This guide provides information on how to:

- Set up Beyond Identity as a passwordless authentication solution for your Okta environment.
- Set up Okta to use Beyond Identity as an Identity Provider.

Prerequisites

Ensure that you have the following:

- An Okta account with **Super** or **Organization** admin privileges to add or edit:
  - Attributes and their mappings in **Directory > Profile Editor**.
  - Identity Providers in **Security > Identity Providers**.
  - Routing rules in **Security > Identity Providers > Routing Rules**.
  - Event Hooks in **Workflow > Event Hooks**. This is optional.
- **OpenID Connect IdP** enabled for the account. Test that **OpenID Connect IdP** is enabled by verifying you have *Security* > *Identity provider* > *Add Identity Provider* > *Add OpenID Connect IdP* available. If not, contact Okta to open a support ticket to enable it. For a template of the ticket, see Open a Ticket to Enable OpenID Connect IDP Connections in Okta.
- **Routing Rules** tab is available on the **Security > Identity Providers** page. If it's missing, contact Okta to open a support ticket to enable it.

Beyond Identity information

Information you'll provide to the Beyond Identity field team

Your Company Name
Your Okta Instance URL For example, https://[your domain].okta.com
Your Okta API Token for Beyond Identity For assistance with creating a new API token in Okta, see Appendix A.
Beyond Identity Admin Portal Application credentials SSO Client ID SSO Client Secret

Your Company Name	
Beyond Identity User Portal Application credentials SSO Client ID SSO Client Secret	*This will be updated by the customer directly in Beyond Identity Admin UI.*
(Optional) A logo for your corporation Logo requirements: - 300 x 150 pixels or less - File size of 10kb or less - File types accepted: SVG, PNG, JPG, or GIF	

Information you'll receive from the Beyond Identity field team

Beyond Identity IdP endpoint URLs **- Issuer** **- Authorization endpoint** **- Token endpoint** **- JWKS endpoint**	**- https://auth.byndid.com/v2** **- https://auth.byndid.com/v2/authorize** **- https://auth.byndid.com/v2/token** **- https://auth.byndid.com/v2/.well-known/jwks.json**
Client ID [From Beyond Identity Console]	
Client Secret	[From Beyond Identity Console]
SCIM / Event Hook API Bearer Token	[From Beyond Identity SE]
Beyond Identity Org ID [From Beyond Identity SE]	
Event Hook API endpoint	https://api.byndid.com/okta_events

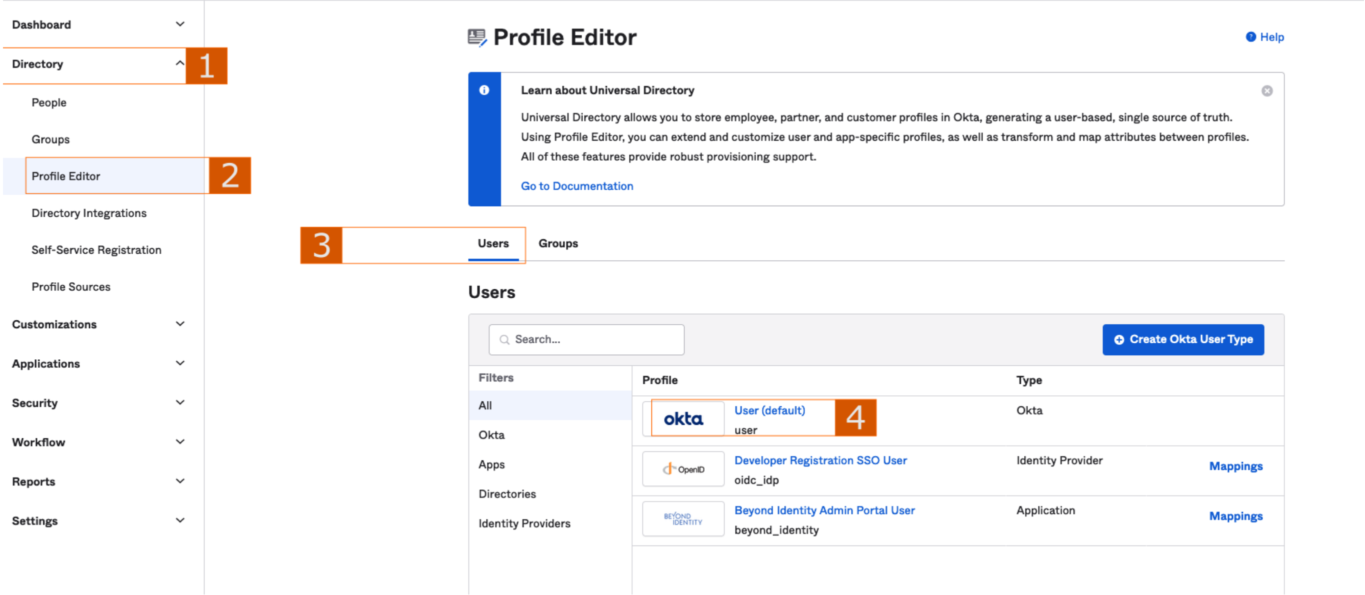
Beyond Identity IdP endpoint URLs **- Issuer** **- Authorization endpoint** **- Token endpoint** **- JWKS endpoint**	**- https://auth.byndid.com/v2** **- https://auth.byndid.com/v2/authorize** **- https://auth.byndid.com/v2/token** **- https://auth.byndid.com/v2/.well-known/jwks.json**
SCIM API endpoint	https://api.byndid.com/scim/v2/Users https://api.byndid.com/scim/v2/Groups

