FIDO2 Deployment Guide

Nymi Connected Worker Platform
v4.0
2025-09-05

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.
3.0	September 30, 2024	Third release of this document. Updated to include details about Standalone Mode Nymi Band and CWP Mode Nymi Band.

Version	Date	Revision history
4.0	September 9, 2025	Fourth release of this document. Updates include: • Changes to the *Using the Nymi Band to Log into Web Applications with Microsoft Credentials* section to include information about how to prepare the user terminal to reduce the number of clicks that the user performs before they can perform the Nymi Band tap. • Introduction of Troubleshooting chapter.

Related Documentation

The Nymi 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 authentication on iOS and Windows device.
- **Nymi Connected Worker Platform—Administration Guide**

  This document provides information about how to use the NES Administrator Console to manage the Connected Worker Platform (CWP) system. This document describes how to set up, use and manage the Nymi Band™, and how to use the Nymi Band Application. This document also provides instructions on deploying the Nymi Band Application and Nymi Runtime components.
- **Nymi SDK Developer Guide—NymiAPI(Windows)**

  This document provides information about how to develop Nymi-enabled Applications by using the Nymi API(NAPI).
- **Nymi SDK Developer Guide—Webapi(Windows)**

  This document provides information about how to understand and develop Nymi-enabled Applications (NEA) on Windows by utilizing the functionality of the Nymi SDK, over a WebSocket connection that is managed by a web-based or other application.
- **Connected Worker Platform with Evidian Installation and Configuration Guide**

The Nymi with Evidian Solution—Deployment Guide provides information about how to deploy the Nymi with Evidian solution 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 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 standard for password-less authentication that offers a fast and secure way to log 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 that results from 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(FIDO passkeys), instead of passwords, to authenticate to back-end applications and identity systems. The private key is used to prove the identity of the user, and the key is stored on the FIDO authenticator for the user, A FIDO authenticator 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 FIDO passkeys 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 FIDO passkeys for their Azure Active Directory account, which are stored on the Nymi Band. To perform the login, the user wears their authenticated Nymi Band and 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 FIDO passkeys with additional applications, and store the FIDO passkeys 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 FIDO passkeys 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

Operating System and Web Browser Requirements

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

Operating System	Web Browser
Windows 10 Windows 11	• Edge (new, Chromium-based): all versions • Edge (legacy): Windows 10 version 1903 • Chrome: 76 • Firefox: 66
macOS	Safari: macOS 10.15.2
iOS / iPadOS	Safari: iOS 13.3 / iPadOS 13.3

Nymi Band Requirements

Nymi provides you with a Nymi Band in either Standalone Mode or CWP mode. Before a user can use their Nymi Band to perform tasks with their FIDO2 passkeys, the user must enroll to the Nymi Band and register their Nymi Band as a FIDO2 authentication method for the relying party.

Enrollment

Enrollment is the process of associating user 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.

The enrollment process differs for each mode:

- Standalone Mode Nymi Band—Users can immediately enroll their fingerprint to the Nymi Band without the need to access additional applications.
- CWP Mode Nymi Band—Users must access the Nymi Band Application on the Nymi Band Application Terminal to enroll their fingerprint to the Nymi Band. The enrollment process associates the Nymi Band with the identity of the user in Active Directory. The enrollment process stores information about the Nymi Band and the Nymi Band user in the Nymi Enterprise Server(NES) database.

Registration

After the user completes enrollment, the user registers their Nymi Band as a FIDO2 authentication method for the relying party. The registration process is the same for a Standalone Mode Nymi Band and a CWP Mode Nymi Band. The registration process writes information that identifies the Nymi Band to user association in the FIDO2 application and the Nymi Band stores the FIDO2 passkeys.

The registration steps differs depending on the FIDO2 application. You can find more information about the registration in this document, within the applicable FIDO2 application chapter.

Determining the Nymi Band Mode

You can determine the Nymi Band mode by putting the Nymi Band on your wrist and pressing any button. A Standalone Mode Nymi Band displays a fingerprint icon

.

A CWP Mode Nymi Band displays a setup code similar to the following image

.

Enrolling a Standalone Mode Nymi Band

You can use a enrolled Standalone Mode Nymi Band with FIDO2, SEOS and Legic technologies to complete authentication activities with a Nymi Band tap.

About this task

To enroll a Standalone Mode Nymi Band, the user wears the Nymi Band, and then performs the following steps:

Procedure

1. When the **`Fingerprint`** icon to appear on the Nymi Band screen, as shown in the following image, place their finger on the fingerprint sensor and the fingerprint bezel that surrounds the sensor.

   Figure 1: FINGERPRINT
2. When the **`LIFT FINGER`** message appears on the screen, lift their finger from the sensor and bezel.

   When the **`TOUCH SENSOR`** message appears on the screen, place their finger on the sensor and bezel.

   The following figures show the **`LIFT FINGER`** and **`TOUCH SENSOR`** messages.

Figure 2: LIFT FINGER

Figure 3: TOUCH SENSOR

3. Repeat the steps to lift their finger and touch the sensor and bezel, as prompted.

   The fingerprint process evaluates and captures 15 images of the fingerprint, and then performs one of the following actions:

   - If the process determines that the images that were captured are acceptable to create a template, then the Nymi Band creates a securely-stored mathematical template of the image, and then deletes the images.
   - If the process determines that the images that were captured are not acceptable to create a template, then the Nymi Band deletes all images and requires the user to repeat the fingerprint capture process.
   - If the process is unable to create a template after three attempts, the process fails and the Nymi Band displays **See Admin**. In this situation, you must perform a delete user data operation on the Nymi Band and retry the enrollment. The *Nymi Connected Worker Platform—Administration Guide* describes how to perform the delete user data operation.

What to do next

After you enroll your Nymi Band, you must register the Nymi Band

Enrolling a CWP Mode Nymi Band

To enroll a CWP Mode Nymi Band, the user puts on their Nymi Band and logs into the Nymi Band Application on the enrollment terminal with 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 passkeys on the Nymi Band.

Using the Nymi Band to Log Into Web Applications with Microsoft Credentials

User can use the Nymi Band as a security key to sign into web-based application that rely on Microsoft credentials, such as Microsoft Office 365.

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**.
5. Navigate to **Security > Conditional Access > Authentication Strengths**, and then click **New Authentication Strength**, as shown in the following figure.
6. Create a strength with the following attributes:
   a)
7. Edit the Access policy and assign the authentication strength.

Prepare the User Terminal

To reduce the number of clicks that a user requires to log into applications with a Nymi Band tap, optimize the options available on the user terminal.

Options to consider include:

- Limiting the Sign in options
- Disabling security key access from Bluetooth Devices

Reducing the Number of Sign In Options

Perform the following actions on each user terminal to reduce the number of sign in options that are available for a user, which reduces the mouse clicks the user must perform before they can perform authentication operations with the .

About this task

Nymi recommends that you leave only the Security key and at least one other sign in option (Password) available.

Procedure

1. Instruct the user to log into the user terminal.
2. From the Search bar, type ***Sign-in options***, and then click **Open**, as shown in the following figure.

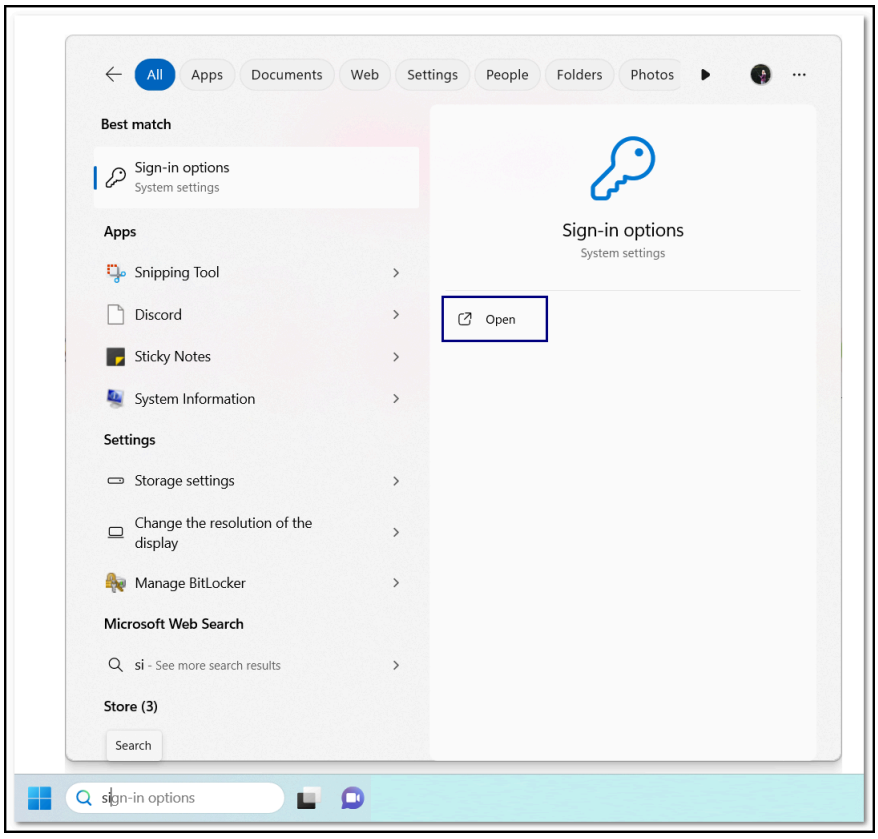


Figure 4: Sign-in Options

3. If the Facial Recognition (Windows Hello) option is configured, click **Remove**, as shown in the following figure.

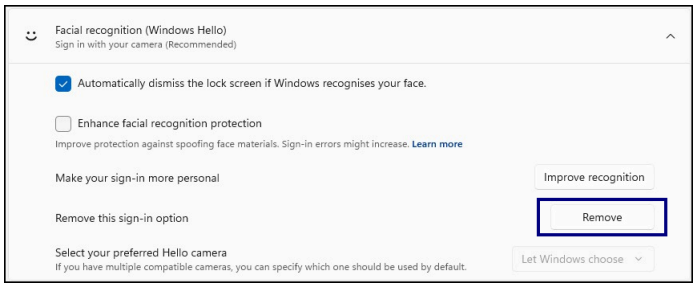


Figure 5: Remove Facial Recognition option

4. Expand the **`Fingerprint Recognition (Windows Hello)`** option. If the option is configured, click **`Remove`**:

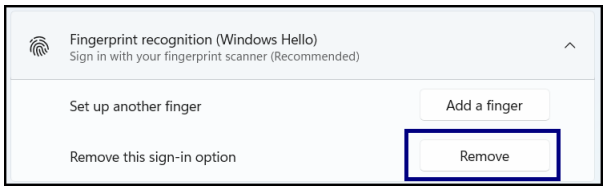


Figure 6: Remove Fingerprint Sign-in Option

5. Expand the **`Pin(Windows Hello)`** option. If the option is configured, perform the following steps:

   a) Click **`I forgot my PIN`**, as shown in the following figure.

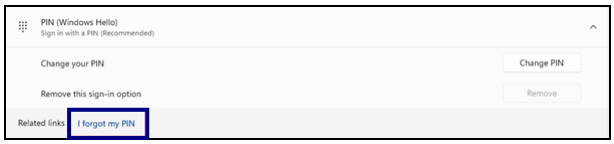


Figure 7: I forgot my PIN option

   b) On the `Are you sure`? window, click **`Continue`**, as shown in the following figure.

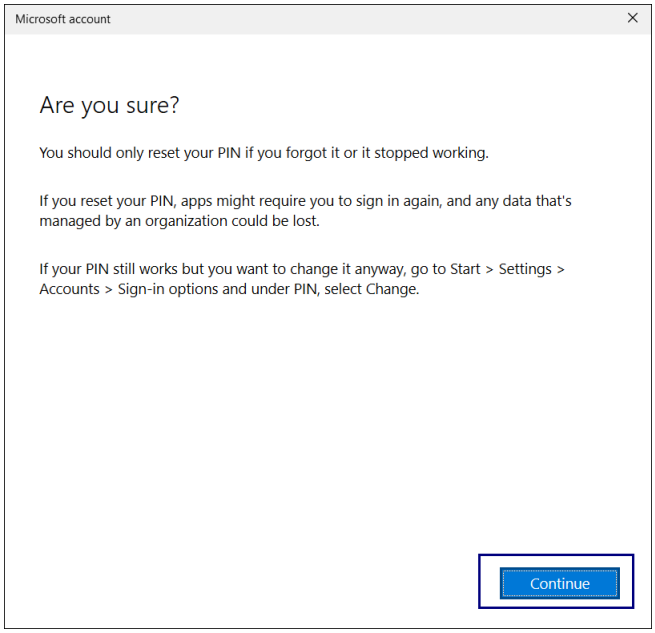


Figure 8: Are you sure window

   c) Click **`Cancel`**, as shown in the following figure.

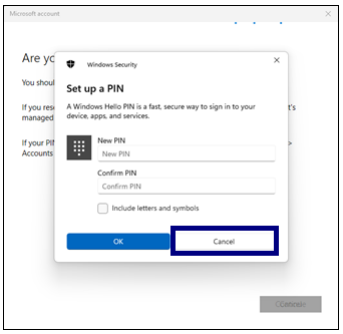


Figure 9: Cancel setup PIN option

d) On the `Did you mean to cancel PIN` window, click **`I'll setup my PIN later`**, as shown in the following figure.

