Overview Guide

Nymi Connected Worker Platform
v1.0
2022-05-16

Contents

Preface

This document is part of the Connected Worker Platform 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. An CWP Administrator is the person in the enterprise that manages the Connected Worker Platform for their work place.

Third-party Licenses

This product comprises subject matter which was obtained under an open source licenses. For details about Third-party Licenses, see the 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	May 16, 2022	First release of this document for the CWP 1.3 release.

Nymi Connected Worker Platform Environment

Nymi's Connected Worker Platform 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.

The Connected Worker Platform 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, Connected Worker Platform addresses numerous use cases. These include, but are not limited to:

- Smart Distancing and Contact Tracing
- Physical Access
- Passwordless Windows Logon
- Automatic Terminal Locking
- Secure Printing
- Manufacturing Execution System (MES) Signing

The goal of the Connected Worker Platform 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.

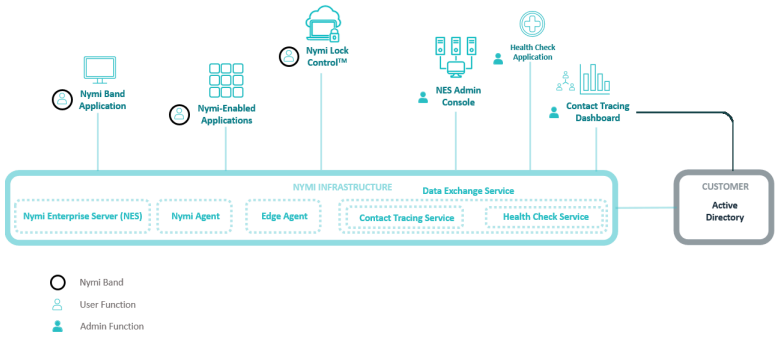

Figure 1: Nymi Connected Worker Platform Core Components

The Connected Worker Platform solution can be used as a stand-alone solution or integrated into third-party applications, devices, or services.

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.

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 NES 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.

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 Lock Control

`Nymi Lock Control` is an application that provides users with the ability to manage access to a terminal, without typing a username and password. `Nymi Lock Control` verifies user access through Active Directory.

When you install `Nymi Lock Control` on a user terminal, the following functionality is supported:

- Unlocking or logging into a terminal by tapping an authenticated Nymi Band on an NFC reader that is attached to the terminal.
- Unlocking or logging into a terminal by placing an authenticated Nymi Band within the range of the Bluetooth adapter, and clicking the **`Submit`** button on the `Nymi Credential Provider Login` screen.
- Automatically unlocking or logging into a terminal by being placing an authenticated Nymi Band within range of the Bluetooth adapter and tapping their keyboard.
- Locking the user terminal when the authenticated user is not within the Bluetooth range of the terminal or when the user removes their Nymi Band.
- Preventing a user terminal from locking by keeping an authenticated Nymi Band within Bluetooth range.

Note: Nymi Lock Control is a single domain solution and does not support cross-domain access. All terminals must be on the same domain as the Nymi Enterprise Server host.

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.

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

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 WebAPI`.

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 WebAPI`

The `Nymi WebAPI` provides Nymi developers with a simplified way to utilize the functionality of the Nymi SDK, over a WebSocket connection. The `Nymi WebAPI` allows developers to write web applications that access services available from the `Connected Worker Platform`. You can configure and enable the `Nymi WebAPI` 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 token and allows secure communications with Nymi Bands using the Nymi Security Protocol. Install the Nymi Agent locally (similar to the Nymi Band Application) 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 WebAPI`: 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 Connected Worker Platform.

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.

Smart Distancing and Contact Tracing

Nymi offers a smart distancing and contact tracing solution that will allow users to accurately track contact events and encourage social distancing behavior.

To implement the Smart Distancing and Contact Tracing (SDCT) functionality, you will install the Nymi Edge Agent on each user terminal in the environment and use the NES Administrator Console to enable settings in the NES active policy.

Using the Contact Tracing Dashboard

Access the Contact Tracing Dashboard to visualize and analyze contact tracing data for employees that are enrolled in the Contact Tracing program.

