POMSnet Integration Guide - Okta OIDC & FIDO2

v1.0
2024-12-06

Contents

Preface

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

Purpose

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

The Nymi Connected Worker Platform—POMSnet Installation and Configuration Guide - Otka oidc and FIDO2s provides information about how to configure POMSnet with Okta via OIDC. After you complete this integration, you can configure the Nymi Band as a FIDO2 security key in Okta to allow users to perform authentication operations in POMSnet

Audience

This guide provides information to NES, POMSnet and Okta Administrators. The responsibilities of these administrators include the management and support of the POMSnet integration with Okta, and also the registration of the Nymi Band as a FIDO2 security key in Okta.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	Novemeber 15, 2024	First release of this document.

Related documentation

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

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

  This document provides the steps that are required to deploy the Connected Worker Platform solution.

  Separate guides are provided for authentication on iOS and Windows device.
- **Nymi Connected Worker Platform—Administration Guide**

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

- **Nymi Connected Worker Platform—FIDO2 Deployment Guide**

  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.

- **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

Nymi Connected Worker Platform with POMSnet Solution

The Nymi-POMSnet solution extends the use of the Nymi Band. The Nymi Band gives users passwordless access to POMSnet and the ability to apply their digital signature to process sign-offs.

The following figure provides a high-level overview of the POMSnet solution integrated with Okta and using the Nymi Band as a FIDO2 security key registered in Okta.

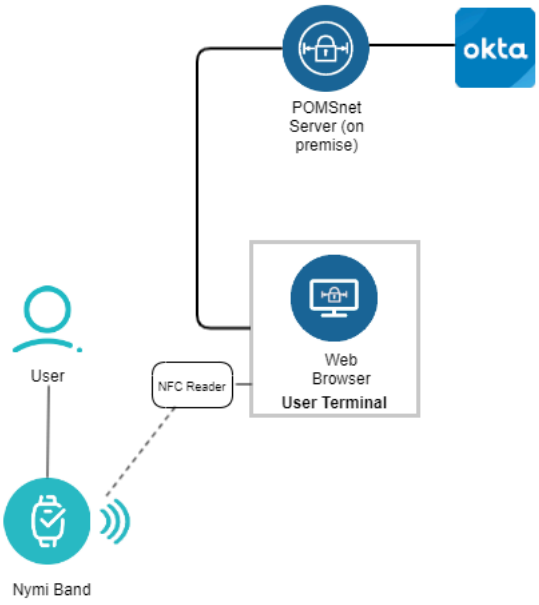

Figure 1: Nymi with POMSnet Overview

Use Cases

A user can use their authenticated Nymi Band to perform the following POMSnet tasks:

- Sign into POMSnet.
- Perform e-signatures.

Enrolling a Standalone Mode Nymi Band

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 2: 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 3: LIFT FINGER

   

   Figure 4: 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.

Configure Okta

Adding an Authenticator and Policy (OIE only)

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.

