FIDO2 Deployment Guide

Nymi Connected Worker Platform
v2.0
2023-02-01

Contents

Preface

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

Purpose

The Nymi Connected Worker Platform—FIDO2 Deployment Guide provides information about how to configure Connected Worker Platform and FIDO2 components to allow authenticated users to use the Nymi Band to perform authentication operations.

Audience

This guide provides information to CWP Administrators and Administrators of FIDO2 relying parties, including Microsoft Azure AD, Okta, Ping and Duo, that use Nymi Bands as FIDO2 authenticators to authenticate users.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	May 6, 2022	First release of this document.
2.0	February 2, 2023	Second release of this document. Updated to include information about how to use the Nymi Band with Microsoft Azure AD.

Related Documentation

The Connected Worker Platform (CWP) documentation suite includes the following guides:

- **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 cloud and on-premise deployments.
- **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 with Evidian Installation and Configuration Guide**

  The Nymi Connected Worker Platform with Evidian Guides provides information about installing the Evidian components and configuration options based on your deployment. Separate guides are provided for Wearable, RFID-only, and mixed Wearable and RFID-only deployments.

- **Nymi Connected Worker Platform—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 Connected Worker Platform with Evidian Troubleshooting Guide**

  This document provides overview information about how to troubleshoot issues that you might experience when using the Nymi solution with Evidian.

- **Connected Worker Platform with POMSnet Installation and Configuration Guide**

  The Nymi Connected Worker Platform—POMSnet Installation and Configuration Guides provides information about how to configure the Connected Worker Platform and POMSnet components to allow authenticated users to use the Nymi Band to perform authentication operations in POMSnet.

- **Nymi Band Regulatory Guide**

  This guide provides regulatory information for the Generation 3 (GEN3) Nymi Band.

- **Third-party Licenses**

  The Nymi Connected Worker Platform—Third Party Licenses Document contains information about open source applications that are used in Nymi product offerings.

- **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.

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

What is FIDO2?

FIDO2 is an Nymi SDK for WebSocket Developer's Guide standard for password-less authentication that offers a fast and secure way of logging into a Microsoft Account without entering credentials such as a username and password.

By eliminating the use of passwords, FIDO2 provides ease of use for end users who often have to manage the credentials for a large number of user accounts, and the inherent security issues due to password reuse. For the enterprise IT system owners, the use of FIDO2 reduces the cost of IT system maintenance due to security breaches, and the help desk costs that are associated with managing password resets.

FIDO2 makes use of public / private key pairs, in lieu of passwords, to authenticate to back-end applications and identity systems. The private key is used to prove the user's identity, and it is stored on the user's FIDO authenticator, which is typically a hardware device in the form of a key fob, a USB device, or a Nymi Band. The public key is stored on the back-end application or identity system, and is tied to the user account. The public key allows the back-end to authenticate the user by verifying a signature generated using the user's private key.

FIDO2 is designed so that a single FIDO authenticator, like a Nymi Band, can be used to store the private keys of a large number of back-end applications and identity systems. Furthermore, the FIDO2 design ensures that user privacy is maintained by preventing the correlation of multiple user accounts to a single user, even though the same FIDO authenticator is used to store the FIDO2 private keys of those accounts.

The FIDO2 standards are managed by the FIDO (Fast IDentity Online) Alliance (https://fidoalliance.org/) and is backed by major companies in the technology industry.

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 Band Certification and Compliance

The FIDO Alliance maintains a certification program to ensure interoperability of FIDO2-capable devices and services, and that all FIDO2 devices meet the necessary security requirements.

The Nymi Band is:

- A certified FIDO2 authenticator.
- Certified as Microsoft-compatible.

Use Cases and Workflow

At the beginning of the work day, the user wears their Nymi Band, and authenticates to the Nymi Band by using biometrics. Applications can access all FIDO2 credentials that are stored on the Nymi Band while the Nymi Band remains authenticated.

A user can use an authenticated Nymi Band to perform the following activities during a typical day for a Nymi Band FIDO2 user:

- Log into their Windows machine that is joined to an Azure Active Directory domain (including hybrid-joined machines) by using the FIDO2 credentials for their Azure Active Directory account, which are stored on the Nymi Band. To perform the login, the user wears their authenticated Nymi Bandand places the Nymi Band over an NFC reader that is connected to the Windows machine. The login does not require any other form of user interaction, including a PIN entry.

  Note: Log in is possible even in situations where the machine does not have a network connection.
- Tap their Nymi Band against an NFC reader to log into:
  - Microsoft online services, for example Office 365, Outlook, and SharePoint.
  - Applications like Salesforce and Google.
  - Single-sign-on platforms, such as Ping, Okta, and Duo. The user can log on through recent versions of all major web browsers.

  Note: The user can register for FIDO2 credentials with additional applications, and store the credentials on their Nymi Band.

At the end of the work day, the user takes off their Nymi Band. The Nymi Band immediately deauthenticates, and applications cannot access the stored FIDO2 credentials until the user authenticates to the Nymi Band again.

Prerequisites

Review this section for information about supported NFC readers and prerequisite requirements.

Nymi-Supported NFC Readers

Nymi only supports PC/SC NFC readers. The following technical requirements are required for NFC readers that will be used with the Connected Worker Platform:

- ISO14443A compatibility
- PC/SC compatibility
- Operation frequency of 13.56 MHz

Nymi recommends the HID 5022 USB Reader for its superior performance. It is fully compatible with the Nymi Band and also supports many other smart card technologies and NFC-enabled devices. Should this reader not address your organization's use case in some way, please contact your Nymi Solution Consultant for additional options.

CWP supports the following NFC readers:

- HID Omnikey 5022
- ACS ACR122U
- Systec CONNECT BOX
- Elatec TWN4 LEGIC NFC USB
- HID Omnikey 5127CK Mini
- ACS ACR1252U
- Identiv CLOUD/uTrust 3700 F
- RFIdeas WAVE ID Nano SDK 13.56MHz CSN Black Vertical USB Reader

Web Browser Requirements

To use Nymi Bands for FIDO2, you require at a minimum the following web browser versions.