Proximity events that are logged in each employee's Nymi Band are uploaded to the Contact Tracing Dashboard via the `Nymi Edge Agent` that is installed on a user terminal. These contact events are viewed on the Contact Tracing Dashboard, where they can be analyzed to provide:

- Timely and targeted response for positive diagnosis.
- Timely and reliable contact tracing history.
- Coverage information and trends on social distancing performance.
- Targeted intervention to modify behavior and prevent an outbreak.

Using Health Attestation

Connected Worker Platform(CWP) provides organizations with the ability to manage access into the workplace based on the results of an individual's self assessment.

When a CWP Administrator enables the **`Attestation on Nymi Band`** option in the active NES policy, the health attestation feature on the Nymi Band is enabled. After a user successfully authenticates to their Nymi Band, the Nymi Band displays a Health Check Status question. If the user provides a positive answer on the Nymi Band, the Nymi Band grants users with the ability to use the

Nymi Band to gain physical access to a SEOS-enabled door. If the user provides a negative answer on the Nymi Band, the ability to use Nymi Band to the gain physical access to a SEOS-enabled door remains disabled.

Optionally, corporate policy might require that users complete an independent health attestation prior to answering the health status question on the Nymi Band. Nymi provides an optional web-based attestation application that allows administrators to display a set of pre-defined health check questions, which the user answers and submits. The application provides the user with the results of the attestation (pass or fail), and the user can then indicate the result on the Nymi Band. The web application also provides Health and Safety personnel with a web-based Health Dashboard to view historical information about attestation results for users and allows personnel to record the outcome of subsequent secondary screening, if required.

Note: The health check questions provided in the application are fixed and a record of each attestation result is stored for 30 days. If you require changes, contact your Nymi Solution Consultant.

Using Temperature Alerts

The CWP solution offers organizations the ability to alert Nymi Band users to elevations in skin temperature, and to prompt the user to perform secondary screening.

When you enable the **`Temperature Alerts`** option in the active NES policy, an authenticated Nymi Band monitors fluctuations in the skin temperature of the wrist over time, and creates a baseline skin temperature profile. When the Nymi Band detects an elevation that deviates from the temperature profile of the Nymi Band user, the Nymi Band displays an alert, and then prompts the user to proceed to a secondary screening station for an additional health assessment. The secondary screening prompt remains on the screen until cleared by an administrator during secondary screening. The Health and Safety personnel access the `Health Check Application` to record secondary screening information for a user when the user receives an alert for an elevated temperature.

You can use temperature alerts in conjunction with health attestation; however, you can use both features independently.

Consider the following information about temperature alerts:

- The Nymi Band does not display an absolute temperature reading for the user and only provides the user with an alert when their wrist temperature is higher than their usual wrist temperature.
- After the Nymi Band creates a temperature profile, an authenticated Nymi Band assesses temperature data for the user hourly. When the Nymi Band detects an elevated temperature for a period of time, the Nymi Band displays an alert to the user.
- A SQL database contains a record of the temperature alerts. The section *Collecting Data From a Nymi Band* provides more information.

Note: The Nymi Band is not a medical device and looks for deviations in skin temperature over time, which is not equivalent to a core body temperature measurement.

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 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

The Connected Worker Platform can be deployed in the following configurations:

