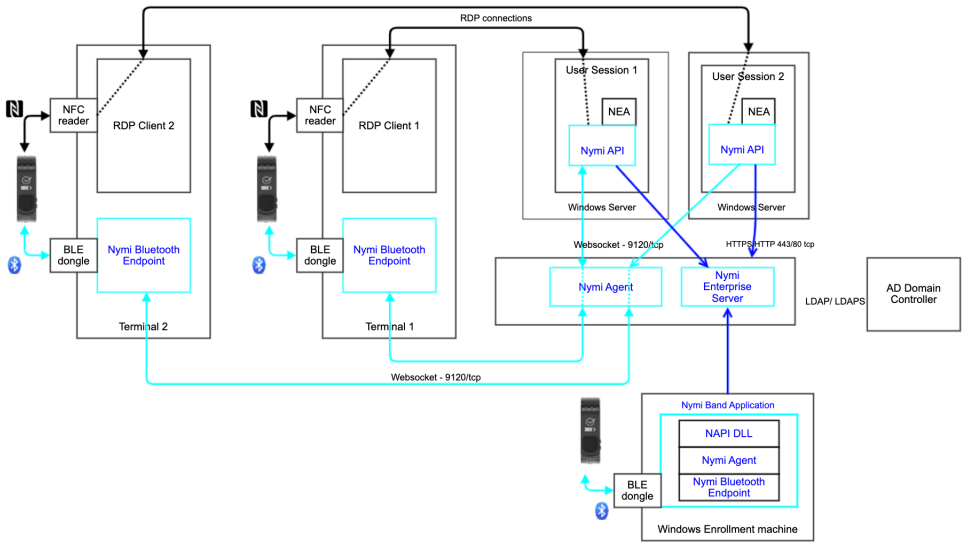

Figure 3: Connected Worker Platform components in a RDP environment

In RDP environments, the user launches an NEA that is installed on a remote session host. Different user sessions run their own NEA instance. In this configuration the NEA communicates with a centralized `Nymi Agent`, which is installed on a single machine or a cluster of two or more machines in the environment.

This figure shows the following configuration:

- The `Nymi Bluetooth Endpoint` is installed on each RDP client. The `Nymi Bluetooth Endpoint` service on each RDP client communicates with the `Nymi Agent` service, which is installed on a separate host, on websocket port 9120.
- The `Nymi Agent` is installed in an central location that is accessible to all user terminals, for example on the NES server.
- An *nbe.toml* file is installed on the RDP client, and is configured with the location of the `Nymi Agent`.
- An NEA runs on the RDP server and includes the *nymi_api* for communicating with Nymi Bands.

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.

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 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 user terminals to provide local BLE communications with Nymi Bands through the Nymi-provided BLE adapter (USB dongle).

Deploy Smart Distancing and Contact Tracing

`Connected Worker Platform` includes many components, which together provide a Smart Distancing and Contact Tracing(SDCT) container clustered service that addresses contact tracing, smart reminders, and attestations requirements to support a safe workplace environment.

The following section provides an overview of the `Connected Worker Platform` with the SDCT service.