Operating System	Web Browser
Windows	• Edge (new, Chromium-based): all versions • Edge (legacy): Windows 10 version 1903 • Chrome: 76 • Firefox: 66

Operating System	Web Browser
macOS	Safari: macOS 10.15.2
iOS / iPadOS	Safari: iOS 13.3 / iPadOS 13.3

Nymi Band Requirements

Before a user can use their Nymi Band to perform tasks with their FIDO2 credentials, the user must enroll to the Nymi Band.

Enrollment is the process of associating a new user identity with a Nymi Band. An administrator is not strictly required to be present while a new user enrolls a new Nymi Band; however, for security purposes, a corporate policy might require supervision.

To start the enrollment process, the user puts on their Nymi Band and logs into the Nymi Band Application on the enrollment terminal their corporate credentials. The Nymi Connected Worker Platform—Administration Guide provides more information about the enrollment process. After enrollment, the user can access supported FIDO2 applications and store FIDO2 credentials on the Nymi Band.

A user can delete their user data from the Nymi Band, which removes all credentials that are stored on the Nymi Band, including the FIDO2 credentials. Before the user can use a Nymi Band again, they must re-enroll to a Nymi Band a repeat the process of storing the FIDO2 credentials on the Nymi Band, by using the appropriate FIDO2 application.

Using the Nymi Band with Microsoft Edge

User can use the Nymi Band as a security key to sign into a Microsoft Account on a computer that is running Windows 10 by performing an NFC tap with their authenticated Nymi Band on the Microsoft Edge login screen.

Adding the Nymi Band as a Security Key

Perform the following steps to add the Nymi Band as a security key.

About this task

Perform the following steps a Windows 10 machine.

Procedure

1. In Microsoft Edge, go to the `Microsoft Account` page, and sign in.
2. Select **`Security > More Security Options`**.
3. Under **`Windows Hello and security key`**, select **`Set up a security key`**.
4. Select the **`NFC`** key type, and then click **`Next`**.
   You are redirected to the setup experience window.
5. When prompted, tap your Nymi Band on the NFC reader.

   Note: You might need to tap and hold theNymi Band on the NFC reader for up to 10 seconds.
6. Optionally, name your security key.
7. Sign out of the Microsoft account page.

Using the Nymi Band to Log Into the Microsoft Account

About this task

Procedure

1. On a Windows 10 terminal, open the `Microsoft Edge` browser.

2. Navigate to the `Microsoft Account login` page.
3. Click **`Sign In with a security key`**.
4. Tap your Nymi Band against the NFC reader.

Results

Log into your Microsoft Account succeeds.

Using the Nymi Band with Microsoft Azure

User can use the Nymi Band as a security key to sign into a Microsoft Account on a computer that is running Windows 10 version 1903 or higher by performing an NFC tap with their authenticated Nymi Band on the Microsoft Azure login screen.

Before You Begin

Ensure that you work with your Azure Administrator to configure the proper settings and pre-requisites to enable FIDO2 usage on your tenant by following the steps in the following Microsoft article: Enable passwordless security key sign-in .

Adding the Nymi Band into the Authentication Methods Policy

Configure the Nymi Band as security key that supports passwordless authentication.

About this task

Perform the following actions in the Azure Console.

Procedure

1. Create a group for the users in your organization that use the Nymi Band to perform authentication.
2. Navigate to **`Azure Active Directory > Security > Authentication methods > Authentication method policy`**.
3. In the **`Methods`** table, click **`FIDO2 Security`**.
4. On the **`Basics`** tab, perform the following actions:
   a) Set **`Enable`** to **`Yes`**.
   b) In the **`Target`** section, click **`Add users and groups`**, and then select the group that you created.
   c) Click **`Save`**.

Registering the End User

Register each Nymi Band user to use the Nymi Band for passwordless authentication.

Before you begin

Configure multi-factor authentication and Combined Security Information.

About this task

Each Nymi Band user must perform the following steps while wearing their authentication Nymi Band on a user terminal with an NFC reader.

Procedure

1. From a web browser, log in to **https:**//myprofile.microsoft.com.
2. Click **`Security Info`**.
3. Click **`+ Add sign-in method`**.
4. From the **`Add method`** list, select **`Security Key`**, and then click **`Add`**.
5. On the `Security Key` window, click **`NFC device`**, and then click **`Next`**.
6. On the `More information required` window, click **`Next`**.
7. When the `Tap your security key on the reader or insert into the USB port` window appears, tap and hold the Nymi Band on the NFC reader.
8. Click **`Done`**. The `Security info` window displays the new security key, as shown in the following figure.

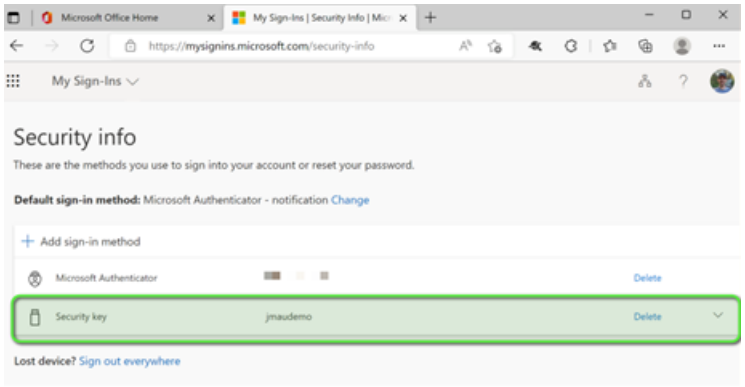


Figure 1: Security Info window

Using the Nymi Band to Log in to Azure

About this task

Perform the following steps on a Windows 10 user terminal.

Procedure

1. Open the `Microsoft Edge` browser.

2. Navigate to the `Microsoft Account login` page.
3. On the `Pick an account` window, select the user.
4. On the `Enter Password` window, click **`Sign in with a security key`**, as shown in the following figure.