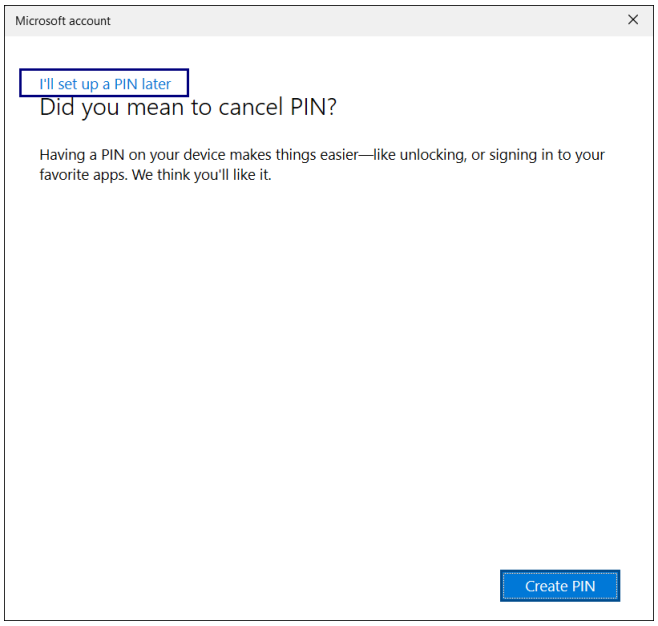
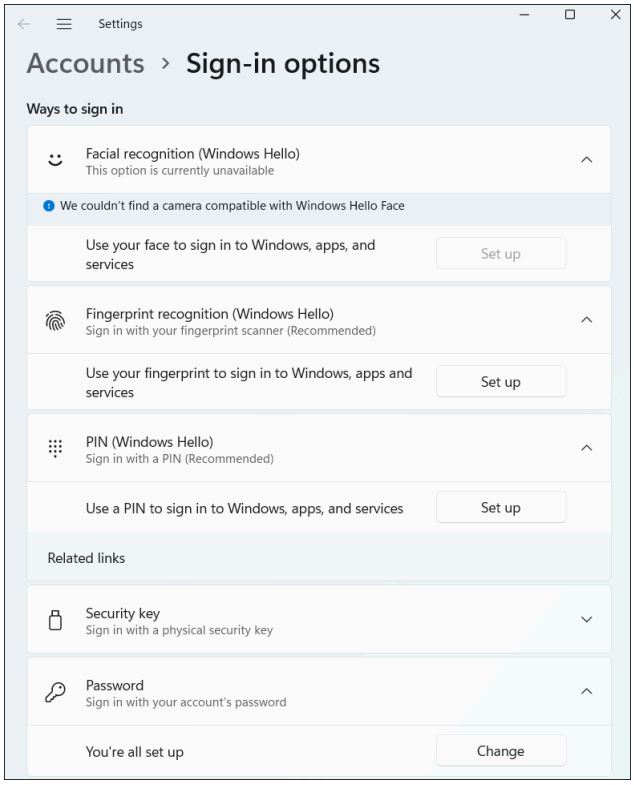


Figure 10: I'll setup my PIN later option

The `Sign in options` window should appear similar to the following:

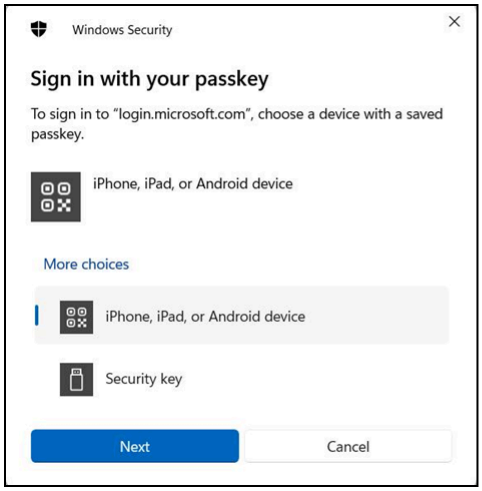


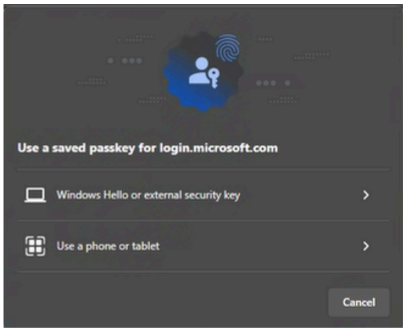
Disabling Security Key Access From Bluetooth Devices

Disable the ability to access a saved passkey from Bluetooth devices such as a tablet, iPad, iPhone, or android device.

About this task

When a user can access a saved passkey from the Bluetooth-enabled device, the user might see one of the following `Sign In windows.`

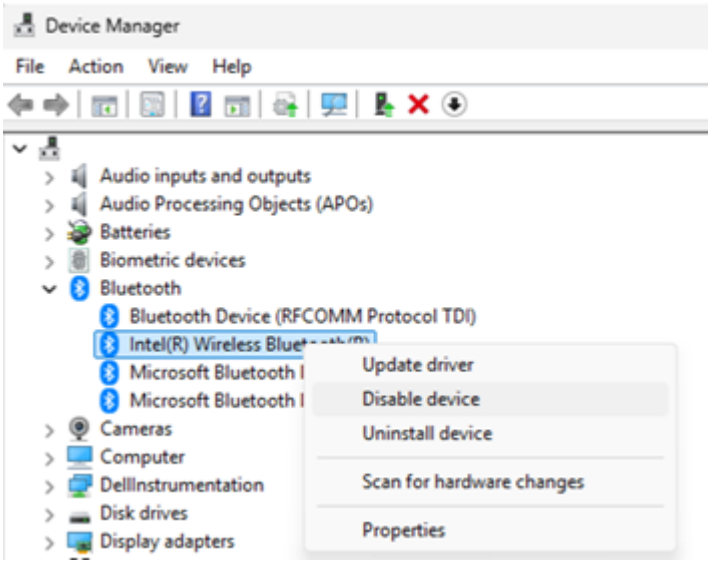




To disable passkey access from Bluetooth-enabled devices, perform the following steps on each user terminal.

Procedure

1. Open `Device Manager`.
2. Expand Bluetooth.
3. Right-click **`Intel(r) Wireless Bluetooth`**, and then select **`Disable device`**, as shown in the following figure.



4. Close `Device Manager`.

Microsoft - 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 user terminal.

Procedure

1. Plug the NFC reader into the user terminal.
2. From a browser log into the `Office 365 login` page, and click to **`View Account`** as shown in the following figure.

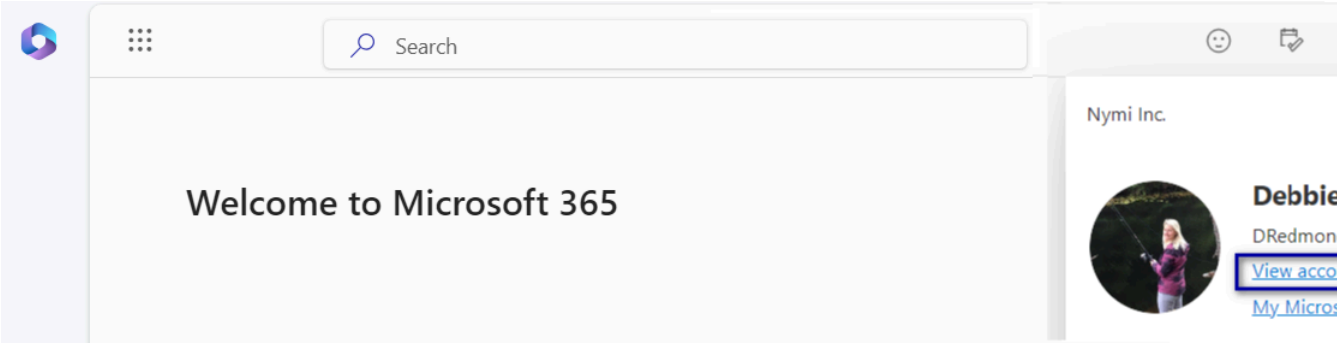


Figure 11: View Account

3. On **`Security Info`**, click **`Update Info`**, as shown in the following figure.

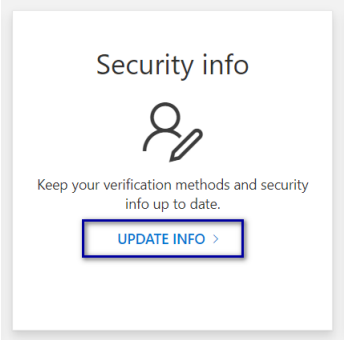


Figure 12: Edit Security Info

4. On the **`Security Info`** window, click **`Add a sign in method`**, as shown in the following figure.

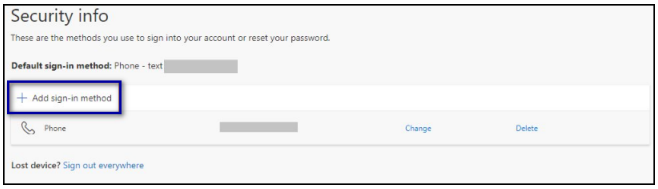


Figure 13: Edit Security Info

5. From the **`Add a method`** list, select **`Security Key`**, as shown in the following figure, and then click **`Add`**.

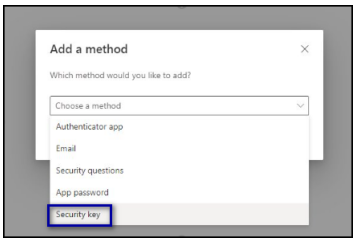


Figure 14: Edit Security Info

6. If the configuration requires multifactor authentication to make changes, on the `Security Key` window, click **`Next`**, as shown in the following figure. Complete your multifactor verification.

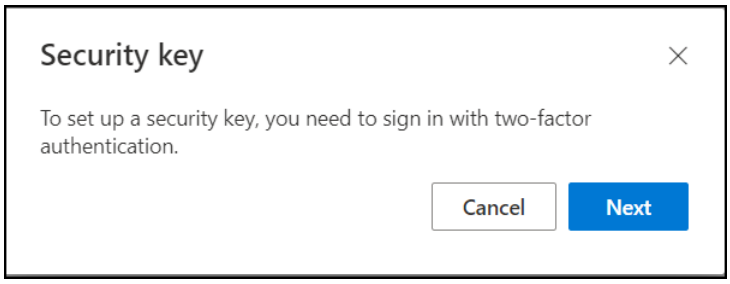


Figure 15: Security Key window

7. From the `Security Key` pop-up, click **`NFC Device`**, as shown in the following figure, and then click **`OK`**.

Figure 16: Security Key

8. On the `Security Key` window, click **`Next`**, as shown in the following figure.

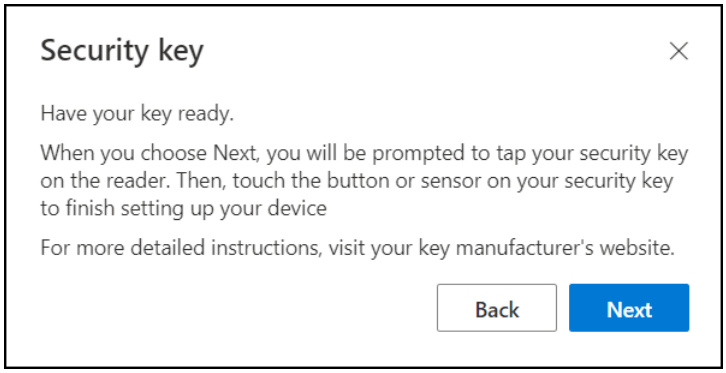


Figure 17: Security Key window - Have your key ready

9. On the `Create a passkey or` pop-up, click **`Use a different device`**, as shown in the following figure, and then click **`OK`**.

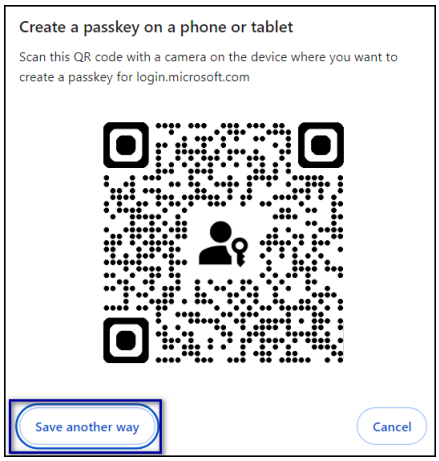


Figure 18: Create a passkey on a phone or tablet

10. On the `Setting up your new sign in method` window, as shown in the following figure, and then click **`Next`**.

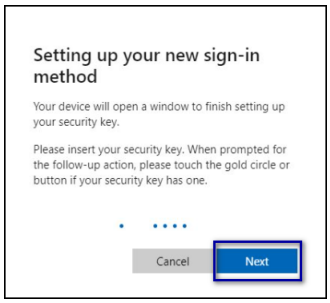


Figure 19: Setting up your new sign in method

11. On the `Choose where to save your passkey` window, click **`Use a phone, tablet, or security key`**, as shown in the following figure.

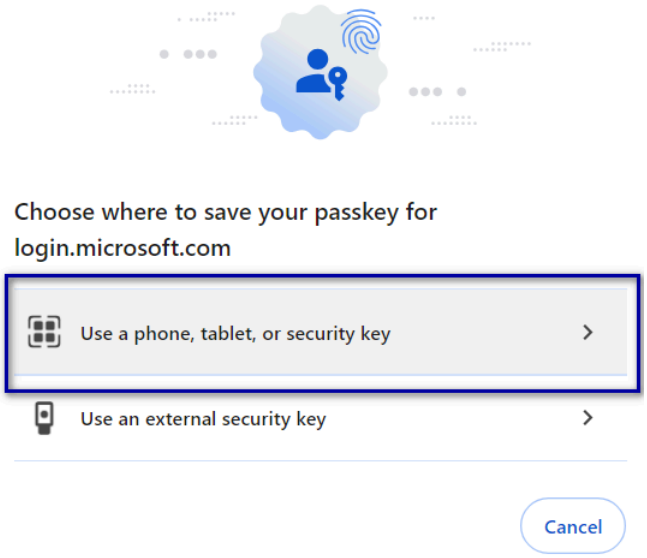


Figure 20: Choose where to save your passkey

12. On the `Create a passkey` window, as shown in the following figure, and then click **`Windows Hello or external security key`**.

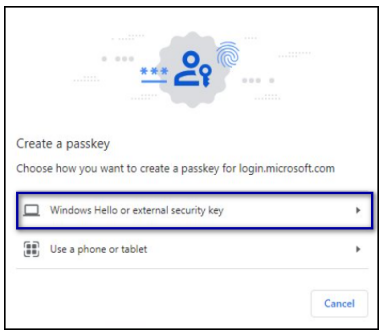


Figure 21: Create a passkey

13. On the `Windows Security` windows that appear, click **`OK`**.
14. On the `Continue setup` window, as shown in the following figure, tap your Nymi Band on the NFC reader.

Figure 22: Continue setup window

Note: You might need to tap and hold theNymi Band on the NFC reader for up to 10 seconds.