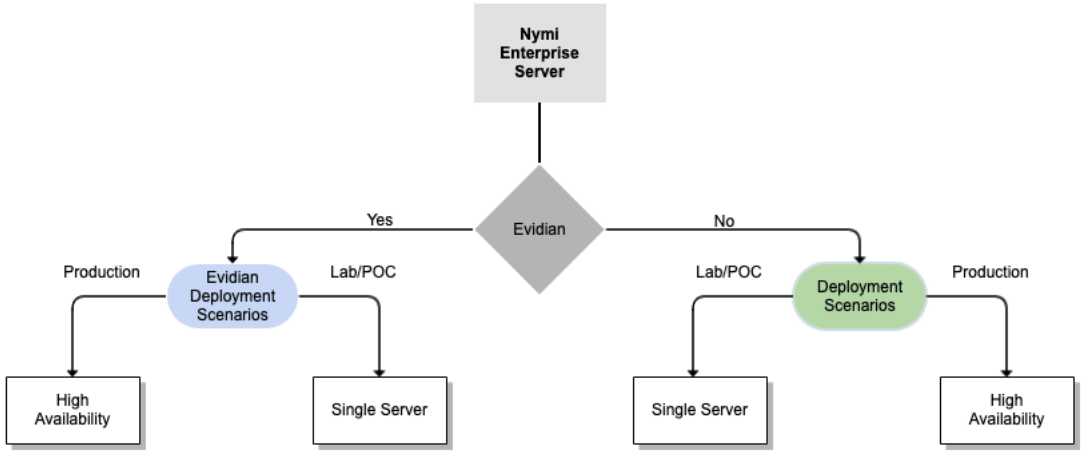

Figure 2: Nymi Enterprise Server Deployments

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 NES Deployment Guide

Deployment Decision	Deployments Details	NymiDocumentation
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 NES 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 NES 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 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 NES 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.

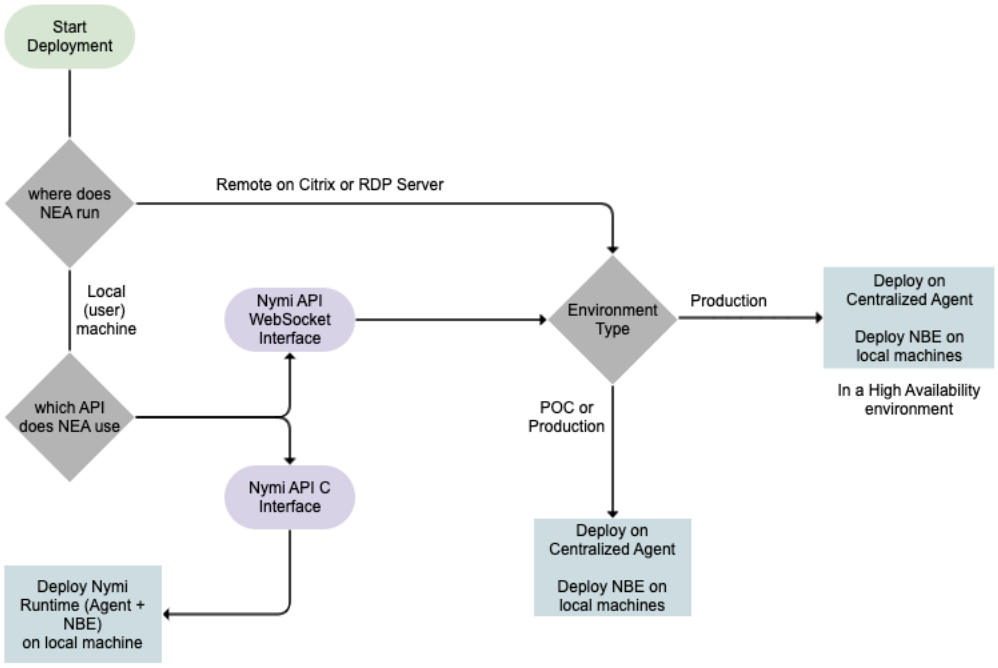

Figure 3: Nymi SDK Deployments

Deployment Decisions

Table 3: SDK Deployment Decisions

Deployments Details	Connected Worker Platform Documentation
On a local user terminal.	Nymi SDK for WebSocket Developer's 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 SDK for WebSocket Developer's 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 SDK for WebSocket Developer's Guide
Deploy `Nymi Runtime` (`Nymi Agent` + `Nymi Bluetooth Endpoint`) on the user terminal.	Nymi SDK for WebSocket Developer's GuideNymi SDK for Linux Developer's 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 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 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 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 NES Deployment Guide**

  This document provides the steps that are required to deploy the Nymi Enterprise Server (NES). This installation uses the `Nymi Token Service` to install certificates that enable communication between components. This document also provides information about deploying the Connected Worker Platform in a Citrix or RDP environment.
- **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 SDK for C Developer's Guide**

  This document provides information about how to develop Nymi-enabled Applications by using the `Nymi API`(`NAPI`).
- **Nymi SDK for WebSocket Developer's Guide**

  This document provides Nymi developers with an alternative way to utilize the functionality of the `Nymi SDK`, over a WebSocket connection managed by a web-based or other applications.
- **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.
- **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`.

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