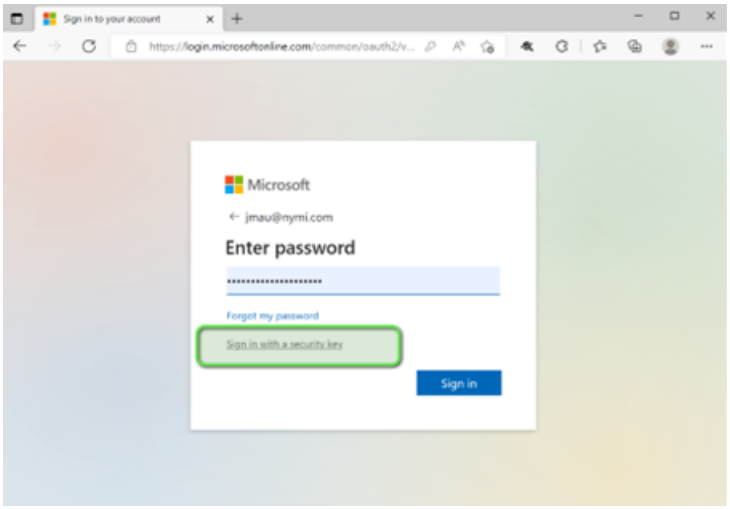


Figure 2: Enter Password window

5. When the `Making sure it's you` window appears, tap your Nymi Band against the NFC reader.

Results

Log in succeeds.

Using the Nymi Band with Okta

You can test the use of the Nymi Band for passwordless login with Okta.

Before you can register the Nymi Band as a FIDO2 toke for testing, you must perform the following actions:

- Create test user groups
- Assign test users to the test user groups
- Create and configure an authentication policy
- Create and configure a new sign on policy

The following sections provide you with high-level steps to perform each task. All supporting screen shots and steps were performed in an Okta tenant.

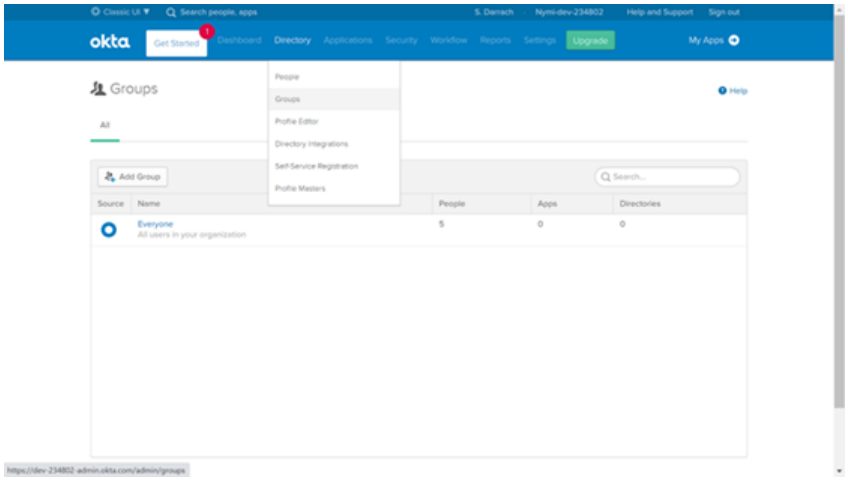
Creating an Okta Usergroup

Perform the following steps in the Okta Management interface.

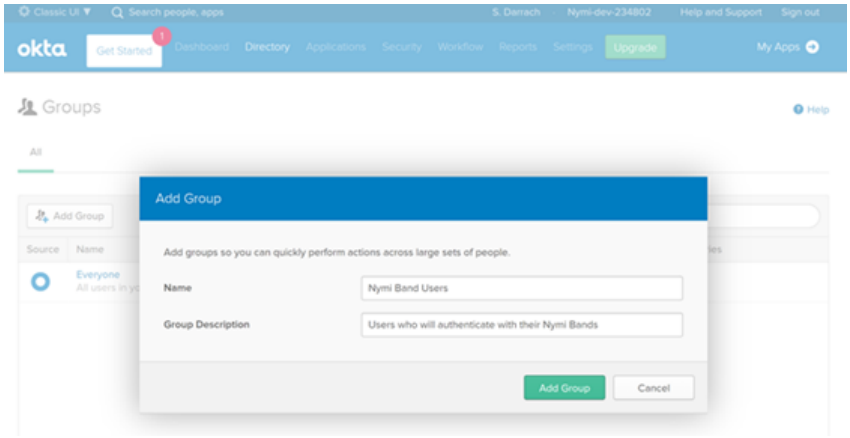
About this task

Procedure

1. From the menu bar, select **`Directory > Groups`**, as shown in the following figure.



2. Click **`Add Group`**.
3. Name the group and provide a short meaningful description, as shown in the following figure.



4. Click **`Add Group`**.

Adding Users to the Usergroup

Perform the following steps to add Okta users to the new Okta usergroup.

About this task

Procedure

1. From the list of groups, select your newly created group.
2. Click **`Manage People`**.
3. In the left-hand column, click the names of people you want to add to the group.
   The following figure provides an example where two users will be added to the group.