15. On the `Enter Password` window, type your password, and then click **`Sign in`**.

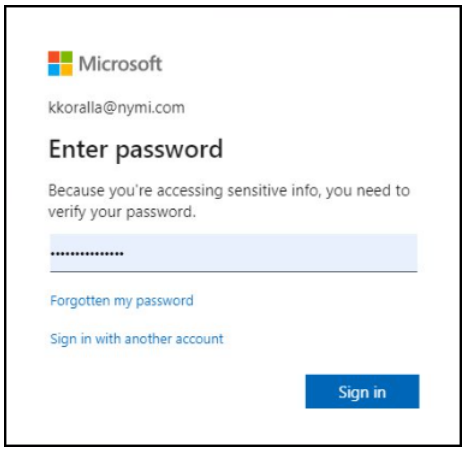


Figure 23: Enter Password window

16. On the `Security Key` page, type identifying name for the Nymi Band, and then click **`Next`**.

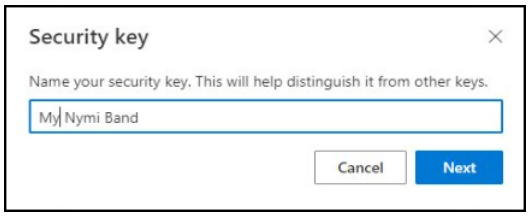


Figure 24: Security Key Identifier

Results

On the Office 365 login window, the Nymi Band identifier appears as a security key in the list of sign in methods.

Logging Into Office 365 with a Nymi Band

You can log into Office 365 with a Nymi Band tap on an NFC reader.

Procedure

1. Plug the NFC reader into the user terminal.
2. On a Windows user terminal, open the browser.
3. Navigate to the Office 365 login page.
4. On the `Sign in` page appears, type your username and then click **`Next`**, as shown in the following figure.

   Note: Some applications use Login Hints to suppress this window. *Application Prompts User for Username* provides more information.

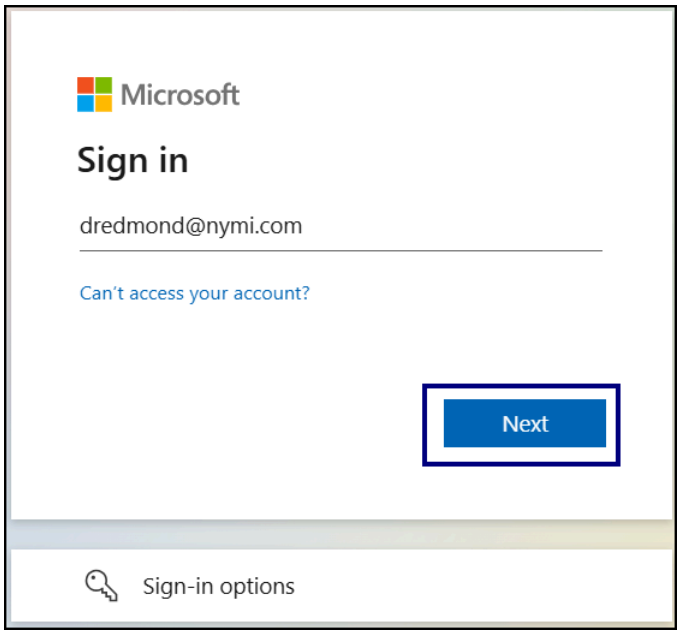


Figure 25: Sign-in options

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

Figure 26: Making sure it's you window

Results

Login succeeds.

Microsoft - Removing the Nymi Band as a Security Key

Perform the following steps to remove the Nymi Band as a security key. For example, when a user re-enrolls their Nymi Band, when you assign a new Nymi band to a user, or you to use the Nymi Band as an authenticator.

Procedure

1. Plug the NFC reader into the user terminal.
2. From a browser log into the `Office 365 login` page, and click to **`View Account`** as shown in the following figure.

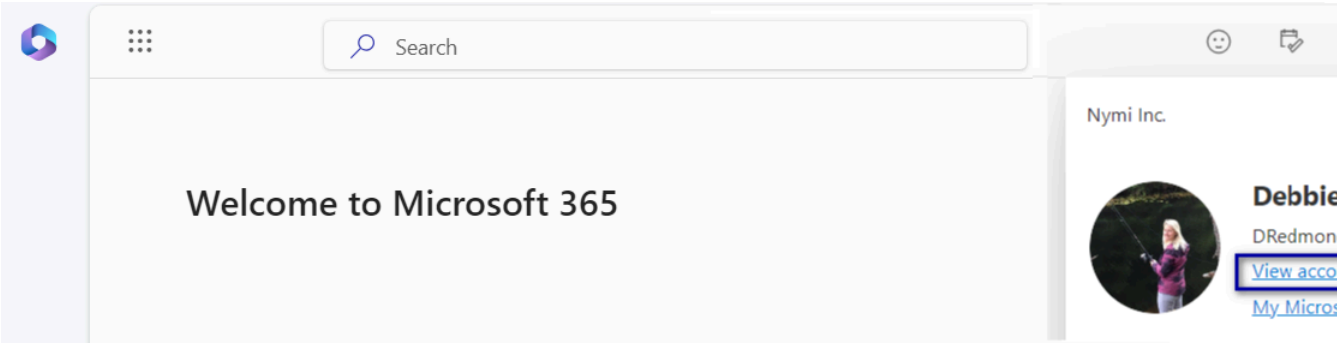


Figure 27: View Account

3. On **`Security Info`**, click **`Update Info`**, as shown in the following figure.

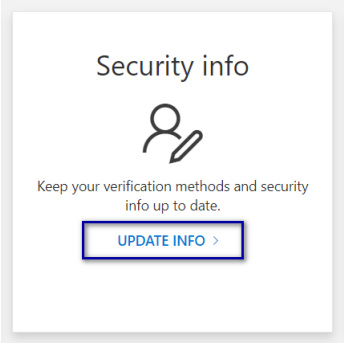


Figure 28: Edit Security Info

4. On the `Security info` window, click **`Delete`** beside the entry for the Nymi Band.

What to do next

After you remove the Nymi Band as a security key, the next steps you take depend on the reason you removed the Nymi Band as a security key and the Nymi Bandmode. The following table provides more information.

Reason	Standalone Nymi Band	CWP Mode Nymi Band
Re-enrollment	Put the Nymi Band on charge and perform the delete user data operation. Instruct the user to enroll their Nymi Band. The section *Enrollment of a Standalone Mode Nymi Band* provides mode information.	Put the Nymi Band on charge and perform the delete user data operation, and then remove the Nymi Band to user association in Nymi Enterprise Server(NES). Instruct the user to access the Nymi Band Application Terminal, and then perform an enrollment. **Note:** In Connected Worker Platform(CWP) 1.16.0 and later you can configure self-service enrollment. The *Nymi Connected Worker Platform—Administration Guide* provides more information about the enrollment and self-service re-enrollment processes.
Assign the Nymi Band to a new user	Put the Nymi Band on charge and perform the delete user data operation. Instruct the new user to enroll the Nymi Band. The section *Enrollment of a Standalone Mode Nymi Band* provides mode information.	Put the Nymi Band on charge, perform the delete user data operation, and then remove the Nymi Band to user association in NES. Instruct the user to access the Nymi Band Application Terminal, and then perform an enrollment. **Note:** In CWP 1.16.0 and later you can configure self-service enrollment. The *Nymi Connected Worker Platform—Administration Guide* provides more information about the enrollment and self-service re-enrollment processes.
Discontinue the use of this Nymi Band as an authenticator.	Put the Nymi Band on charge and perform the delete user data operation.	Put the Nymi Band on charge, perform the delete user data operation, and then remove the Nymi Band to user association in NES. The *Nymi Connected Worker Platform—Administration Guide* provides more information.

Using the Nymi Band to Log into Windows Desktop

User can use the Nymi Band as a security key to sign into a Microsoft Account on a computer that is running Windows 11 or Windows 10 (version 1903 or higher) by performing an NFC tap with their authenticated Nymi Band on the Microsoft Azure login screen.

Pre-requisites for Hybrid Azure Active Directory

You can use the Nymi Band in a Hybrid Azure Active Directory(AAD) environment.

Review the following requirements for Hybrid AAD.

- Windows 10 User terminals must run version 2004 or later.
- Windows Domain controllers with the following patches:
  - Windows 2016—KB4534307
  - Windows 2019—KB4534321
  - Domain controllers with AES_256_HMAC_SHA1 encryption enabled when you enable the `Network Security: Configure encryption types allowed for Kerberos` policy.
  - Active Directory server that you synchronize to Microsoft Entra ID by using Microsoft Entra Connect.
  - User account that have the following Microsoft Entra attributes,which you populate through Microsoft Entra Connect:
    - onPremisesSamAccountName (accountName in Microsoft Entra Connect)
    - onPremisesDomainName (DomainFQDN in Microsoft Entra Connect)
    - onPremisesSecurityIdentifier (objectSID in Microsoft Entra Connect)

(Hybrid Azure only) Enabling Security Key Login on Devices

In an Hybrid Azure environment, you must enable security key login on user terminals.

Perform one of the following actions to enable security key login on the user terminals:

- Perform the following steps on each user terminal to create the registry key:

  1. Navigate to **`HKLM > Software > Policies > Microsoft > FIDO`**
  2. Create a new DWORD (32 bit) value named ***enableFIDODeviceLogin***
  3. Set the value to ***1***.
- Use Group Policy Objects(GPO) to push the changes to each user terminal. The following table summarizes the policy settings:

Group Policy Path	Group Policy Setting	Value
`Computer Configuration > Administrative Templates > Windows Components > Windows Hello for Business` or **`User Configuration > Administrative Templates > Windows Components > Windows Hello for Business`**	Use Windows Hello for Business	Enabled
`Computer Configuration > Administrative Templates > Windows Components > Windows Hello for Business`	Use cloud Kerberos trust for on-premises authentication	Enabled
`Computer Configuration > Administrative Templates > Windows Components > Windows Hello for Business`	Use a hardware security device	Enabled

You can

To create registry key on each user

Enabling a FIDO2 Credentials In Azure Active Directory

Procedure

1. Log into `Microsoft Entra`.

2. Navigate to **`Security > Authentication Methods > Policies`**.
3. From the **`Methods`** list, click **`FIDO2 security key`**, as shown in the following figure.

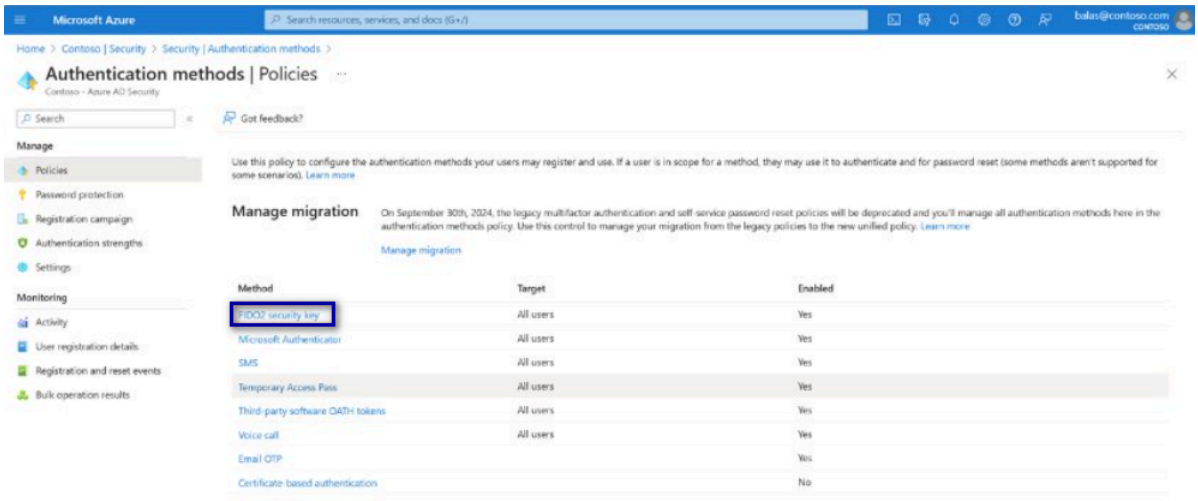


Figure 29: FIDO2 security key

4. On the **`FIDO Security Keys`** window, toggle the switch to **`Enable`**, as shown in the following figure.

Figure 30: Enable FIDO2

5. On the **`Config`** tab, configure FIDO2 security key method settings, as required.

Microsoft - 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 user terminal.

Procedure

1. Plug the NFC reader into the user terminal.
2. From a browser log into the `Office 365 login` page, and click to **`View Account`** as shown in the following figure.

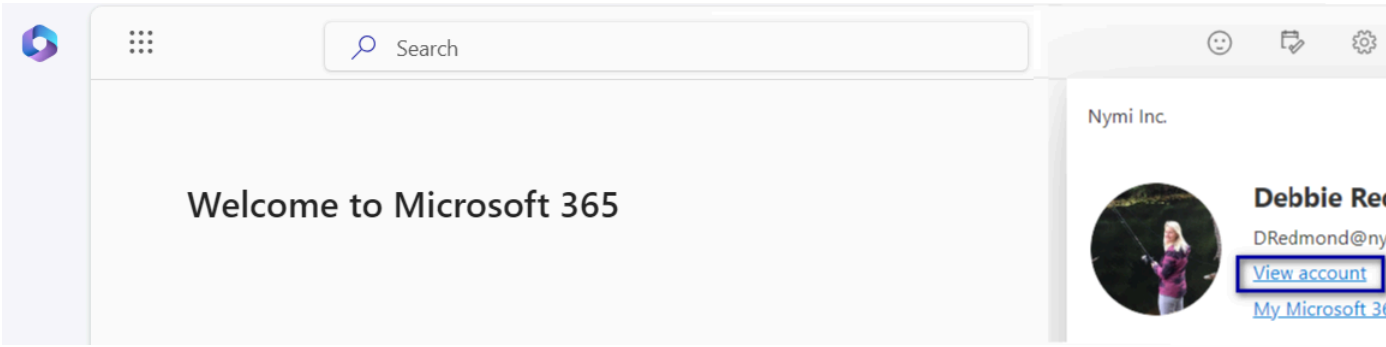


Figure 31: View Account

3. On **`Security Info`**, click **`Update Info`**, as shown in the following figure.

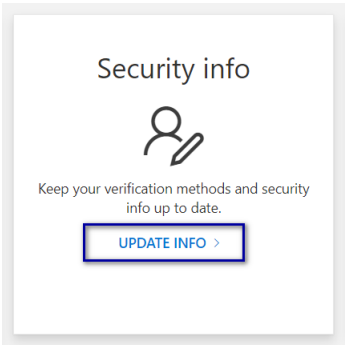


Figure 32: Edit Security Info

4. On the **`Security Info`** window, click **`Add a sign in method`**, as shown in the following figure.

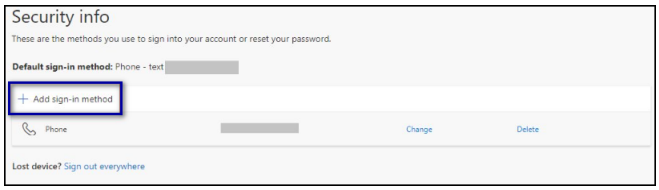


Figure 33: Edit Security Info

5. From the **`Add a method`** list, select **`Security Key`**, as shown in the following figure, and then click **`Add`**.