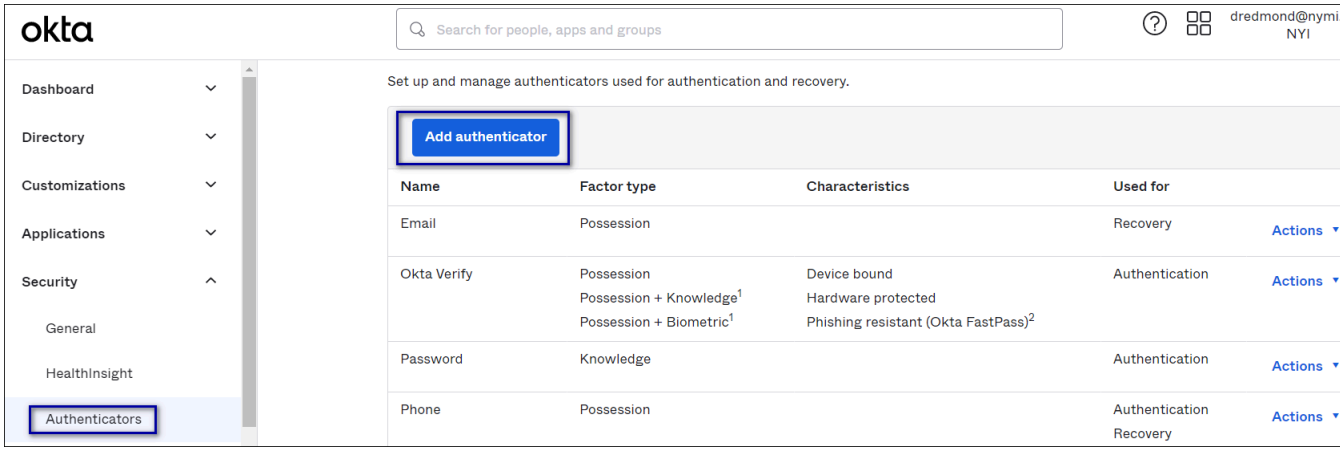

Figure 5: Add Authenticator button

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

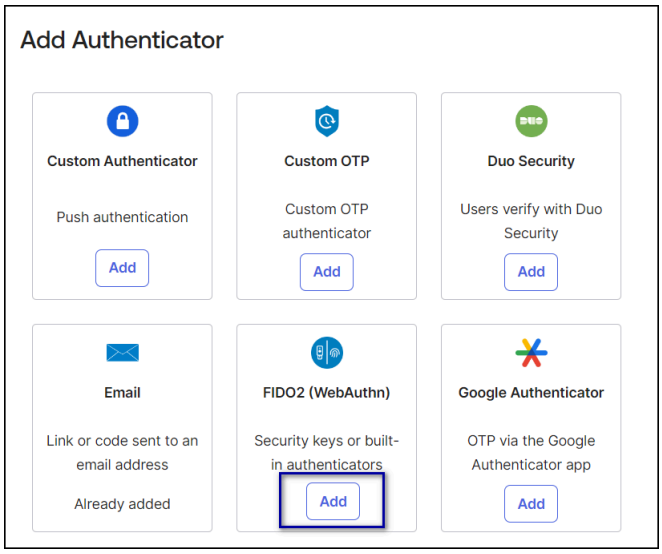

Figure 6: Add FIDO2(WebAuthn)

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.

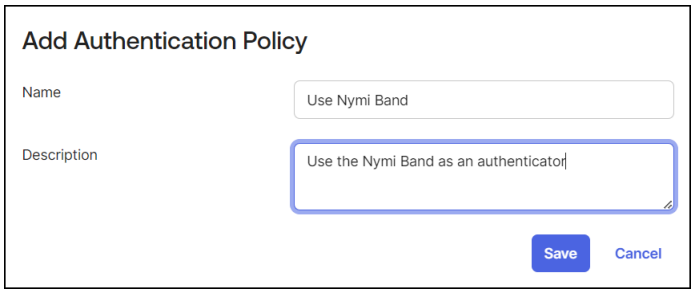

Figure 7: Assign to groups window

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 8: 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**.

Integrating POMSnet with Okta

About this task

POMSnet Aquila 2022.2.0 and later supports an integration with Okta OIDC.

Procedure

1. Login to okta.com.
2. In the left mavigation pane, expand **Applications**, select **Applications**, and then click **Create App Integration**, as shown in the following figure.