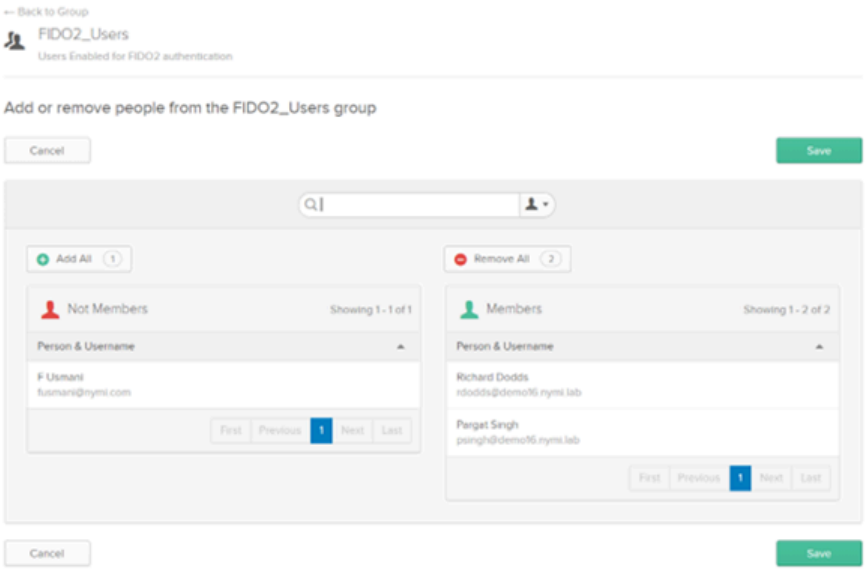


Figure 3: Adding Users to Okta Usergroup

4. Click **Save**.

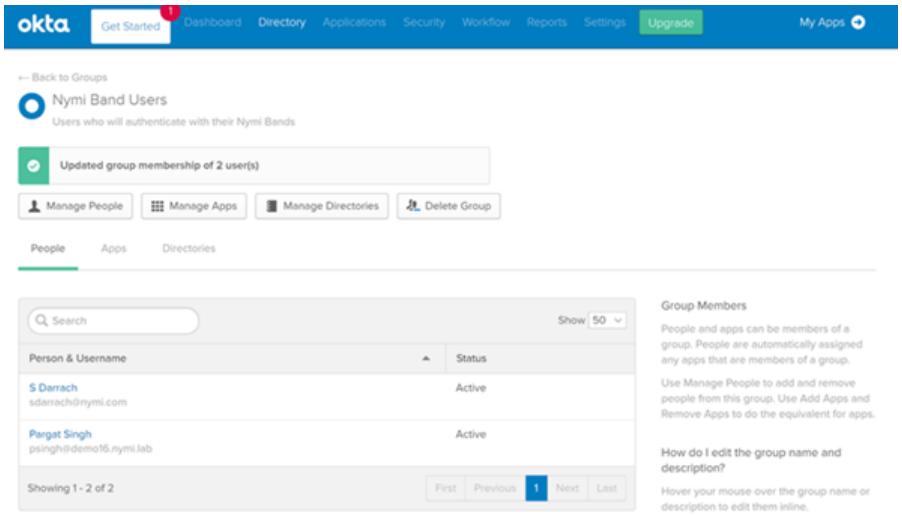


Figure 4: Viewing Users in Okta Usergroup

The `Group` page displays the group with the included members.

Configuring Multifactor Authentication

Multifactor Authentication(MFA) enable users to register their token (Nymi Band) for use with Okta.

About this task

Perform the following steps to configure MFA.

Procedure

1. On the main menu, select **`Security > Multifactor`**.
2. From the **`Factor Types`** list, select **`FIDO2 (WebAuthn)`**.
3. In the upper right corner of the **`Factor Types`** section, click the **`Inactive`** button, and then select **`Activate`**.

   The following figure shows the **`Activate`** button.

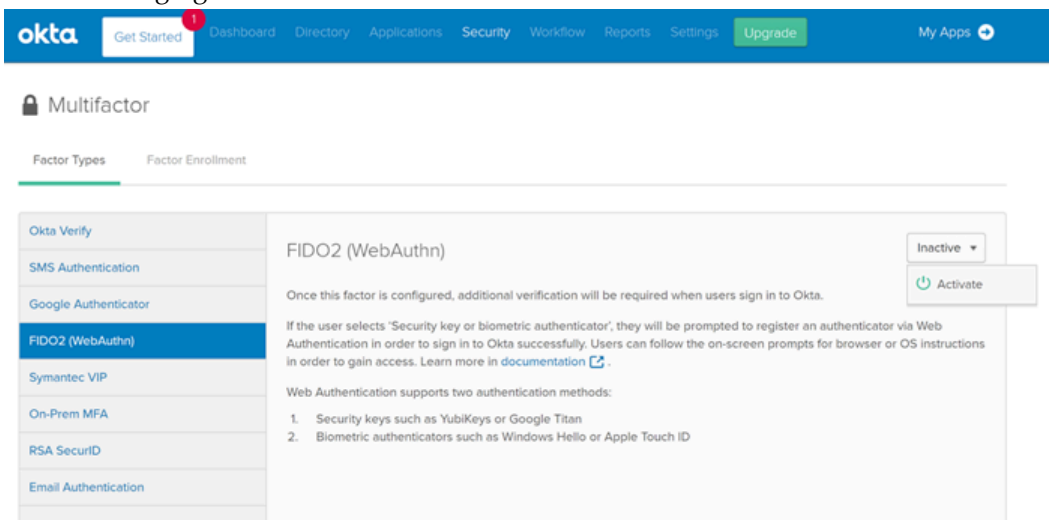


Figure 5: Activating FIDO2 in Okta

4. Click **`Factor Enrollment`**.
5. Click **`Add Multifactor Policy`**.
6. On the `Add Policy` window, perform the following steps.
   a) In the **`Name`** field type the name of the new policy.
   b) Optionally, in the **`Description`**, type an informative description for the policy.
   c) In the **`Assign to groups`** field, and start typing the name of the group you created.

      The group that you created appears, as shown in the following figure.