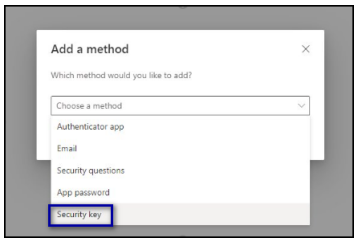


Figure 34: Edit Security Info

6. If the configuration requires multifactor authentication to make changes, on the `Security Key` window, click **`Next`**, as shown in the following figure. Complete your multifactor verification.

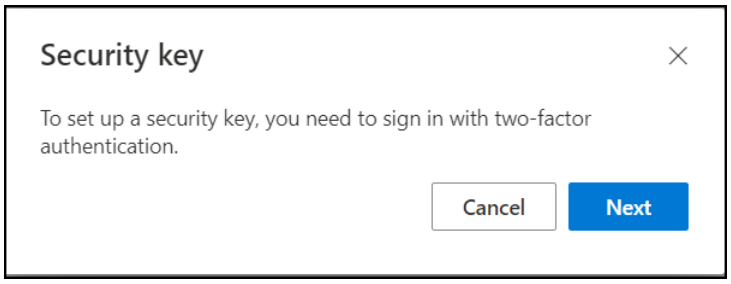


Figure 35: Security Key window

7. From the `Security Key` pop-up, click **`NFC Device`**, as shown in the following figure, and then click **`OK`**.

Figure 36: Security Key

8. On the `Security Key` window, click **`Next`**, as shown in the following figure.

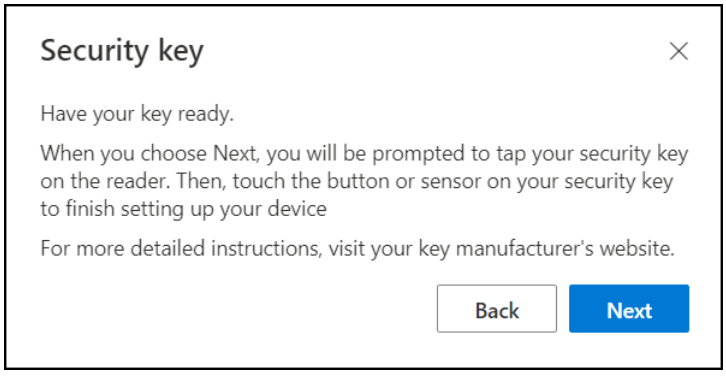


Figure 37: Security Key window - Have your key ready

9. On the `Create a passkey or` pop-up, click **`Use a different device`**, as shown in the following figure, and then click **`OK`**.

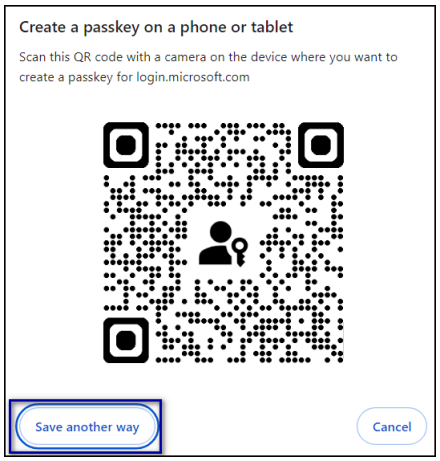


Figure 38: Create a passkey on a phone or tablet

10. On the `Setting up your new sign in method` window, as shown in the following figure, and then click **`Next`**.

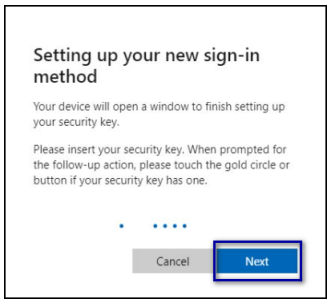


Figure 39: Setting up your new sign in method

11. On the `Choose where to save your passkey` window, click **`Use a phone, tablet, or security key`**, as shown in the following figure.

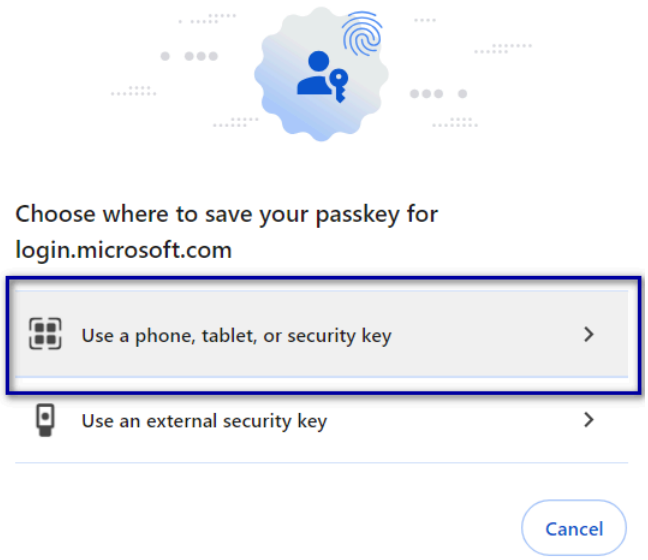


Figure 40: Choose where to save your passkey

12. On the `Create a passkey` window, as shown in the following figure, and then click **`Windows Hello or external security key`**.

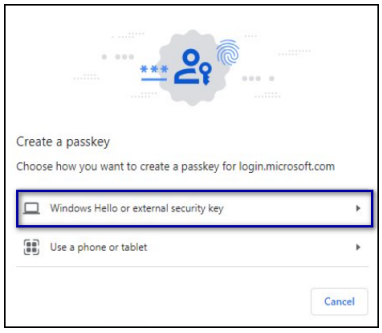


Figure 41: Create a passkey

13. On the `Windows Security` windows that appear, click **`OK`**.
14. On the `Continue setup` window, as shown in the following figure, tap your Nymi Band on the NFC reader.

Figure 42: Continue setup window

Note: You might need to tap and hold theNymi Band on the NFC reader for up to 10 seconds.

15. On the `Enter Password` window, type your password, and then click **`Sign in`**.

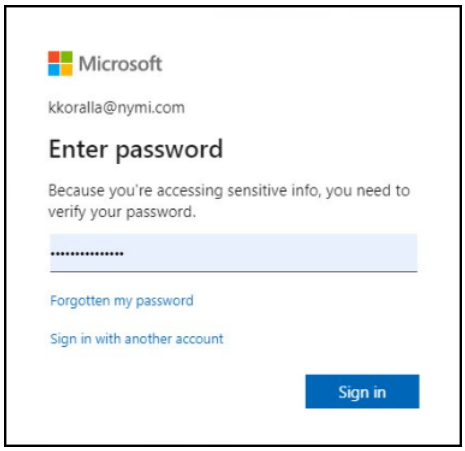


Figure 43: Enter Password window

16. On the `Security Key` page, type identifying name for the Nymi Band, and then click **`Next`**.

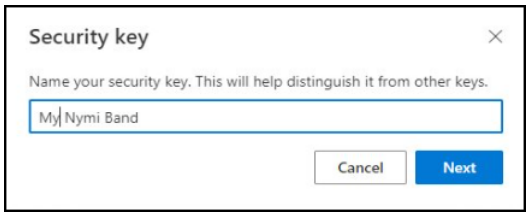


Figure 44: Security Key Identifier

Results

On the Office 365 login window, the Nymi Band identifier appears as a security key in the list of sign in methods.

Joining User Terminals to the Azure Active Directory

Perform the following steps to add each user terminal to the Azure Active Directory(AAD)

About this task

To complete these step, you must log into the user terminal with account that an local administrator privileges.

Procedure

1. From `Windows Settings`, click **`Accounts`**, as shown in the following figure.

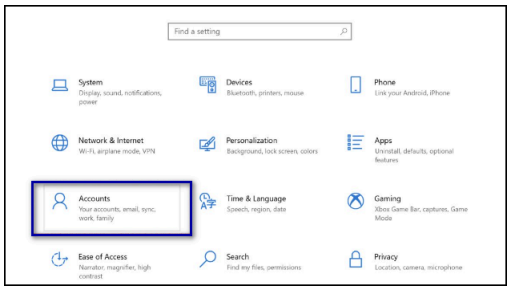


Figure 45: Accounts option

2. In the left navigation pane, select **`Access work or school`**, as shown in the following figure.

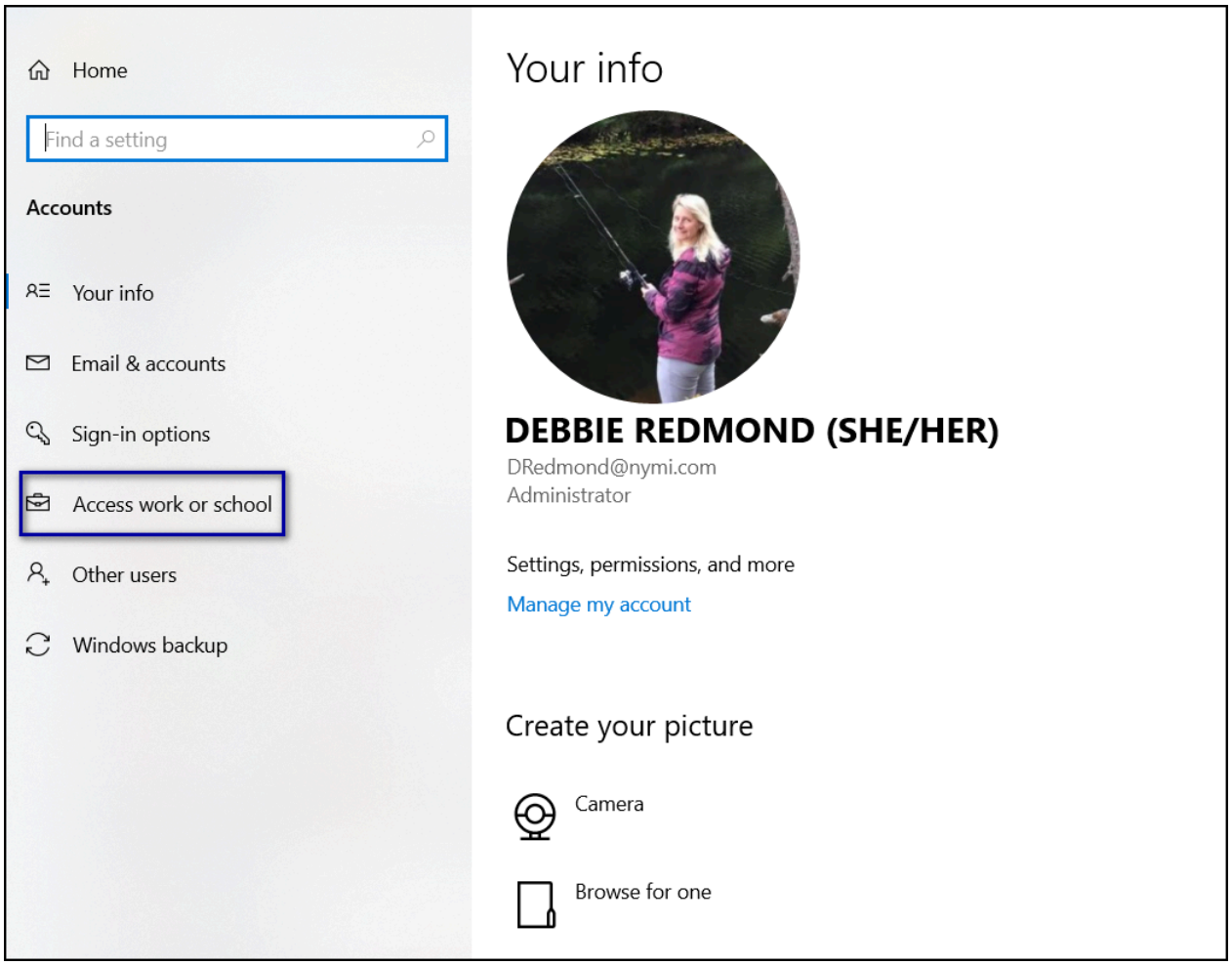


Figure 46: Access work or school option

3. On the window, click Connect, as shown in the following figure.

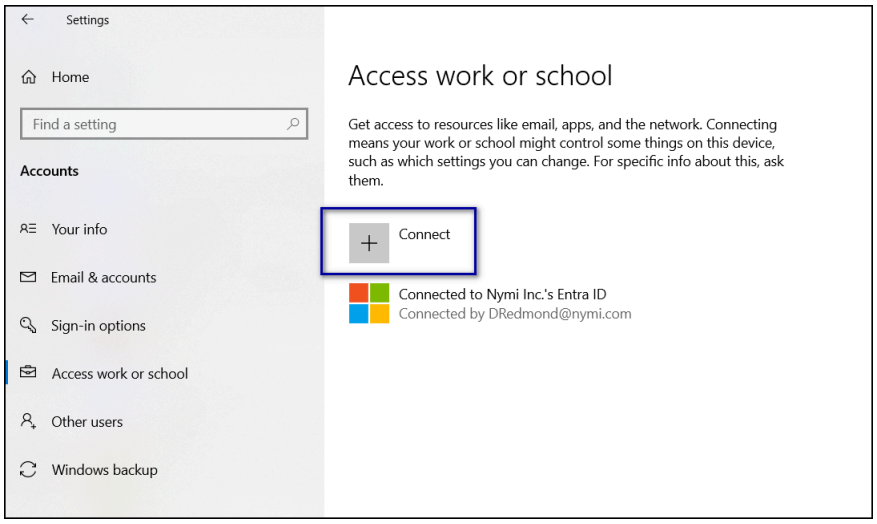


Figure 47: Access work or school option

4. On the `Microsoft Account` window, click **`Join this device to Azure Active Directory`** , as shown in the following figure.