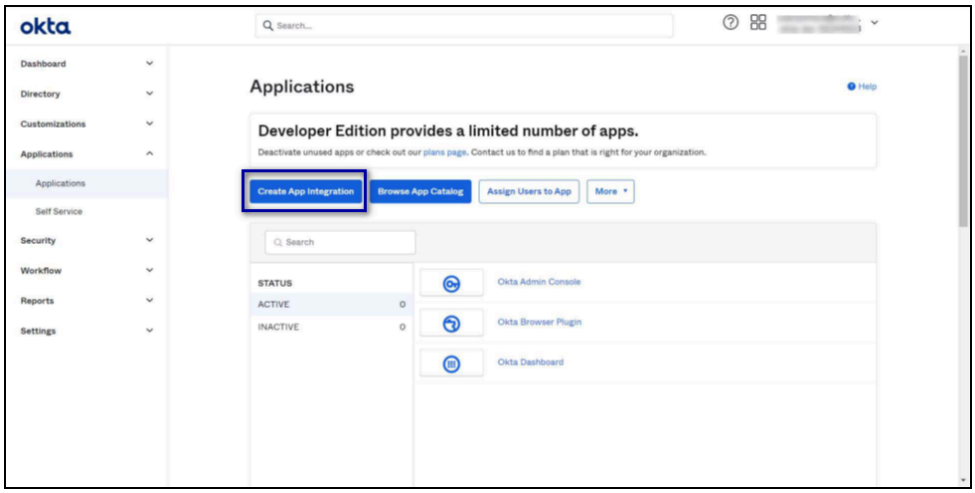

Figure 9: Create App Integration

3. In the `Sign-in method` section, select **`OIDC (Open ID Connect)`**, and in the **`Application type`** section, select **`Single-page Application`**, as shown in the following figure. Click **`Next`**.

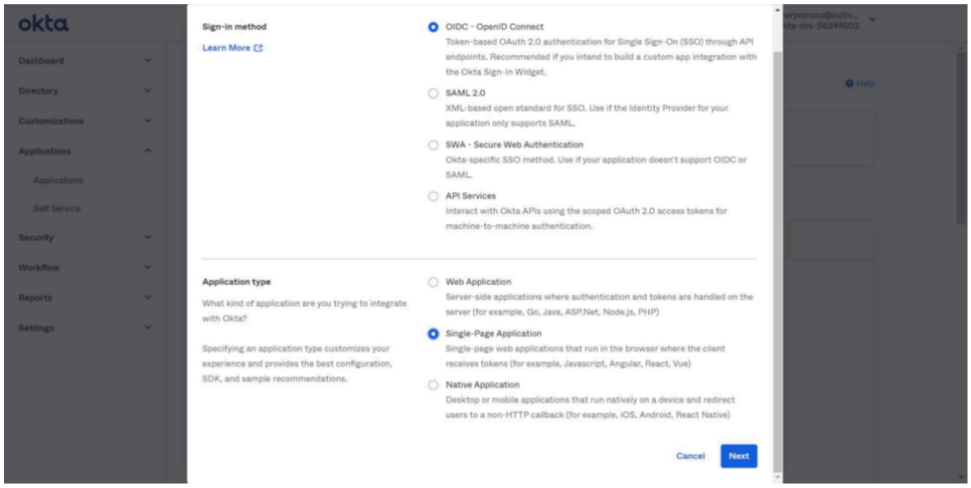

Figure 10: Create ODIC SSO Application window

4. On the New Single-Page App Integration window, perform the following steps:
   a) In the **`App Integration Name`** field, enter a name for the application, for example, ***POMSnet***.
   b) In the **`Sign-in redirect URIs`** field, specify the URL to the POMSnet User Sign in page, in the following format:

      https://hostname/poms/SAMLSignon.aspx

      where *hostname* is the FQDN of the POMSnet server.
   c) Leave the default values in the other fields, scroll down, and then click **`Save`**.