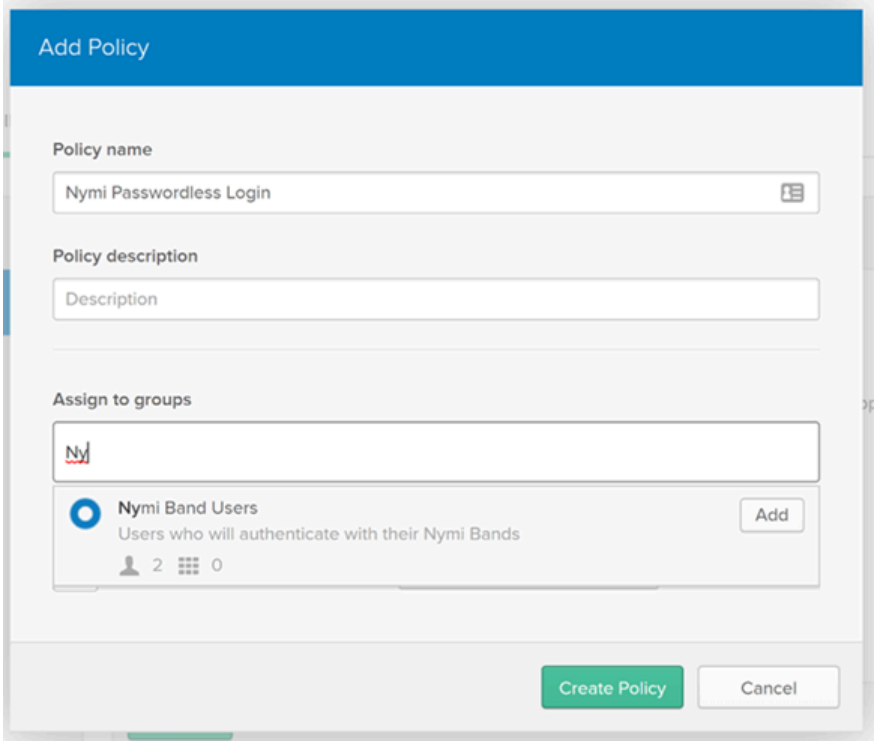


Figure 6: Assign to groups window

d) Click Add**Add** to select your group.
e) In the **`Effective factors`** section, set **`FIDO2 (WebAuthn)`** to **`Required`**.
f) Click **`Create Policy`**.

7. In the Add `Rule` dialog, perform the following steps.

a) In the **`Name`** field, type the name of the rule, for example, Enroll MFA.
b) Optionally, in the **`Exclude Users`** field, type the users to exempt from this rule.
c) For the **`THEN`** statement, select **`Allowed`**.
d) Select **`Prompt for Factor`**.
e) Select **`Per Session`**.
f) Click **`Create Rule`**.

Creating an Okta Sign On Policy

About this task

Procedure

1. From the main menu, select **`Security > Authentication`**.
2. Under **`Authentication`**, select **`Sign On`**.

3. Click **Add New Okta Sign-on Policy**.
4. On the Add Policy window, perform the following steps.
   a) In the **Policy Name** field type the name of the new policy.
   b) Optionally, in the **Description**, type an informative description for the policy.
   c) Click **Create Policy and Add Rule**.
5. In the Add Rule dialog, perform the following steps.
   a) In the **Name** field, type the name of the rule, for example, Enforce Passwordless Login.
   b) Optionally, in the **Exclude Users** field, type the users to exempt from this rule.
   c) Leave the default options for the **IF**, **AND**, and **THEN** statements, select **Allowed**.
   d) Scroll down so until the **Authentication** section is fully visible.
   e) For **Authentication methods**, select **Factor Sequence**.
   f) In the first drop-down, select **FIDO2 (WebAuthn)**.
   g) Optionally, set the session expiry.
   h) Click **Create Rule**.

Registering the Nymi Band

After you configure Okta to support the Nymi Band, users can enroll their Nymi Band as a Security Key the first time that they log in.

Before you begin

Ensure that the user wears their authenticated Nymi Band.

About this task

After the user logs into Okta, the enrollment process starts automatically.

Procedure

1. On the Okta Enroll window, click **Enroll**.
   The following figures shows the Okta Enroll window.

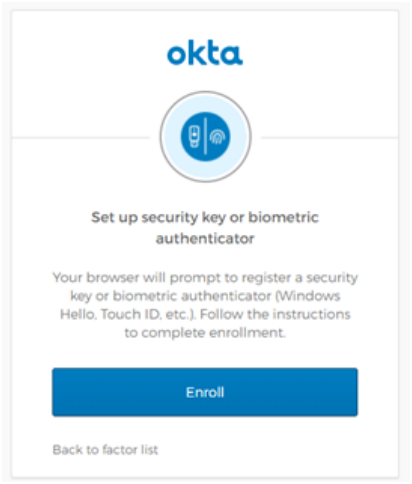


Figure 7: Okta Enroll window

2. On the `Set up Multifactor` window, click **`Configure Factor`**.
   The following figure shows the `Set up Multifactor` window.

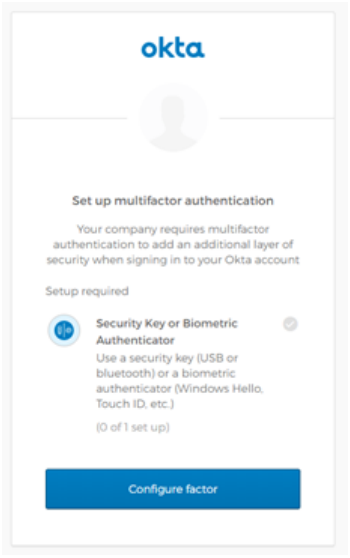


Figure 8: Set up Multifactor window

3. On the `Allow this site to see your security key` dialog, click **`Allow`**.
   The following figure shows the `Allow this site to see your security key` window.