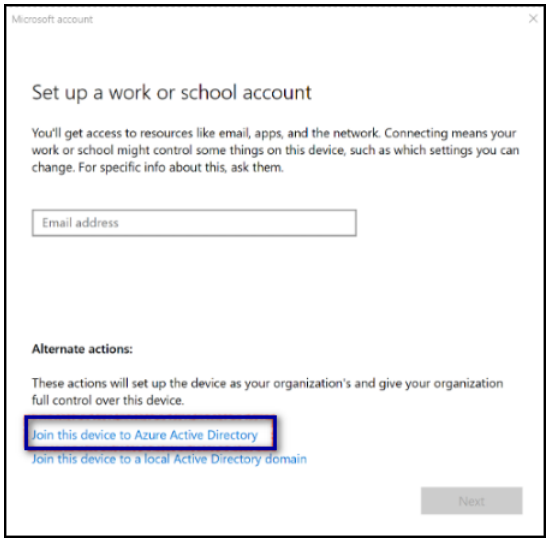


Figure 48: Join this device to Azure Active Directory

5. Sign into your account.
6. On the `Make sure this is your organization` window, click **`Join`**, as shown in the following figure.

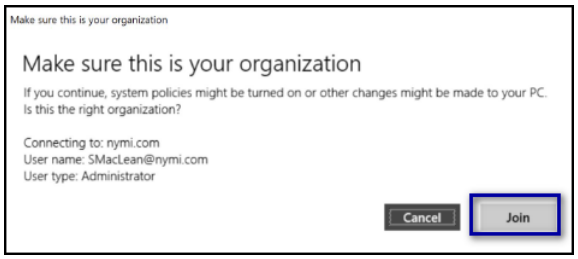


Figure 49: Make sure this is your organization

7. On the click **Done**, as shown in the following figure.

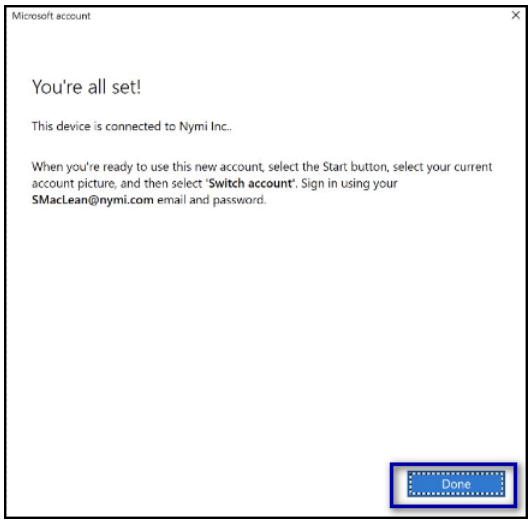


Figure 50: Make sure this is your organization

(Hybrid Azure only) Installing the AzureADHybridAuthenticationManagement Module

If you have an on-prem Active Directory(AD) that is joined with Azure AD, you must ensure that your configuration uses TLS 1.2 and you must install install the `AzureADHybridAuthenticationManagement` module.

About this task

Review https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-passwordless-security-key-on-premises for more information.

Perform the following steps on any domain connected computer.

Procedure

1. Open `Powershell` as an administrator.
2. Type the following command to ensure that the user terminal uses TLS 1.2

   [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12;
3. Type the following command to install the `AzureADHybridAuthenticationManagement` module.

   Install-Module -Name AzureADHybridAuthenticationManagement -AllowClobber
4. Perform the following steps to create a new Microsoft Entra Kerberos server object both in your on-premises Active Directory domain and in your Microsoft Entra tenant
   a) Type the following command to specify an on premise user domain:

      $domain = $env:USERDNSDOMAIN
   b) Type the following command to define the UPN of a Azure Active Directory global administrator

      $userPrincipalName = "`admin_upn`"

      where *`admin_upn`* is the UPN of your domain global administrator account.
   c) Type the following command, and on the pop-up that appears type the username and password of a domain administrator account.

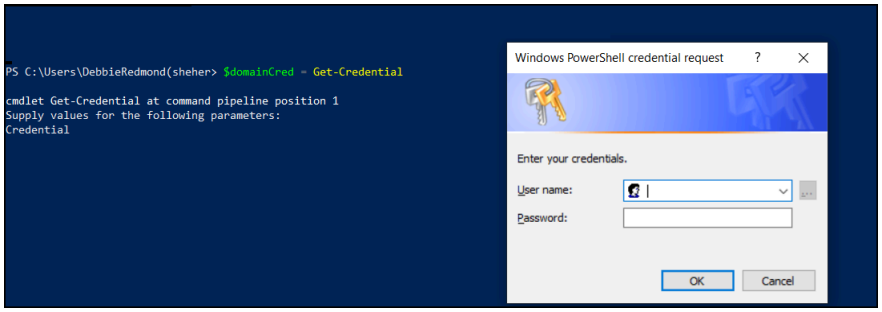


Figure 51: Domain Administrator Credentials

   d) Type the following command create the new Azure AD Kerberos Server object in Active Directory,and then publish the object to the Azure AD.

      Set-AzureADKerberosServer -Domain $domain -UserPrincipalName $userPrincipalName -DomainCredential $domainCred

Logging in to Windows Desktop with a Nymi Band

After you configure the Azure environment to allow users to use their Nymi Band as a security key in Azure Active Directory, the Windows login screen prompts the user to tap the security key to log into the desktop, as shown in the following figure.

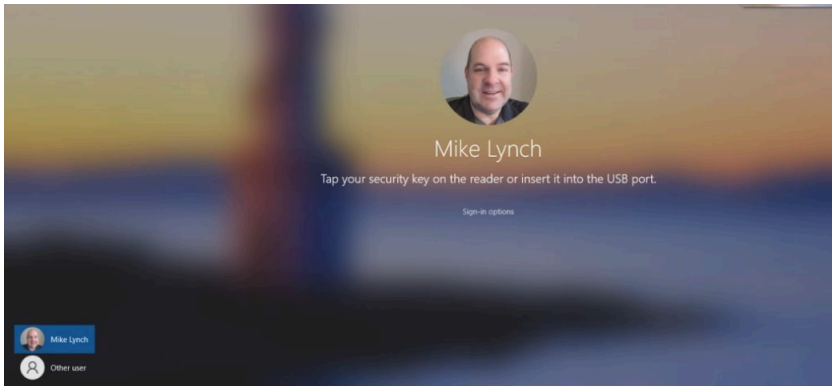


Figure 52: Windows Login screen

If you do not see this screen, perform the following steps:

1. On the `Login` screen, click **`Sign-in options`**, as shown in the following figure.

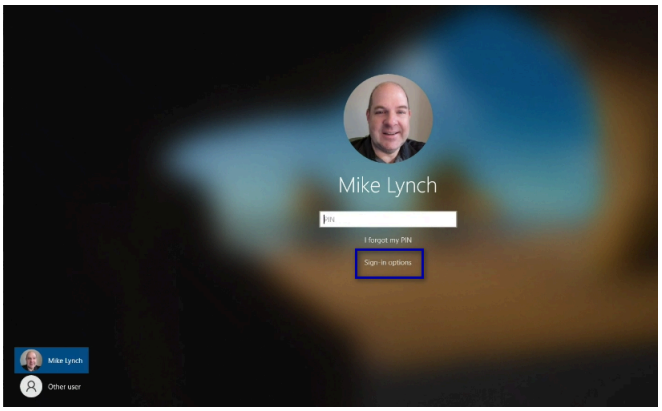


Figure 53: Sign-in options

2. Click the security key icon, as shown in the following figure.

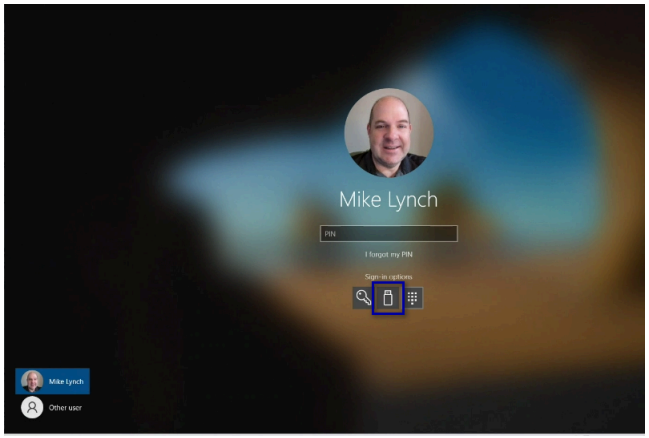


Figure 54: Sign-in options

Microsoft - Removing the Nymi Band as a Security Key

Perform the following steps to remove the Nymi Band as a security key. For example, when a user re-enrolls their Nymi Band, when you assign a new Nymi band to a user, or you to use the Nymi Band as an authenticator.

Procedure

1. Plug the NFC reader into the user terminal.
2. From a browser log into the `Office 365 login` page, and click to **`View Account`** as shown in the following figure.

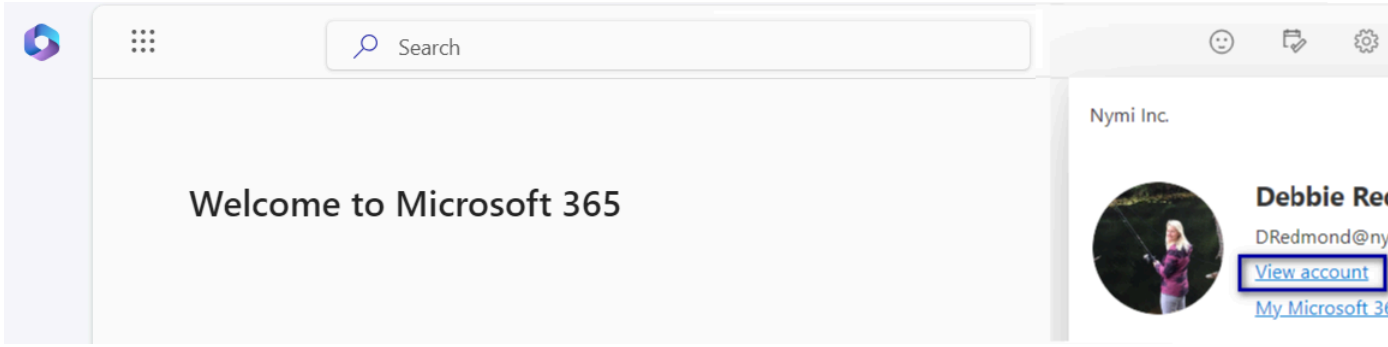


Figure 55: View Account

3. On **`Security Info`**, click **`Update Info`**, as shown in the following figure.

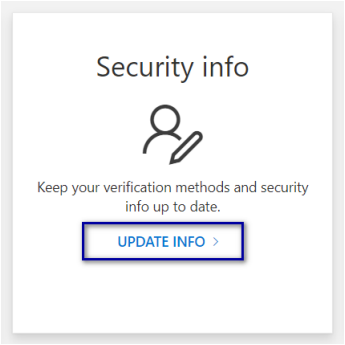


Figure 56: Edit Security Info

4. On the `Security info` window, click **`Delete`** beside the entry for the Nymi Band.

What to do next

After you remove the Nymi Band as a security key, the next steps you take depend on the reason you removed the Nymi Band as a security key and the Nymi Bandmode. The following table provides more information.

Reason	Standalone Nymi Band	CWP Mode Nymi Band
Re-enrollment	Put the Nymi Band on charge and perform the delete user data operation. Instruct the user to enroll their Nymi Band. The section *Enrollment of a Standalone Mode Nymi Band* provides mode information.	Put the Nymi Band on charge and perform the delete user data operation, and then remove the Nymi Band to user association in Nymi Enterprise Server(NES). Instruct the user to access the Nymi Band Application Terminal, and then perform an enrollment. **Note:** In Connected Worker Platform(CWP) 1.16.0 and later you can configure self-service enrollment. The *Nymi Connected Worker Platform—Administration Guide* provides more information about the enrollment and self-service re-enrollment processes.

Reason	Standalone Nymi Band	CWP Mode Nymi Band
Assign the Nymi Band to a new user	Put the Nymi Band on charge and perform the delete user data operation. Instruct the new user to enroll the Nymi Band. The section *Enrollment of a Standalone Mode Nymi Band* provides mode information.	Put the Nymi Band on charge, perform the delete user data operation, and then remove the Nymi Band to user association in NES. Instruct the user to access the Nymi Band Application Terminal, and then perform an enrollment. **Note:** In CWP 1.16.0 and later you can configure self-service enrollment. The *Nymi Connected Worker Platform—Administration Guide* provides more information about the enrollment and self-service re-enrollment processes.
Discontinue the use of this Nymi Band as an authenticator.	Put the Nymi Band on charge and perform the delete user data operation.	Put the Nymi Band on charge, perform the delete user data operation, and then remove the Nymi Band to user association in NES. The *Nymi Connected Worker Platform—Administration Guide* provides more information.

Using the Nymi Band with Okta

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

Before you users can register the Nymi Band as a FIDO2 token, you must perform the following actions:

- Create user groups
- Assign users to the 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 with Okta Identity Engine(OIE). When there are major differences between steps in OIE and Okta Classic, they will be called out.

Creating an Okta User group

Perform the following steps in the Okta Admin Dashboard.

About this task

Procedure

1. From the left navigation pane, select **`Directory > Groups`**, and then click **`Add Group`**, as shown in the following figure.