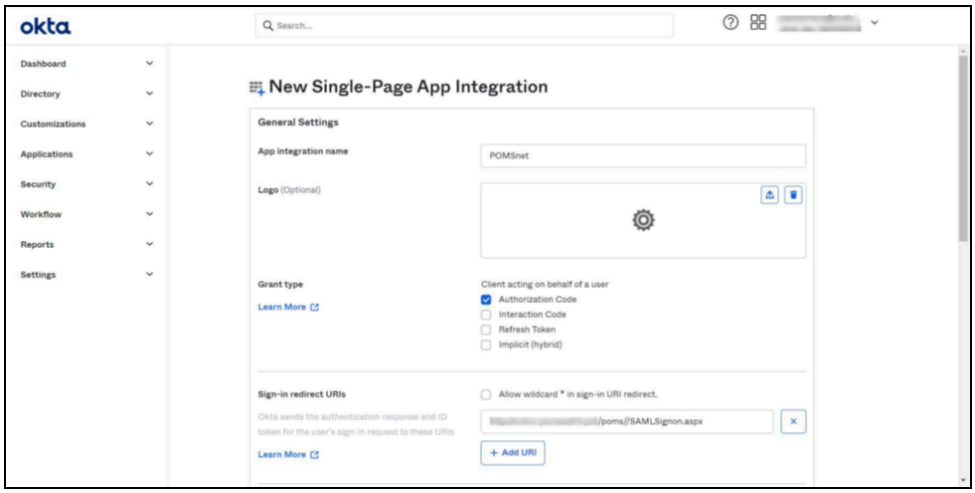

Figure 11: Create App Integration

5. On the **`Client credentials`** window, make note of the value in the **`Client ID`** field.

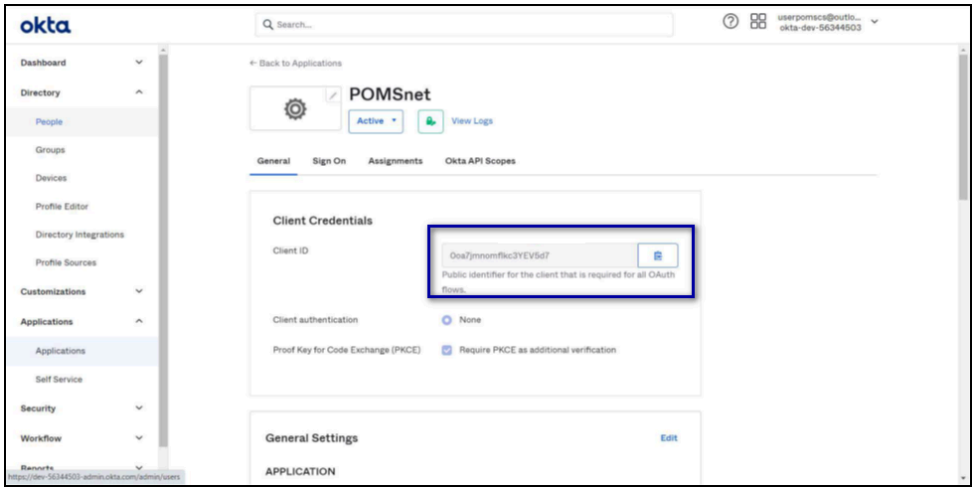

Figure 12: Create App Integration

6. From the left navigation pane, expand **`Directory`**, select **`People`**, and then click **`Add Person`**, as shown in the following figure.

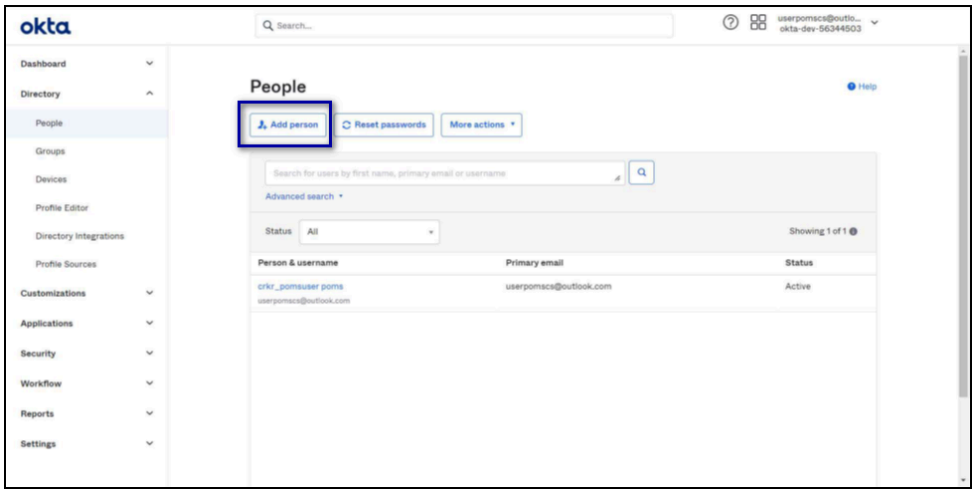

Figure 13: Create App Integration

7. In the Add `Person` window, type information about the user. POMSnet requires that you specify values in the **`First name`** and **`Last Name`** fields.
8. Click **`Save`**, or to add another user, click **`Save and Add Another`**.
9. Make note of the *subdomain* of the Okta webpage URL. The following figure highlights the subdomain.