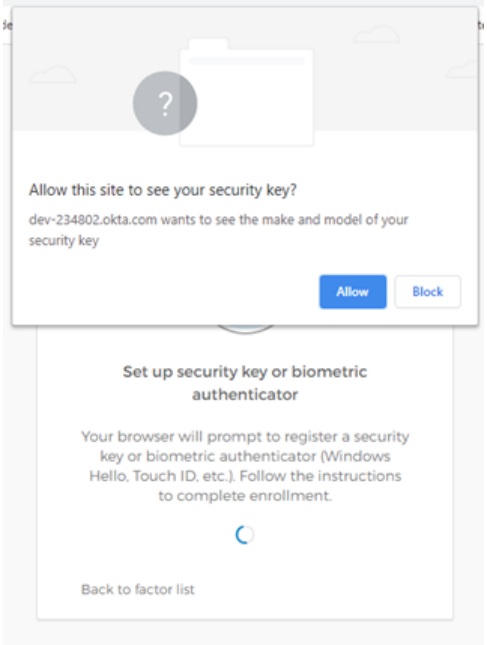


Figure 9: Allow this site to see your security key

4. When prompted to sign in, tap the Nymi Band against the NFC reader.
   The following figure shows sign in window.

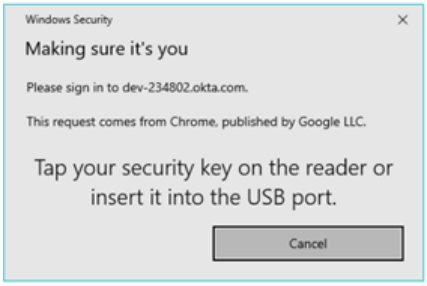


Figure 10: Okta Sign In window

5. On the `Set up Multifactor authentication` window, click **`Finish`**.
   The following figure shows sign in window.

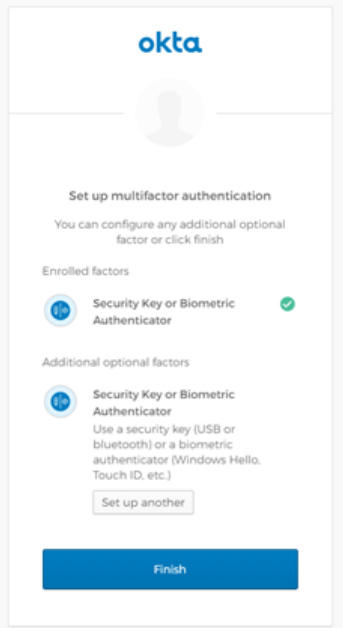
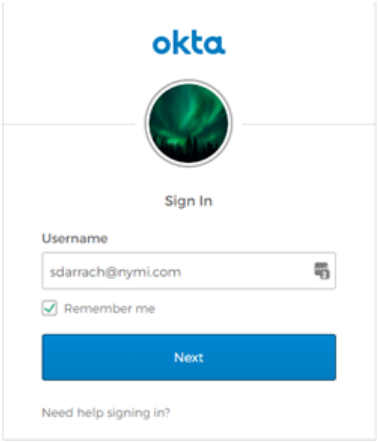


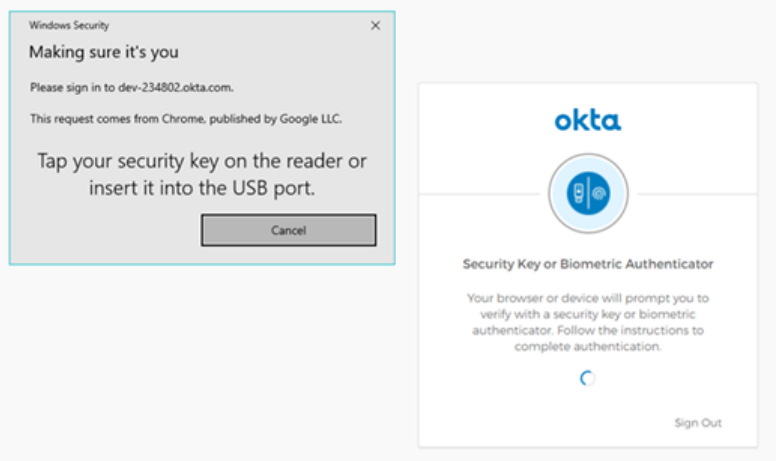
Figure 11: Set up Multifactor window

Results

The `Okta Login` window changes after enrollment completes, as shown in the following figure.



When the user clicks **`Next`**, a pop-up appears prompting the user to sign in, as shown in the following figure. Users can tap their Nymi Band against the NFC reader to login, and when login completes, their home screen appears.



Removing Multfactor Authentication for a User

If required, perform the following steps to remove Multifactor Authentication (MFA).

About this task

When you remove MFA, users cannot use their Nymi Band to log into Okta.

1. Admin User - Go to the Dashboard.
2. In the Shortcuts list, select Reset Multifactor.

Procedure

1. Log into the Dashboard as an admin user.
2. From the shortcuts list, select **`Reset Multifactor`**, as shown in the following figure.
   Figure 12: Reset Multifactor
3. From the user list, select the user, and then click **`Reset Multifactor Authentication`**.
4. On the `Reset Multifactor Authentication` dialog, click **`Reset`**
   The following figures shows the `Reset Multifactor Authentication` dialog.

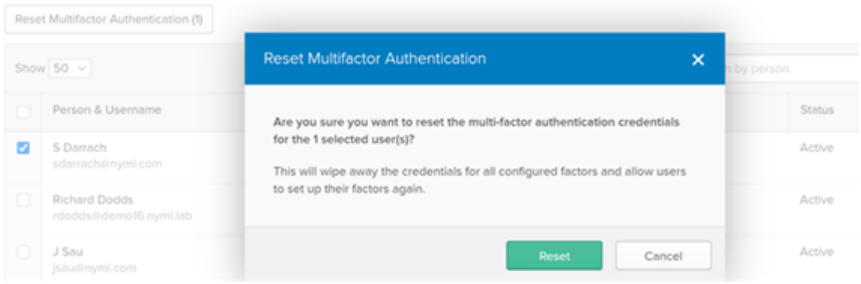


Figure 13: Reset Multifactor Authentication dialog

Using Nymi with Ping

You can use the Nymi Band for passwordless login with Ping or as the second factor in multifactor authentication.

Before you can register the Nymi Band, you must configure security key authentication in PingID or PingFederate. The following articles provide detailed information:

- PingID - Configure Security Key Authentication
- PingFederate – Configure Policy for Passwordless Authentication with a Security Key
- Multifactor authentication

Enrolling the Nymi Band

After you configure Ping to support the Nymi Band, users can enroll their Nymi Band as a Security Key the first time that they log in.

Before you begin

Ensure that an NFC reader is plugged into the user terminal and that the user is wearing their authenticated Nymi Band.

About this task

Perform the following steps on a user terminal.