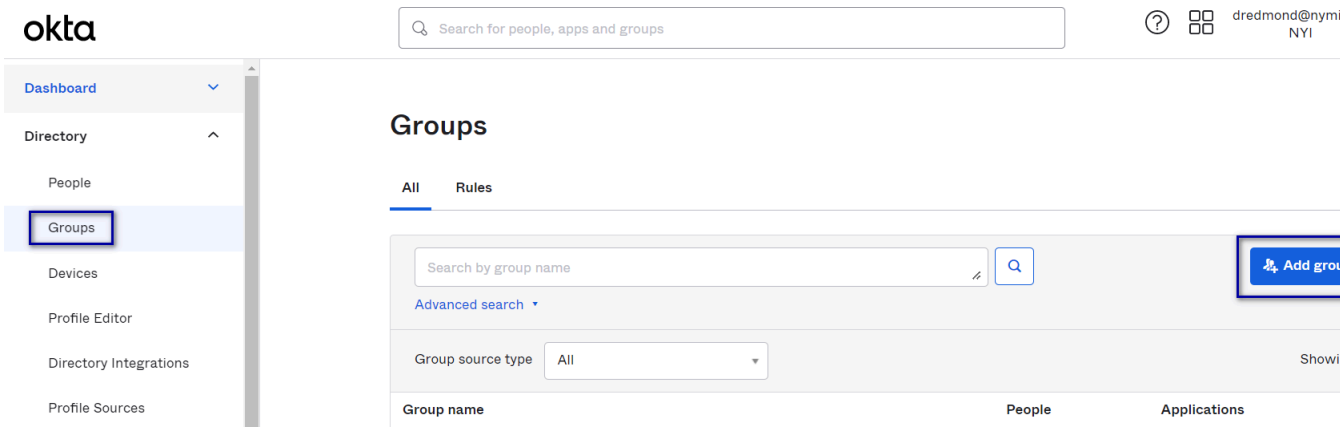


Figure 57: Add group button

2. Name the group and provide a short meaningful description, and then click **Save**, as shown in the following figure.

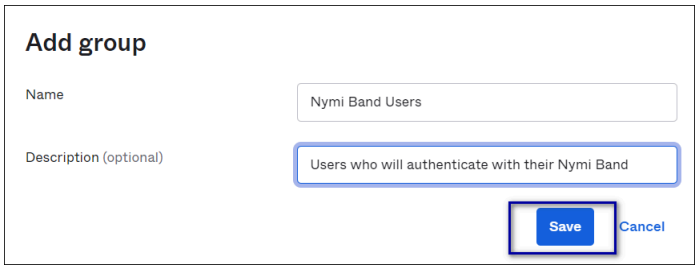


Figure 58: Add group window

Adding Users to the Group

Add users that use a Nymi Band for authentication to the new Okta group.

About this task

Perform the following steps in the Okta Admin Console.

Procedure

1. From the list of groups, select your newly created group.
2. Click **`Assign People`**, as shown in the following figure.

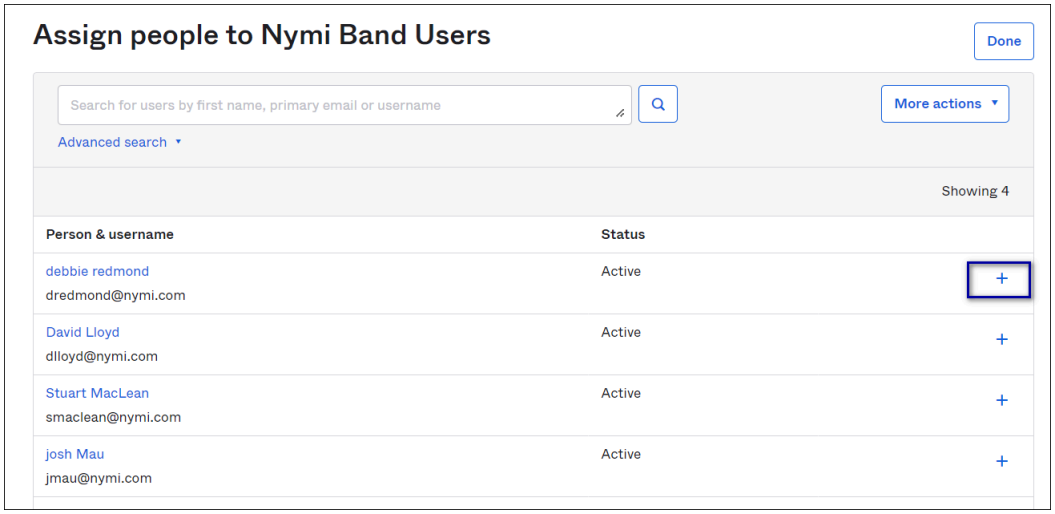


Figure 59: Assign People option

3. From the list of users, click the **+** symbol to the right of 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.

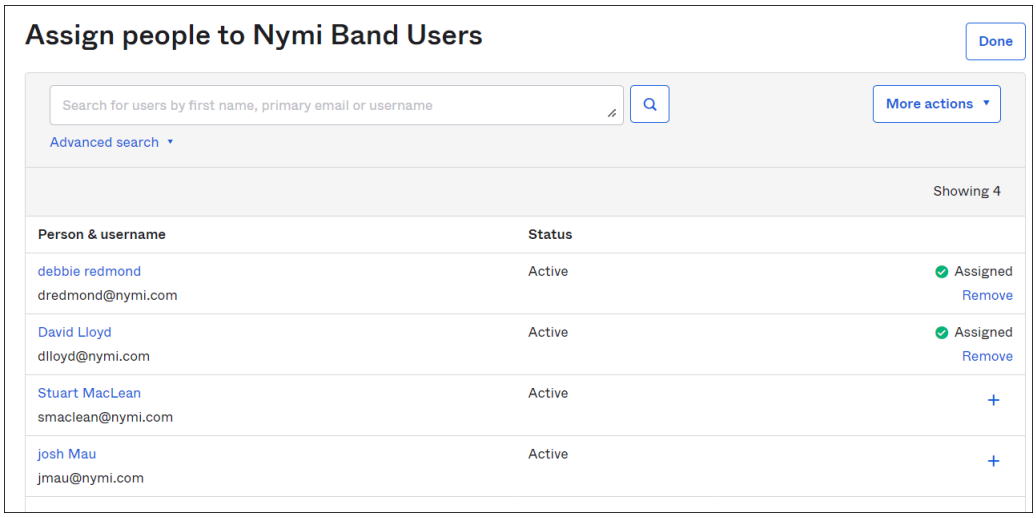


Figure 60: Adding Users to Okta Group

4. Click **Done**.
   The `Group` page displays the group with the included members.

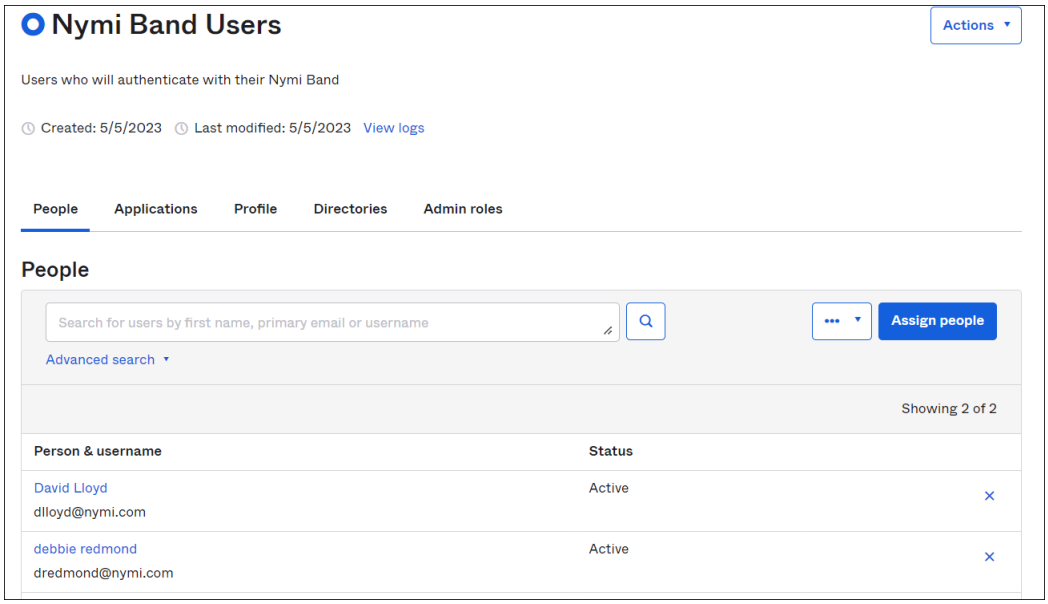


Figure 61: Viewing Users in Okta Group

(Okta Classic only) Configuring Multifactor Authentication and Policy

Multifactor Authentication(MFA) enables 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.

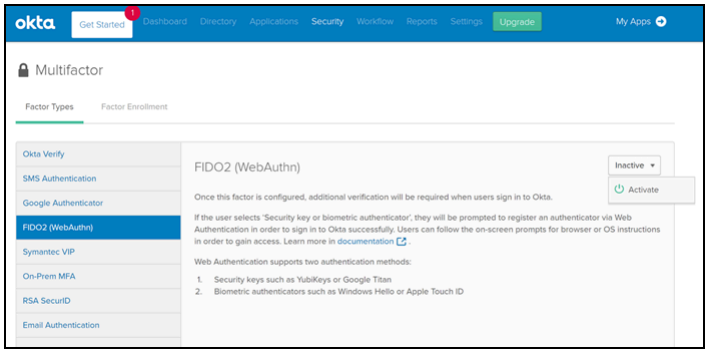


Figure 62: Activating FIDO2 in Okta

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.

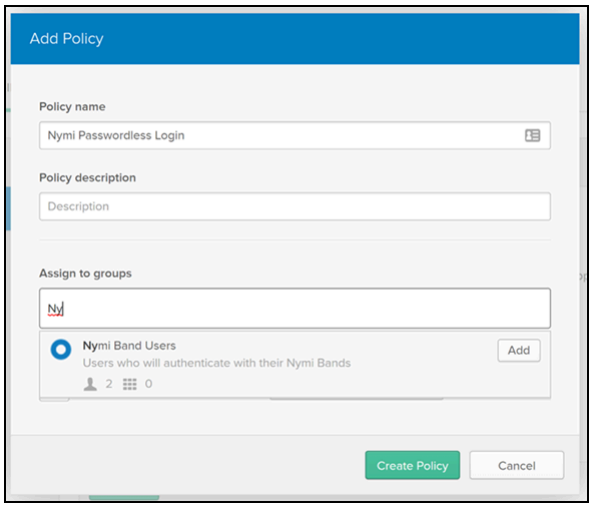


Figure 63: Assign to groups window

   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**.

(OIE only) Adding an Authenticator and Policy

FIDO2(Webauthn) enables users to use their Nymi Band with Okta.

About this task

Add a the FIDO2 Authenticator to Okta, and then create a policy that allows use to use a FIDO2 Authenticator (the Nymi Band) for authentication.

Procedure

1. In the left navigation pane, expand **Security > Authenticators**, and then click **Add Authenticator**, as shown in the following figure.

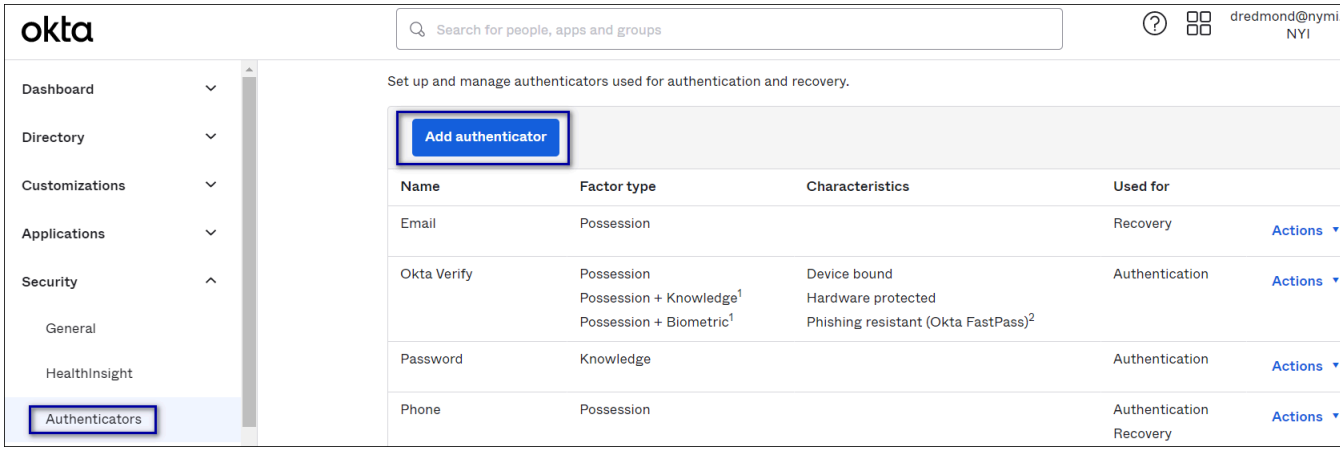


Figure 64: Add Authenticator button

2. On the **Add Authenticator** window, click **Add** under **FIDO2 (WebAuthn)**, as shown in the following figure.

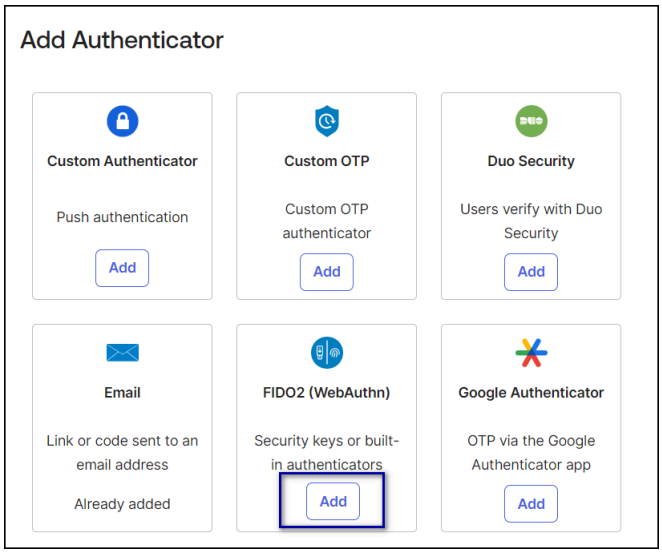


Figure 65: Add FIDO2(WebAuthn)

3. Configure the appropriate **`User verification`**, and then click **`Add`**.
4. Navigate to **`Security > Authentication Policies`**, and then click Add Policy.
5. 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.
   The following figure provides an example of the `Add Policy` window.