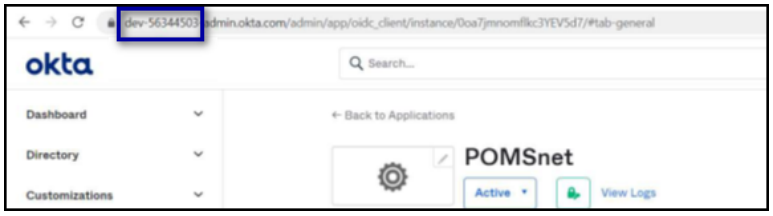

Figure 14: Okta URL Subdomain

Configure POMSnet

Create an new identity provider and then add Nymi Band users to POMSnet.

Creating a New Identity Provider

Create a new identity provider for Okta.

Procedure

1. Log into POMSnet as an administrator.
2. Navigate to **`System Administration > Security Administrator > Identity Providers.`**, as shown in the following figure.

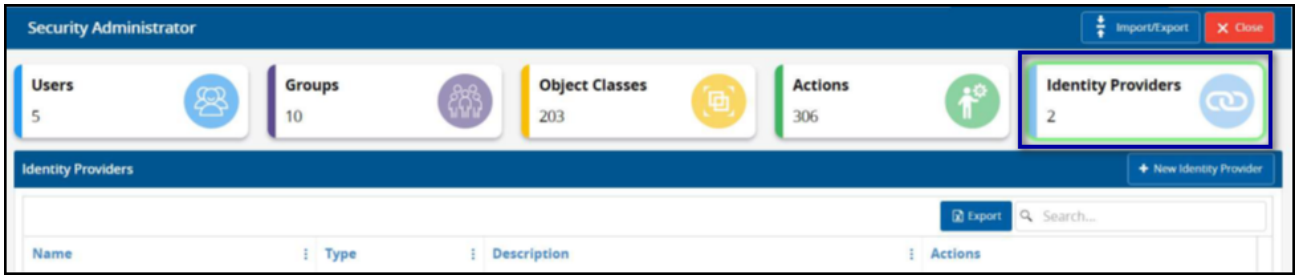

Figure 15: Identity Providers tab

3. Click **`New Identity Provider`**.
4. On the `Tasks for New Identity Provider` window, perform the following actions:
   a) In the **`Provider Name`** field, type a name for the identity provider, for example, ***OpenID_login***
   b) From the **`Provider Type`** list, select **`OpenID`**.
   c) Optionally, in the **`Description`** field, type descriptive information about the new identity.
5. On the `OpenIDSettings` tab, perform the following actions:
   a) In the **`BaseURL`** field, type:

      https://okta_subdomain.okta.com/oauth2/v1

      Where *subdomain* is the Okta URL subdomain value that you recorded in *Using OIDC to Integrate POMSnet with Okta*

      For example, ***https://dev-57306104.okta.com/oauth2/v1***
   b) In the **`ClientID`** field, type the ClientID value that you recorded in *Using OIDC to Integrate POMSnet with Okta*.

   The following figure provides an example of the `OpenIDSettings` tab.