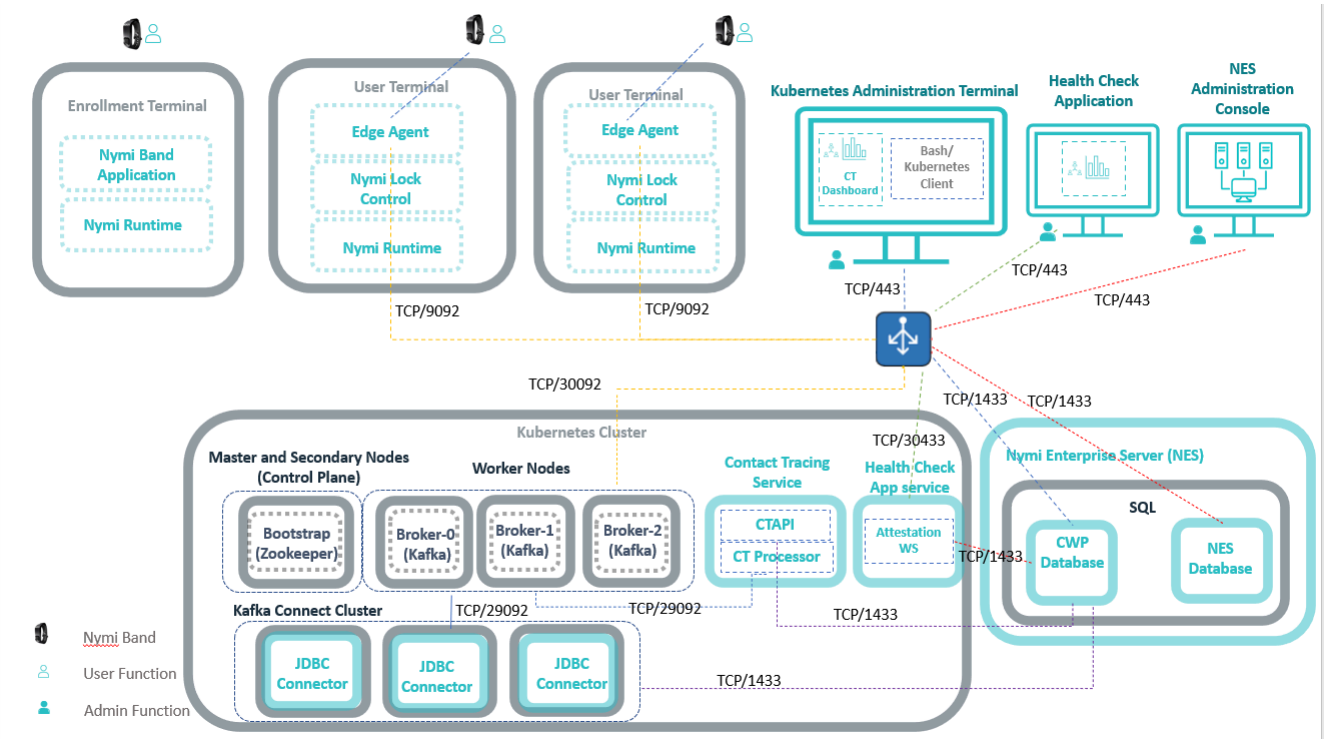

Figure 4: Connected Worker Platform with SDCT Environment

Enrollment Terminal

Terminal on which you install the `Nymi Band Application`. User access the `Nymi Band Application` to enroll to a Nymi Band. The `Nymi Band Application` also installs the `Nymi Runtime` application.

Contact Tracing Events

When a user wearing an authenticated Nymi Band stays in close proximity to another user wearing an authenticated Nymi Band for approximately 15 cumulative minutes over a 24-hour period.

User Terminal

A thick or thin client that is used by a Nymi Band user to perform daily tasks. When you install `Nymi Lock Control` and `Nymi Runtime` on the user terminal, users can lock and unlock the user terminal with an authenticated Nymi Band.

Nymi Edge Agent

The `Nymi Edge Agent` is installed on each user terminal in the environment and establishes BLE communication with Nymi Bands via `Nymi Bluetooth Endpoint` and the `Nymi Agent` services that are installed by `Nymi Runtime`.

`Nymi Edge Agent` retrieves contact tracing data from Nymi Bands within 3-4 meters of the user

terminal. `Nymi Edge Agent` sends the data to the Kafka processing system in the Kubernetes cluster.

Kubernetes Cluster

Provides container cluster deployment, orchestration, scaling, failover and management for the SDCT container clusters. The Kubernetes cluster includes:

- At least one master node and one or more secondary nodes on which Zookeeper resides. Also referred to as the control plane. The control plane consists of control plane master nodes that manage Kubernetes controllers, such as replication controller, endpoint controller, namespace controller, and service accounts controller. A control plane may consist of one or more master nodes (control plane master nodes) to run across multiple computers for high availability, however only one master node may be active at a time.
- Three or more worker nodes on which the brokers and Kafka reside. The worker nodes run containerized applications and host pods (components of an application's workload).

  Each node consists of:

  - kubelet, which ensures that containers are running in a pod
  - kube-proxy, which directs network traffic to and from pods
  - container runtime, which runs the containers.

  Each node is managed by the control plane. Typically, there are several nodes in a cluster, and a pod typically has one container.

  Zookeeper sends jobs to the brokers. SDCT interacts with 5 services in the cluster: bootstrap, broker-0, broker-1, broker-2, and `Contract Tracing API` (`CTAPI`).
- Contact Tracing Service, which includes:

  - `CTAPI` is the part of Contact Tracing Service that provides the contact tracing dashboard and an API to access contact tracing graph data.
  - `Contact Tracing Processor` is the part of Contact Tracing Service that generates contact tracing graph data from contact tracing events.
- Kafka, receives and processes contact tracing data from `Nymi Edge Agent`. The Kafka processing system and the `Contact Tracing Processor` transform contact tracing data and then send the data to the CWP Database.

- Kafka Connect Cluster contains Kafka Connect Nodes. Each Kafka Connect Node contains a JDBCConnector.
- JDBCConnector uses Kafka Connect to store authentication and temperature information events in the CWP Database. The configuration of the JDBCConnector determines how the information that is retrieved from the Nymi Band (and published on Kafka) is stored in the CWP Database.

CWP Database

Stores information about contact tracing, Nymi Band authentication, temperature sensing, and Health Attestation results that are received from `CTCS`. Contact tracing data contains information from the Nymi Enterprise Server for contact tracing purposes.

SDCT Management Terminal

Provides the CWP Administrator with the following tools to manage the SDCT environment.

- bash to create and manage the Kubernetes cluster.
- kubectl (AWS only) to manage the Kubernetes cluster and services.
- Contact Tracing Dashboard, a web-based application that allows you to visualize and analyze contact tracing data from the CWP Database for employees that are enrolled in the Contact Tracing program. Use the Contact Tracing Dashboard to view the relationships between contact tracing events from different users. Contact Tracing Dashboard retrieves events in the `CWP Database` via `CTAPI`.