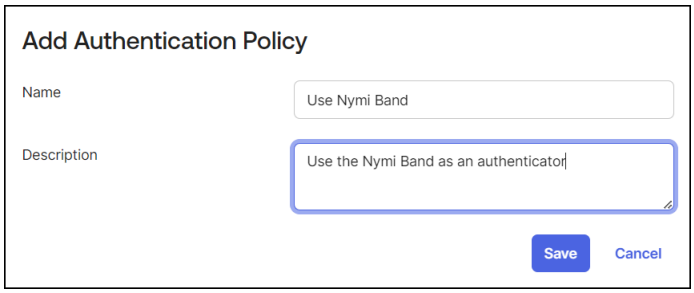


Figure 66: Assign to groups window

6. Optionally, in the `Rules` view, click **`Add rule`**, and then configure the rules, as required.
   The following figure shows the Add rule option.

Figure 67: Add rule

7. On the **`Applications`** tab, click **`Add App`**.
8. On the `Add Apps to this policy` window, search for the application in which users will use the Nymi Band for authentication, and click **Add** beside the each application name, and then click **Done**.

Okta - Registering the Nymi Band as a Security Key

After an administrator configures 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 a 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.

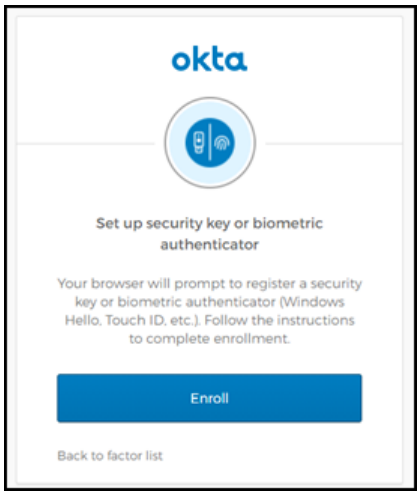


Figure 68: Okta Enroll window

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

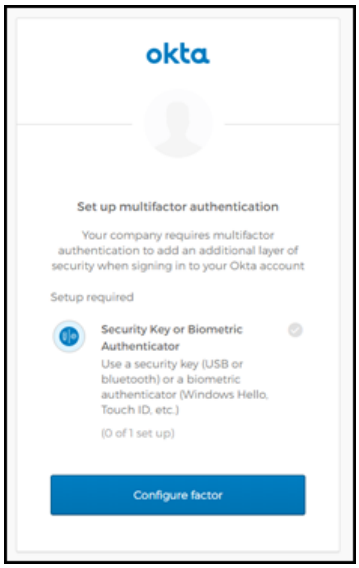


Figure 69: Set up Multifactor window

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.

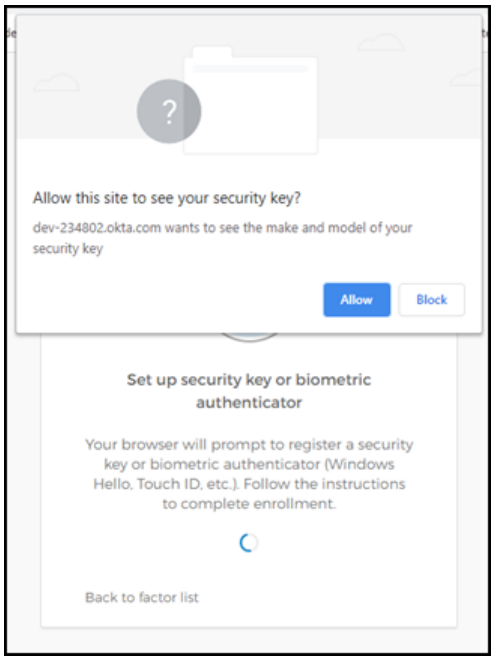


Figure 70: Allow this site to see your security key

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

Figure 71: Okta Sign In window

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

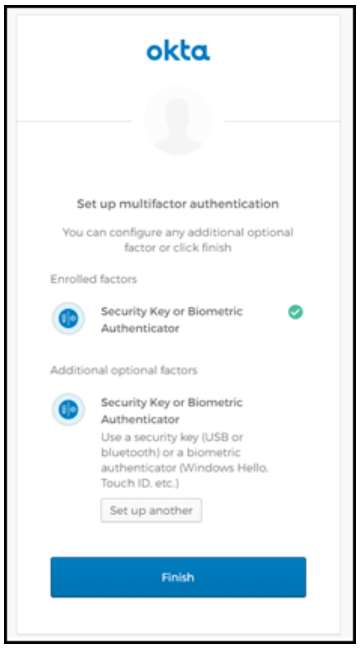


Figure 72: Set up Multifactor window

Results

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

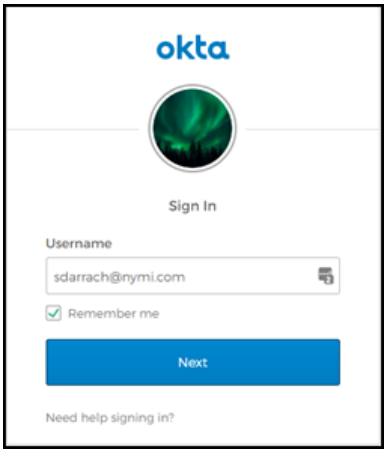


Figure 73: Okta Sign In windows

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.

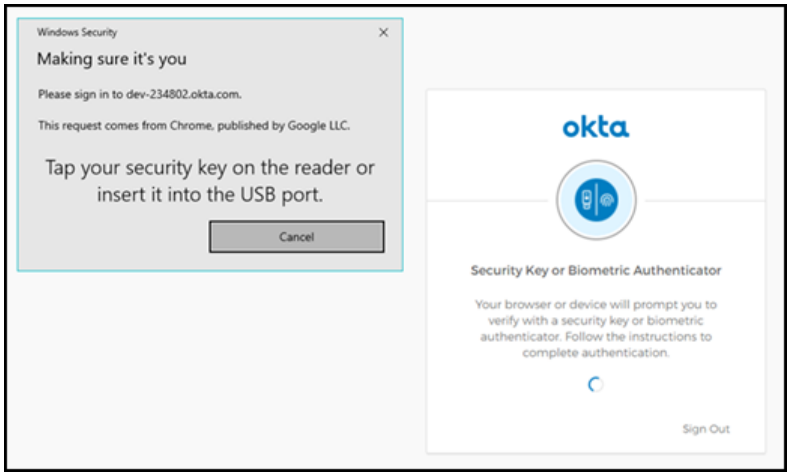


Figure 74: Making sure it's you window

Okta - Logging in with a Nymi Band

About this task

Perform the following steps on a Windows user terminal while you wear your authenticated Nymi Band.

Procedure

1. Open a browser and navigate to the `Okta login` page.
2. Click **`Sign in with Okta FastPass`**.
   The `Verifying your Identity` window appears
3. When the `Making sure its you` window appears, tap your Nymi Band on the NFC reader.
4. On the `Enter Password` window, click **`Sign in with a security key`**, as shown in the following figure.

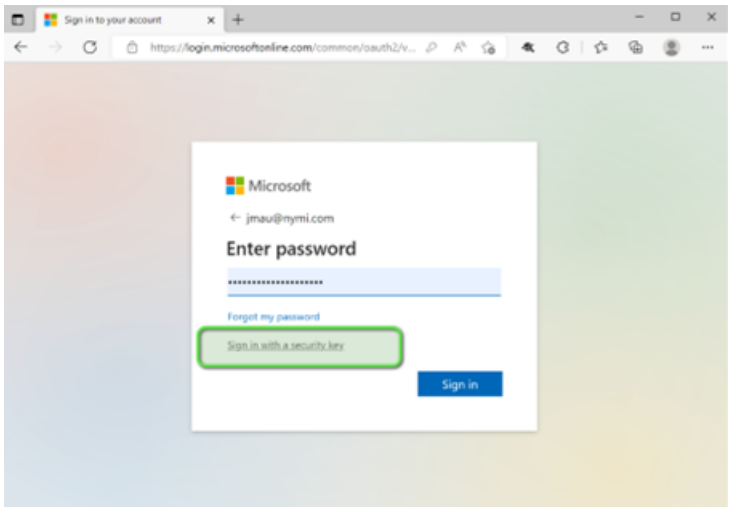


Figure 75: Enter Password window

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

   The following figure provides an example of the window.

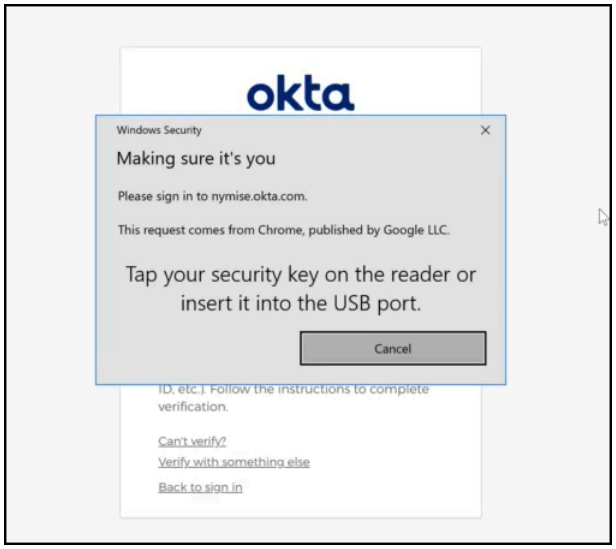


Figure 76: Making sure it's you window

Results

Log in succeeds.

(Okta Classic only) Removing Multifactor 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.

Procedure

1. Log into the `Okta Admin Dashboard` website.
2. From the shortcuts list, select **`Reset Multifactor`**, as shown in the following figure.

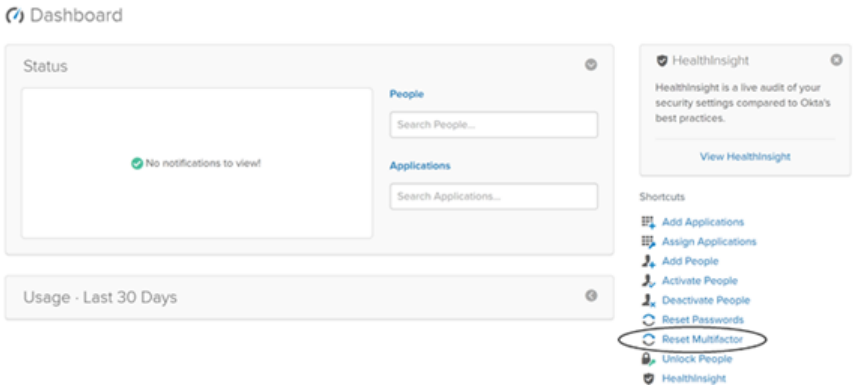


Figure 77: Reset Multifactor

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.

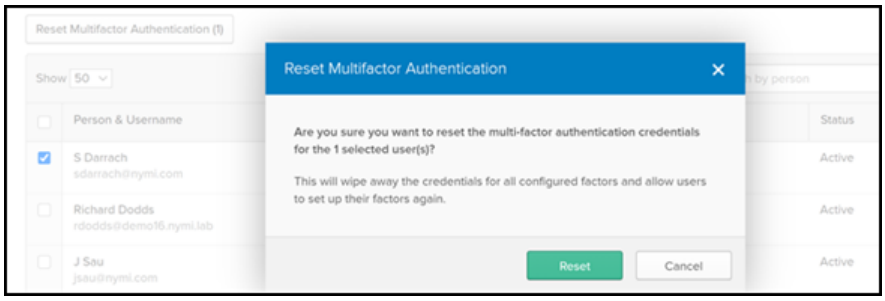


Figure 78: Reset Multifactor Authentication dialog

What to do next

After you remove the Nymi Band as a security key, the next steps you take depend on the reason you removed the Nymi Band as a security key and the Nymi Bandmode. The following table provides more information.

Reason	Standalone Nymi Band	CWP Mode Nymi Band
Re-enrollment	Put the Nymi Band on charge and perform the delete user data operation. Instruct the user to enroll their Nymi Band. The section *Enrollment of a Standalone Mode Nymi Band* provides mode information.	Put the Nymi Band on charge and perform the delete user data operation, and then remove the Nymi Band to user association in Nymi Enterprise Server(NES). Instruct the user to access the Nymi Band Application Terminal, and then perform an enrollment. **Note:** In Connected Worker Platform(CWP) 1.16.0 and later you can configure self-service enrollment. The *Nymi Connected Worker Platform—Administration Guide* provides more information about the enrollment and self-service re-enrollment processes.

Reason	Standalone Nymi Band	CWP Mode Nymi Band
Assign the Nymi Band to a new user	Put the Nymi Band on charge and perform the delete user data operation. Instruct the new user to enroll the Nymi Band. The section *Enrollment of a Standalone Mode Nymi Band* provides mode information.	Put the Nymi Band on charge, perform the delete user data operation, and then remove the Nymi Band to user association in NES. Instruct the user to access the Nymi Band Application Terminal, and then perform an enrollment. **Note:** In CWP 1.16.0 and later you can configure self-service enrollment. The *Nymi Connected Worker Platform—Administration Guide* provides more information about the enrollment and self-service re-enrollment processes.
Discontinue the use of this Nymi Band as an authenticator.	Put the Nymi Band on charge and perform the delete user data operation.	Put the Nymi Band on charge, perform the delete user data operation, and then remove the Nymi Band to user association in NES. The *Nymi Connected Worker Platform—Administration Guide* provides more information.

(OIE only) Removing the Nymi Band as an Authenticator for a User

Perform the following steps the Nymi Band as an Okta authenticator. For example, when a user re-enrolls their Nymi Band, when you assign a new Nymi Band to a user or you do not want a user to use their Nymi Band as an Okta authenticator.

Procedure

1. Log into the `Okta Admin Dashboard` website.
2. From the search bar, type the username for the user.
3. From the **`More Actions`** list select **`Reset Authenticators`**, as shown in the following figure.