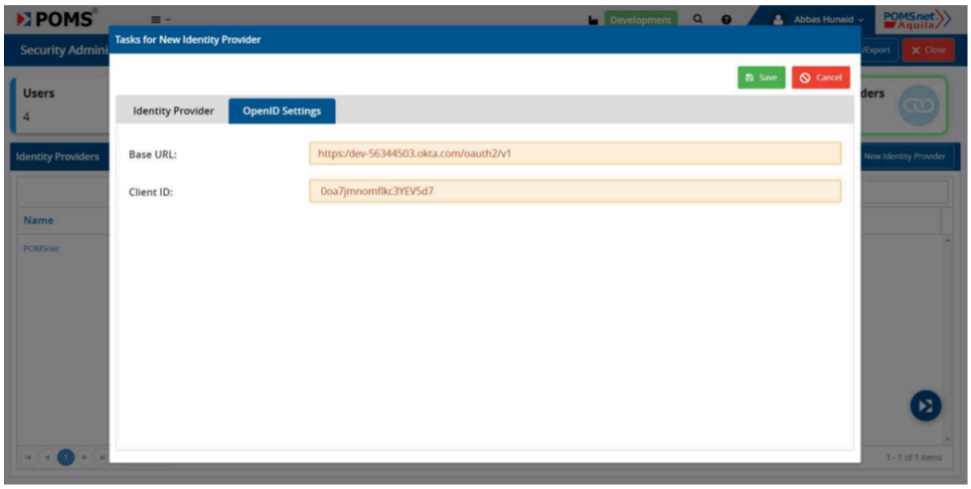

Figure 16: OpenIDSettings tab

6. Click **Save**.
   The creation of the identity provider completes.

Adding a User

Create a new POMSnet user for each person that you provide a Nymi Band.

About this task

Perform the following steps for each Nymi Band user.

Procedure

1. On the POMSnet `Security Administration` window, select the **`User`** tab, and then click **`Add User`**, as shown in the following figure.

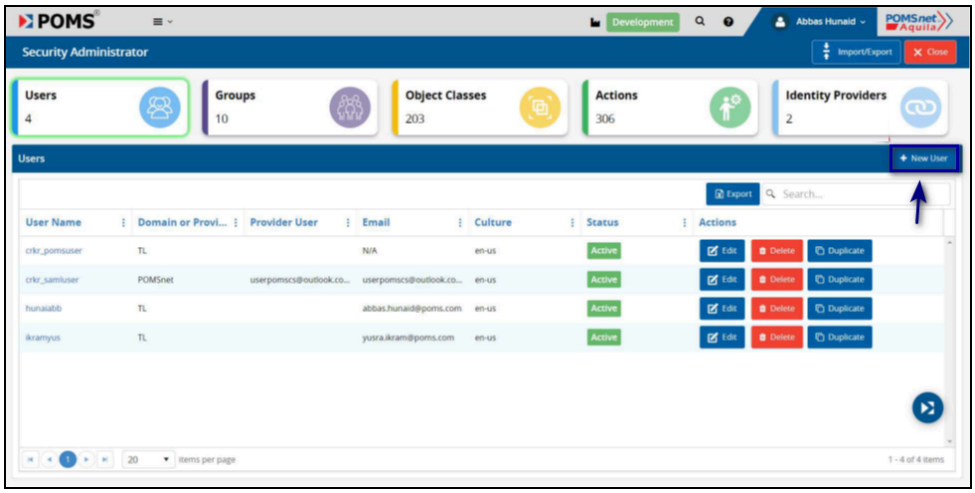

Figure 17: Add User

2. In the `Tasks for New Users` window, perform the following actions:
   a) From the **`Provider`** list, select **`OpenID_Login`**.
      The the **`Domain`** field disappears and the **`Provider User`** field appears.
   b) In the **`Provider user`** field, enter the email address of the user.
   c) In the **`Username`** field, enter the username of the user.
   d) Complete other fields as required, and then click **`Save`**.

Registering the Nymi Band as a Security Key

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.