Procedure

1. On the `Sign On` window, type your username and password, and then click **`Sign on`**.
2. On the `Id` window, click the link **`I want to use my Nymi band`**, as shown in the following figure.

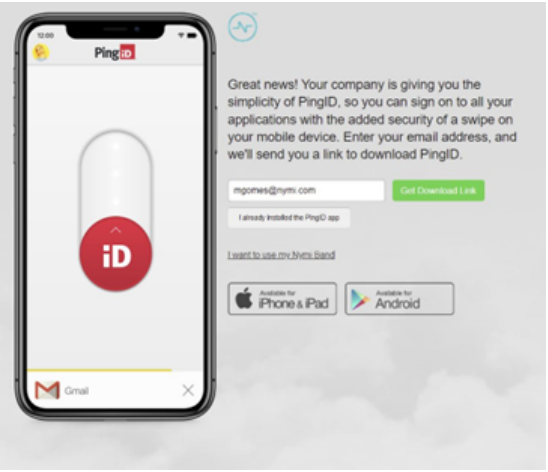


Figure 14: Id window

The following window appears while the Nymi Band pairing occurs.

Figure 15: Nymi Band pairing

3. On the `Alternate Authentication` window, click **`Next`**.

   The following figure shows the `Alternate Authentication` window.

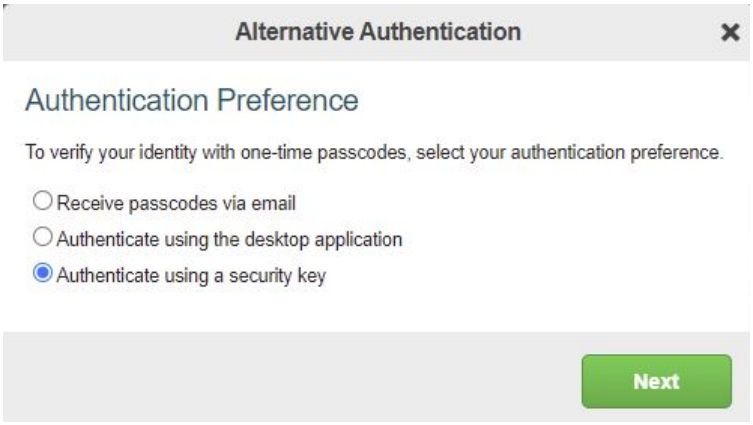


Figure 16: Alternate Authentication window

4. On the `Security key setup` window, click **OK**.

   The following figure shows the `Security key setup` window.

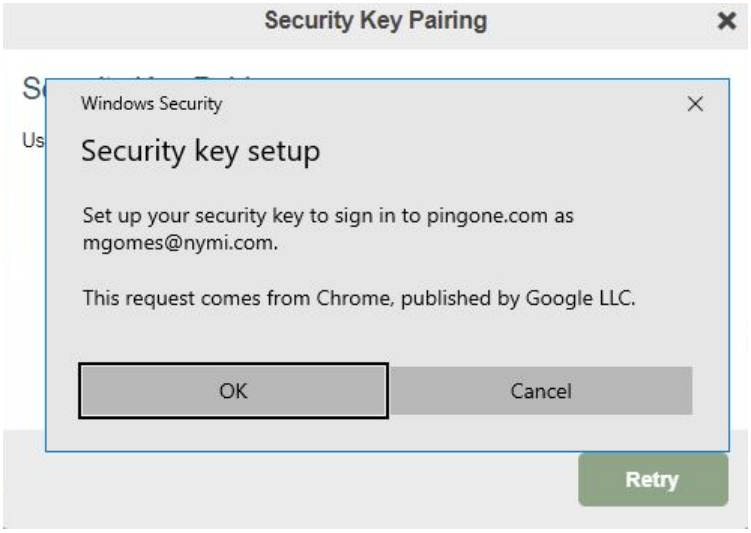


Figure 17: Security key setup window

5. On the `Continue setup` window, click **OK**.

   The following figure shows the `Continue setup` window.

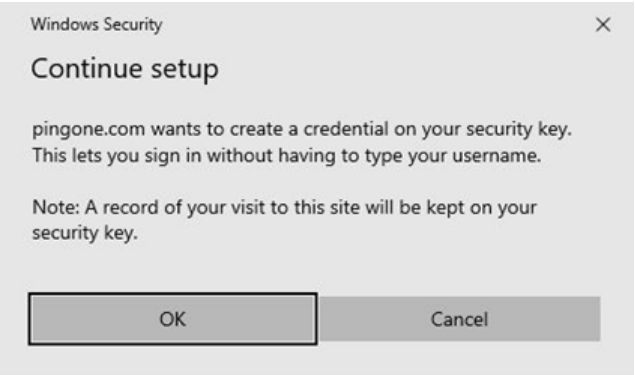


Figure 18: Continue setup window

6. When the `Making sure it's you` window appears, tap the Nymi Band against the NFC reader.

   The following figure shows the `Making sure it's you` window.

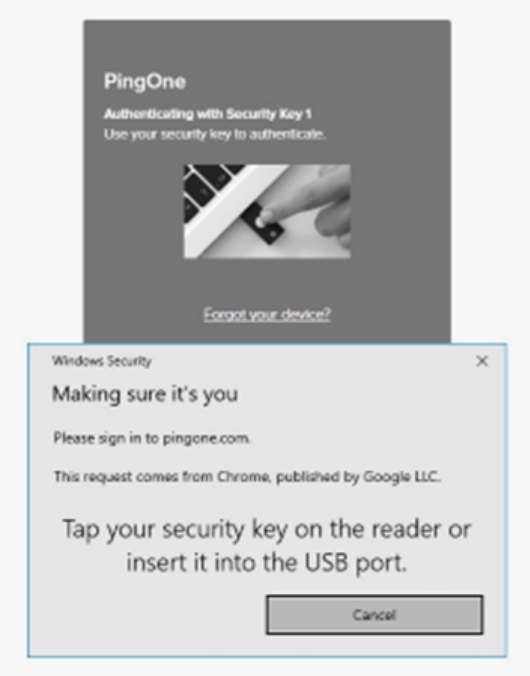


Figure 19: Making sure it's you

The user sees a Success message and is directed back to the login prompt.