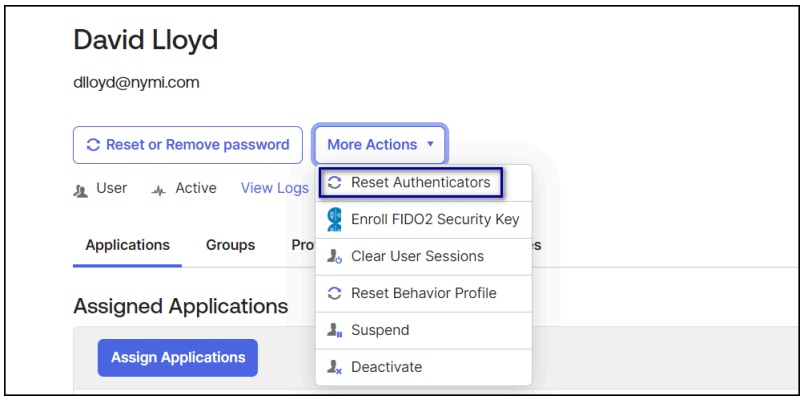


Figure 79: Reset Authenticators

4. On the `Reset Authenticators` window, select **`Nymi FIDO2 Authenticator`**, and then click **`Reset Selected Authenticators`**, as shown in the following figure.

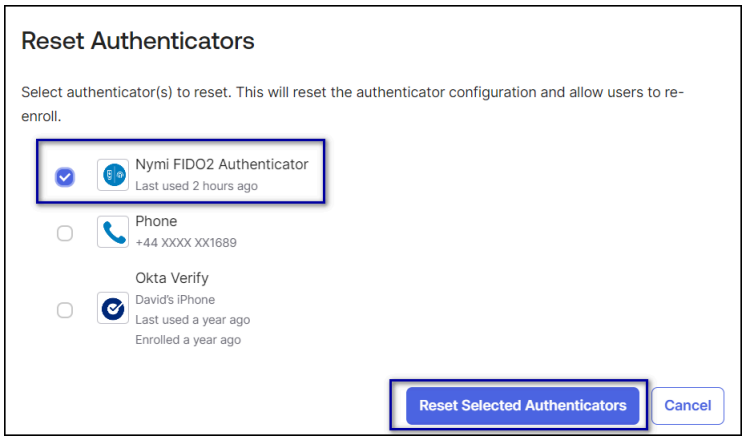


Figure 80: Reset Authenticators

What to do next

After you remove the Nymi Band as a security key, the next steps you take depend on the reason you removed the Nymi Band as a security key and the Nymi Bandmode. The following table provides more information.

Reason	Standalone Nymi Band	CWP Mode Nymi Band
Re-enrollment	Put the Nymi Band on charge and perform the delete user data operation. Instruct the user to enroll their Nymi Band. The section *Enrollment of a Standalone Mode Nymi Band* provides mode information.	Put the Nymi Band on charge and perform the delete user data operation, and then remove the Nymi Band to user association in Nymi Enterprise Server(NES). Instruct the user to access the Nymi Band Application Terminal, and then perform an enrollment. **Note:** In Connected Worker Platform(CWP) 1.16.0 and later you can configure self-service enrollment. The *Nymi Connected Worker Platform—Administration Guide* provides more information about the enrollment and self-service re-enrollment processes.
Assign the Nymi Band to a new user	Put the Nymi Band on charge and perform the delete user data operation. Instruct the new user to enroll the Nymi Band. The section *Enrollment of a Standalone Mode Nymi Band* provides mode information.	Put the Nymi Band on charge, perform the delete user data operation, and then remove the Nymi Band to user association in NES. Instruct the user to access the Nymi Band Application Terminal, and then perform an enrollment. **Note:** In CWP 1.16.0 and later you can configure self-service enrollment. The *Nymi Connected Worker Platform—Administration Guide* provides more information about the enrollment and self-service re-enrollment processes.
Discontinue the use of this Nymi Band as an authenticator.	Put the Nymi Band on charge and perform the delete user data operation.	Put the Nymi Band on charge, perform the delete user data operation, and then remove the Nymi Band to user association in NES. The *Nymi Connected Worker Platform—Administration Guide* provides more information.

Using Nymi Band 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

Ping - Registering the Nymi Band

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

Before you begin

Ensure that you plug an NFC reader 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.

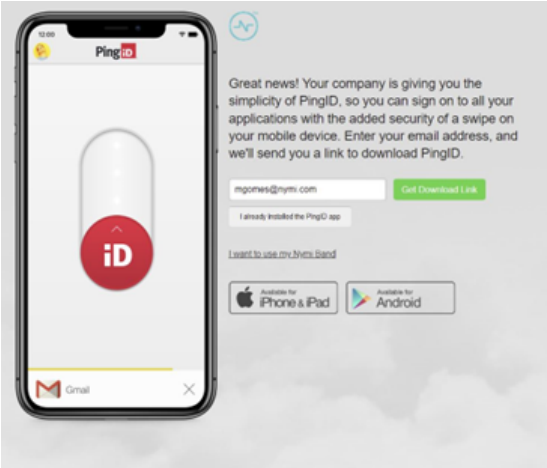


Figure 81: Id window

The following window appears while the Nymi Band pairing occurs.

Figure 82: Nymi Band pairing

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

   The following figure shows the `Alternate Authentication` window.

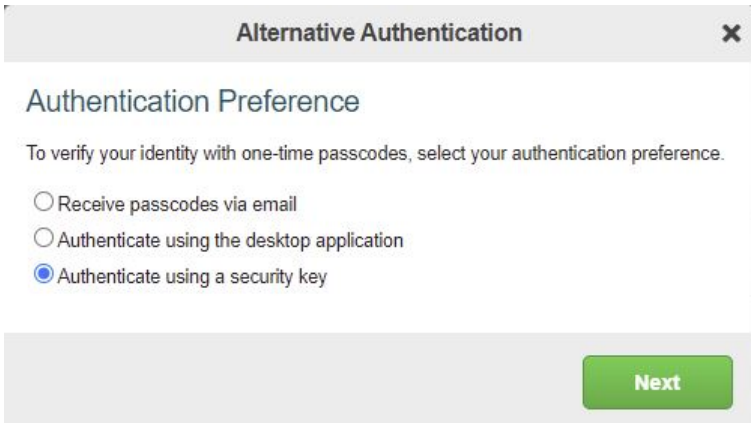


Figure 83: Alternate Authentication window

4. On the `Security key setup` window, click **OK**.
   The following figure shows the `Security key setup` window.

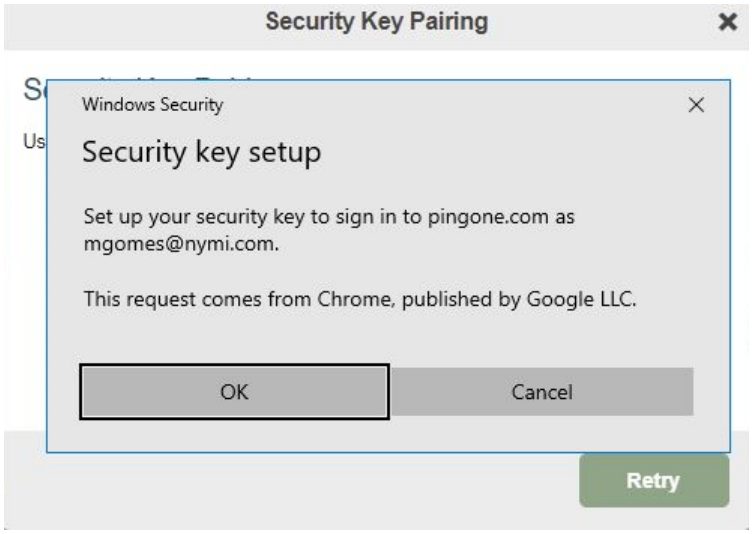


Figure 84: Security key setup window

5. On the `Continue setup` window, click **OK**.
   The following figure shows the `Continue setup` window.

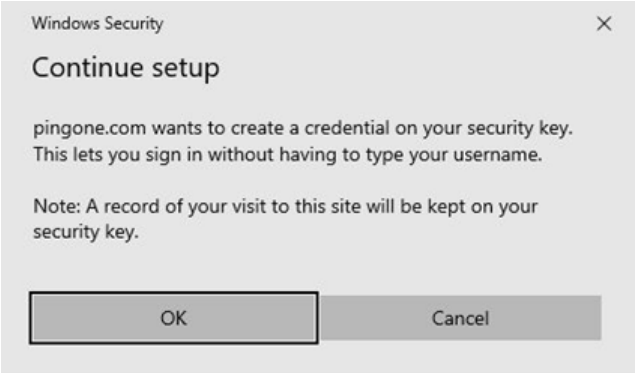


Figure 85: Continue setup window

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.

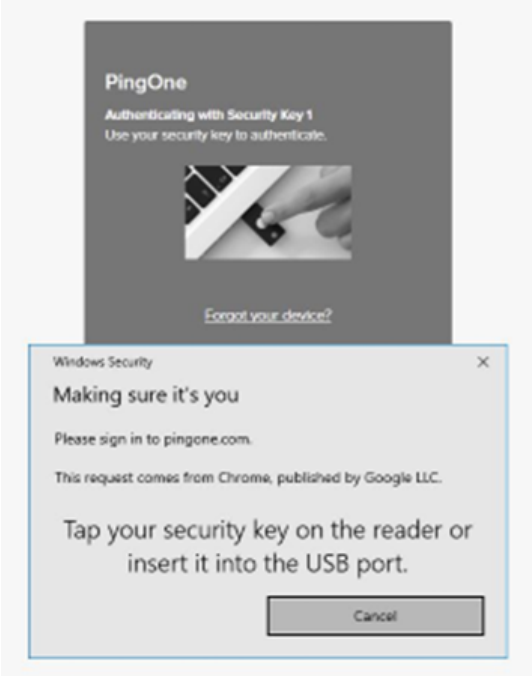


Figure 86: Making sure it's you

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.

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

- Configuring Multifactor Authentication
- Configuring passwordless authentication

Duo - Registering the Nymi Band

After you configure Duo to support the Nymi Band, users can register 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.

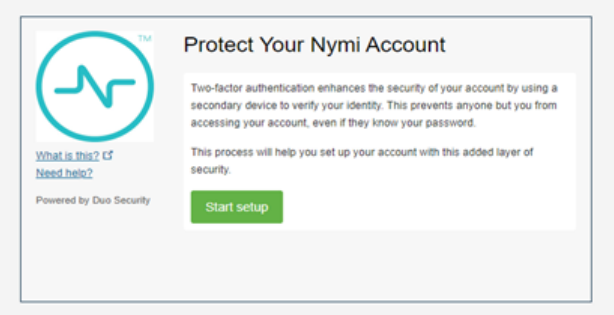


Figure 87: Project your Company account window

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.

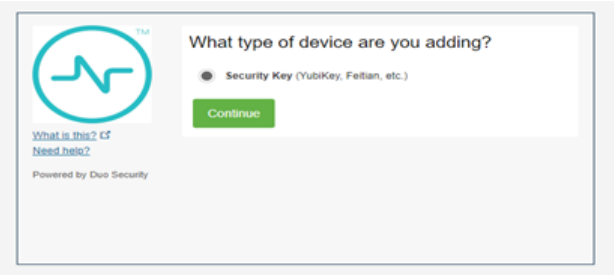


Figure 88: What type of device are you adding? window

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

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

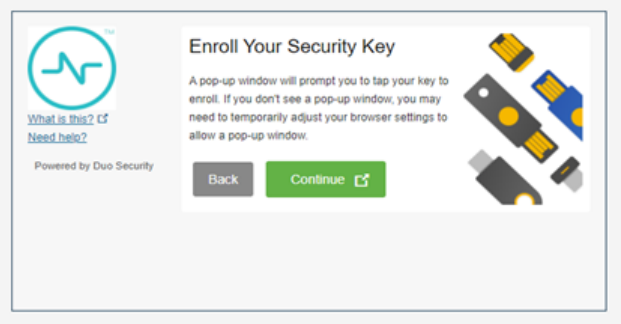


Figure 89: Enroll your Security Key window

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 90: 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.

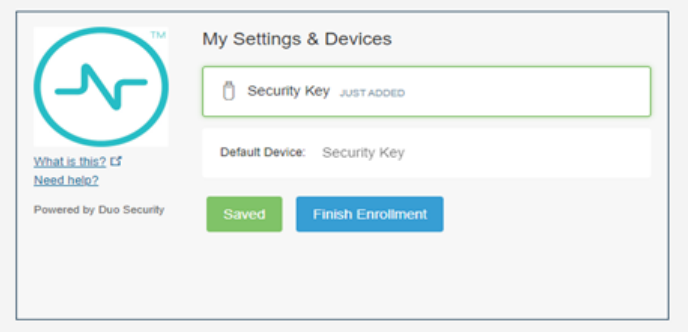


Figure 91: My settings and devices window

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

   .

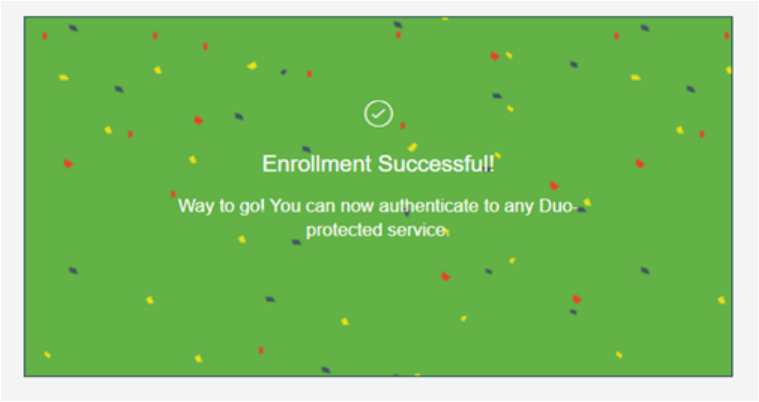


Figure 92: Enrollment Success window

Results

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

Troubleshooting FIDO2

Review this section for troubleshooting information related FIDO2

Application Prompts User for Username

When a user performs a Nymi Band tap, the login window prompts the user to type their username, as shown in the following figure.

Cause

Application configuration.

Resolution

Modify the design of the application to use login_hint.

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