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

Hardware and Software 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.

Software requirements

NES has the following software requirements.

- Microsoft Windows Server 2016 or 2019
- Microsoft IIS
- Microsoft SQL Server 2016 and later
- Microsoft .NET Framework 4.8

Note: Microsoft SQL Server Express 2017 and Microsoft .NET Framework 4.8 are bundled in the NES installer.

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

Minimum requirements for the Nymi Band Application

The section summarizes the minimum software and hardware requirements for the Nymi Band Application.

Software requirements

- Windows 10, 64-bit
- Windows 7, 64-bit

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
- Bluetooth Low Energy (BLE) radio antenna, present in Bluegiga BLED112 BLE adapter.

Minimum Requirements for Nymi Lock Control

`Nymi Lock Control` supports the following operating system versions:

- Windows 10, 64-bit

Other considerations:

- `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..

Minimum Requirements for User Terminals

CWP 1.3 supports the following operating systems on which you can install `Nymi Runtime` and use the Nymi Band to perform authentication tasks in an MES application.

- Windows 10 x86-64, including on Citrix, RDP, and VMWare Horizon
- HP ThinPro x86-64, including on VMWare Horizon
- IGEL OS v10, including IGEL Thin Client on Citrix

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. Usernames and passwords are not stored by NES.
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 the NFC reader if 3 cm of plexiglass is between the NFC reader and the 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.

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.

Smart Distancing and Contact Tracing Hardware and Software Requirements

This section describes the hardware and software requirements for Smart Distancing and Contact Tracing.

NES

- Microsoft SQL Server Management Studio
- Windows 2016
- Windows 2019

Note: Refer to the Nymi Connected Worker Platform Deployment Guide for more information about NES requirements and deployment information.

User Terminal

Review the following requirements for the user terminals on which you install Nymi Edge Agent.

- Supported Operating Systems:
  - Windows 10 64-bit

- TLS 1.2 enabled
- Oracle Java SE Runtime 8 32-bit or 64-bit (included in Oracle JDK 1.8.x)
- OpenSSL (latest version)
- Resides on the same domain as NES
- Root CA certificate for NES and Kafka

Kubernetes Administration Terminal

Review the following requirements for the user terminal that you use to access the Kubernetes cluster:

- OS that supports *kubectl* and *bash* terminal, including Windows 10 64-bit with Linux Bash Shell
- Oracle Java JDK 8 or later (32-bit or 64-bit)
- Javascript-enabled browser, such as Microsoft Edge, Google Chrome, Safari, or Mozilla Firefox

Kubernetes Cluster Deployment

The requirements for the Amazon Linux 2 Kubernetes Cluster deployment include:

- Control plane node: AWS Elastic Kubernetes Services (EKS)
- Worker node: EC2 instance with Amazon Linux II OS (ex. t3.xlarge, t4g.large), 4-core CPU, 16 GB RAM, 512 GB SSD
- Self signed or CA-issued TLS certificates for Kafka and `CTAPI`.

  Note: TLS certificate for `CTAPI` and Kafka can be the same, but the SubjectAlternativeNames must include all of the FQDNs.

CWP Database

The Contact Tracing, Health Attestation and Temperature Alert features store data in a Microsoft SQL database that supports TLS 1.2 and later.

The following Microsoft SQL versions are supported:

- SQL Server or SQL Server Express 2016
- SQL Server or SQL Server Express 2017
- SQL Server or SQL Server Express 2019

If your NES database is one of these supported versions, you can deploy the CWP Database on the SQL server with the NES instance.

Note: SQL Server / SQL Express 2016 and SQL Server / SQL Express 2017 require a patch to provide TLS 1.2 support. Microsoft provides more information.

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 6: 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	NES maintains an audit log of Nymi Band user assignments Evidian maintains an audit log of Nymi Band user assignments The Smart Distancing and Contact Tracing database maintain an audit log of contact tracing events, high skin temperature alerts, employee health attestation records, and secondary screening records. • A record of each change (create, update, delete) to a system record must be kept, including the date and operator ID. • The audit log must be accessible to the enterprise that deployed the `Connected Worker Platform` solution, without support from Nymi. • The audit log must be stored in an intelligible, well-defined format, and be available at any time for review, even past the lifetime of NES. • Additional fields can be added to the log later without affecting existing records (e g. a "reason for change" field could be added later). • The existence of the audit log and a procedure for viewing its administrator. • Nothing in the Nymi system will allow a user to change audit log records after the record has been generated.

Interfaces

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

Table 7: 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-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 8: 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 user to a Nymi Band in environments where Evidian and NEAs developed with the `Nymi SDK` coexist.

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 9: 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 10: Functional specifications for MES support

URS #	User Specification	FS #	Functional Specification
URS-014 URS-023	The Solution provides user authentication to Windows and the MES by using AD credentials. 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 #	User Specification	FS #	Functional Specification
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 11: 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	FS-ENV-003	The Nymi Band can be sanitized with an alcohol wipe or spray.

Glossary

Definitions/acronyms used throughout this document are defined below.

Table 12: 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.

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