Results

The Nymi Band registration completes. On the `Login` window, the user performs one of following actions:

- For passwordless login, theuser enters in their username, and then clicks **`Sign On`**.
- For multifactor authentication, the types their username and password, and then clicks **`Sign On`**.

The `Continue setup` window appears and the user taps the Nymi Band on the NFC reader to gain access to their workspace with their authorized applications.

Using the Nymi Band with Duo

You can use of the Nymi Band for passwordless authentication or as the second factor for multifactor authentication in Duo. login with Duo.

Before you can register the Nymi Band, you must configure security key authentication in PingID or PingFederate. The following articles provide detailed information:

- Configuring Multifactor Authentication
- Configuring passwordless authentication

Enrolling the Nymi Band

After you configure Duo to support the Nymi Band, users can enroll their Nymi Band as a Security Key the first time that they log in.

Before you begin

Ensure that an NFC reader is plugged into the user terminal and that the user is wearing their authenticated Nymi Band.

About this task

Perform the following steps to enroll the Nymi Band

Procedure

1. Navigate to the provided by your administrator.
2. On the `Protect your company account` window, click **`Start Setup`**.
   The following figure shows the`Protect your Company account` window.

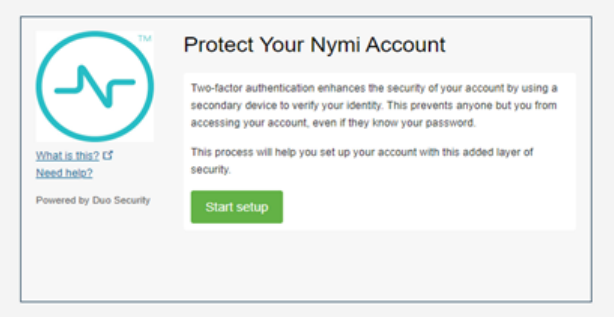


Figure 20: Project your Company account window

3. On the `What type of device are you adding?` window, click **`Continue`**.
   The following figure shows the`What type of device are you adding?` window.

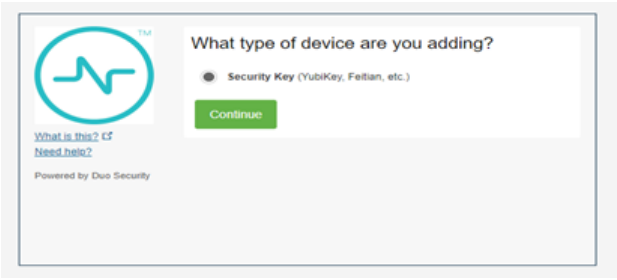


Figure 21: What type of device are you adding? window

4. On the `Enroll your Security Key` window, click **`Continue`**.

   The following figure shows the`Enroll your Security Key` window.

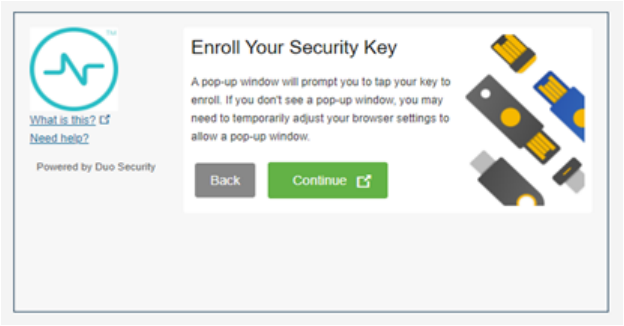


Figure 22: Enroll your Security Key window

5. When the `Making sure it's you` window appears, tap the Nymi Band against the NFC reader.

   The following figure shows the `Making sure it's you` window.

Figure 23: Making sure it's you

6. On the `My settings and devices` window, the security key appears. Click **`Finish Enrollment`**.

   The following figure shows the `Making sure it's you` window.

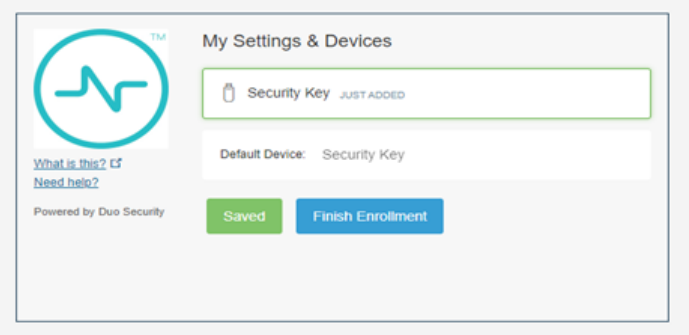


Figure 24: My settings and devices window

7. When enrollment succeeds, the `Enrollment Success` window appears, as shown in the following figure. Close the `Enrollment Success` window

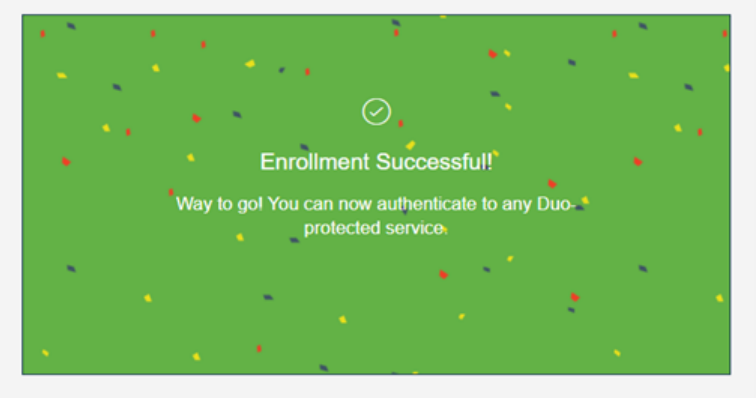


Figure 25: Enrollment Success window

Results

The user can use the Nymi Band to log into Duo.

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