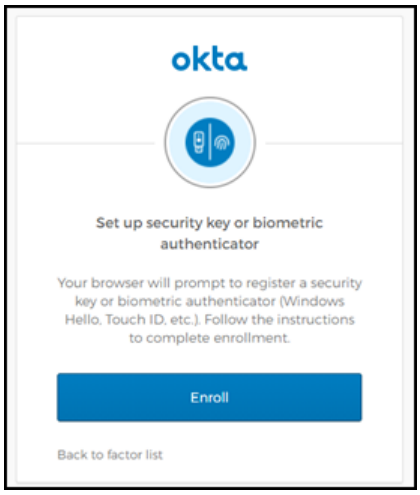

Figure 18: Okta Enroll window

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

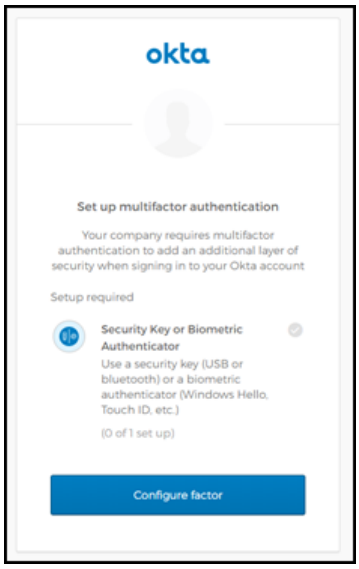

Figure 19: Set up Multifactor window

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.

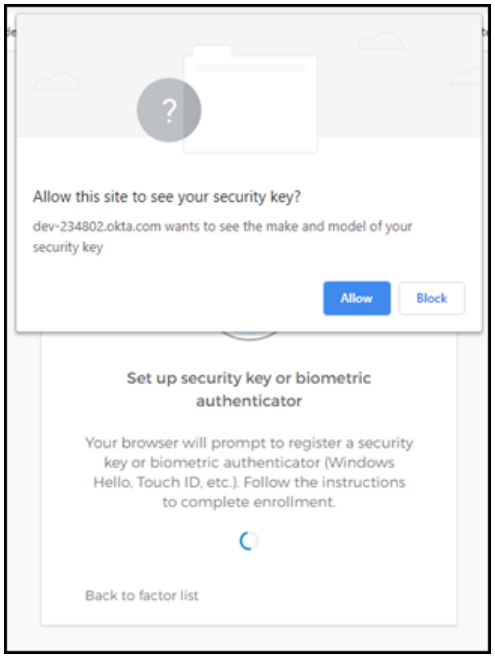

Figure 20: Allow this site to see your security key

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

Figure 21: Okta Sign In window

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

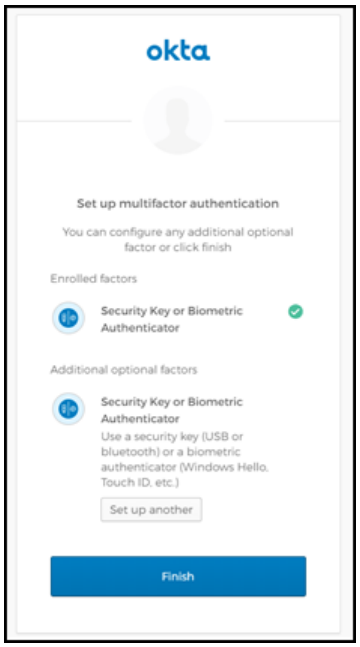

Figure 22: Set up Multifactor window

Results

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

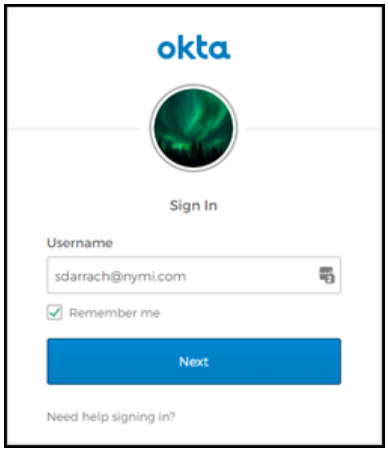

Figure 23: Okta Sign In windows

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.

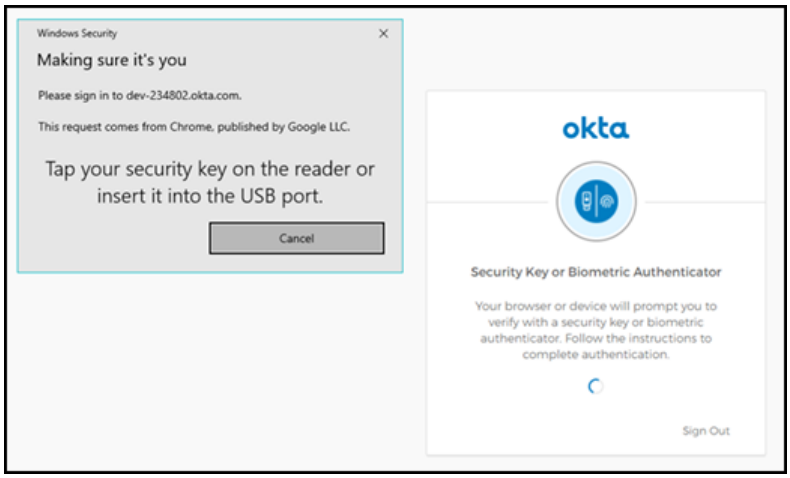

Figure 24: Making sure it's you window

Using the Nymi Band with POMSnet and Okta

Use the Nymi Band to sign into POMSnet and to perform e-signatures.

About this task

Perform the following steps on a user terminal with a connected NFC Reader and Bluetooth adapter.

Procedure

1. Connect to the POMSnet Aquila login page.
   The POMSnet webpage display an **`OpenID_Login Identity`** button, as shown in the following figure.

Figure 25: POMSnet Aquila web page

2. Click the **`OpenID_Login Identity`** button.
3. On the `Okta Sign In` window, tap an authenticated Nymi Band against the NFC reader.
   The user log in completes and the POMSnet application appears.

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

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.

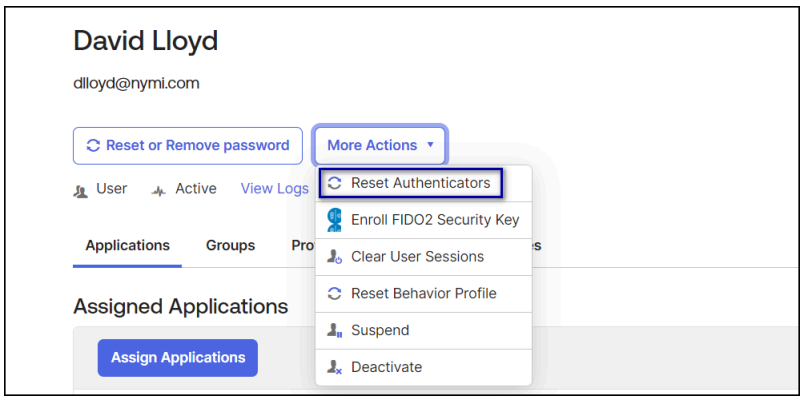

Figure 26: Reset Authenticators

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

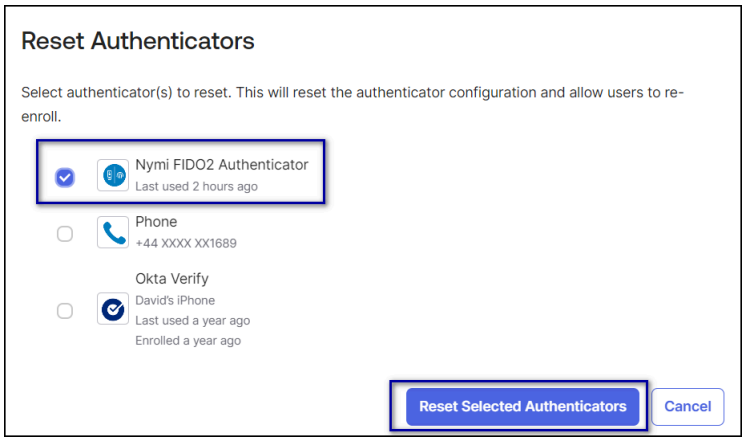

Figure 27: Reset Authenticators

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.

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.

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