Okta configuration

To configure Beyond Identity as the IdP in Okta, follow the steps below. Once done, you'll be ready to enable Beyond Identity for test users.

Step 1: Navigate to the Profile Editor

The following image is an example of an administrator view in Okta. It illustrates the actions listed below to navigate to the Profile Editor:



Learn about Universal Directory

Universal Directory allows you to store employee, partner, and customer profiles in Okta, generating a user-based, single source of truth. Using Profile Editor, you can extend and customize user and app-specific profiles, as well as transform and map attributes between profiles. All of these features provide robust provisioning support.

Go to Documentation

Profile	Type
User (default) user	Okta
Developer Registration SSO User oidc_idp	Identity Provider
Beyond Identity Admin Portal User beyond_identity	Application

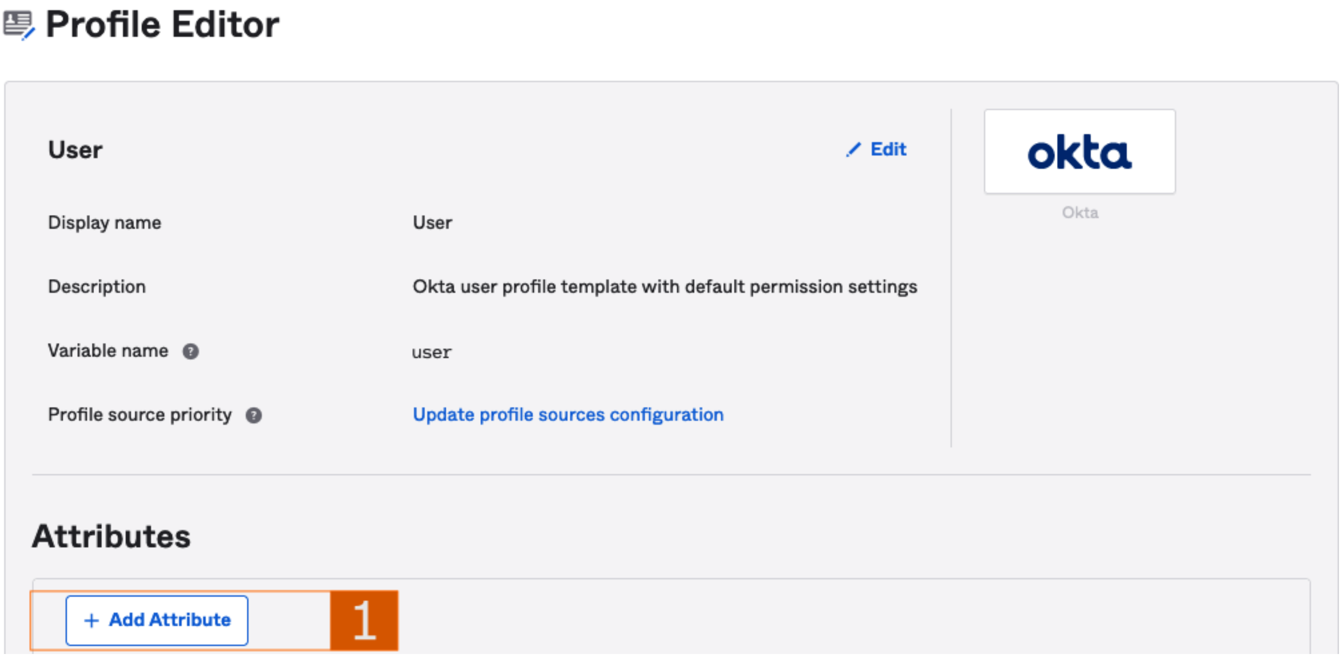
1. Sign into the Okta portal as an administrator.

2. In the main Okta menu, select **Directory**.

3. In the **Directory** drop-down menu, select **Profile Editor**.

4. Find your **Okta** profile and select the **user(default)**.

5. Under the user profile editor, you will see an action to **Add Attribute**.



Profile Editor

User

Edit

Display name: User

Description: Okta user profile template with default permission settings

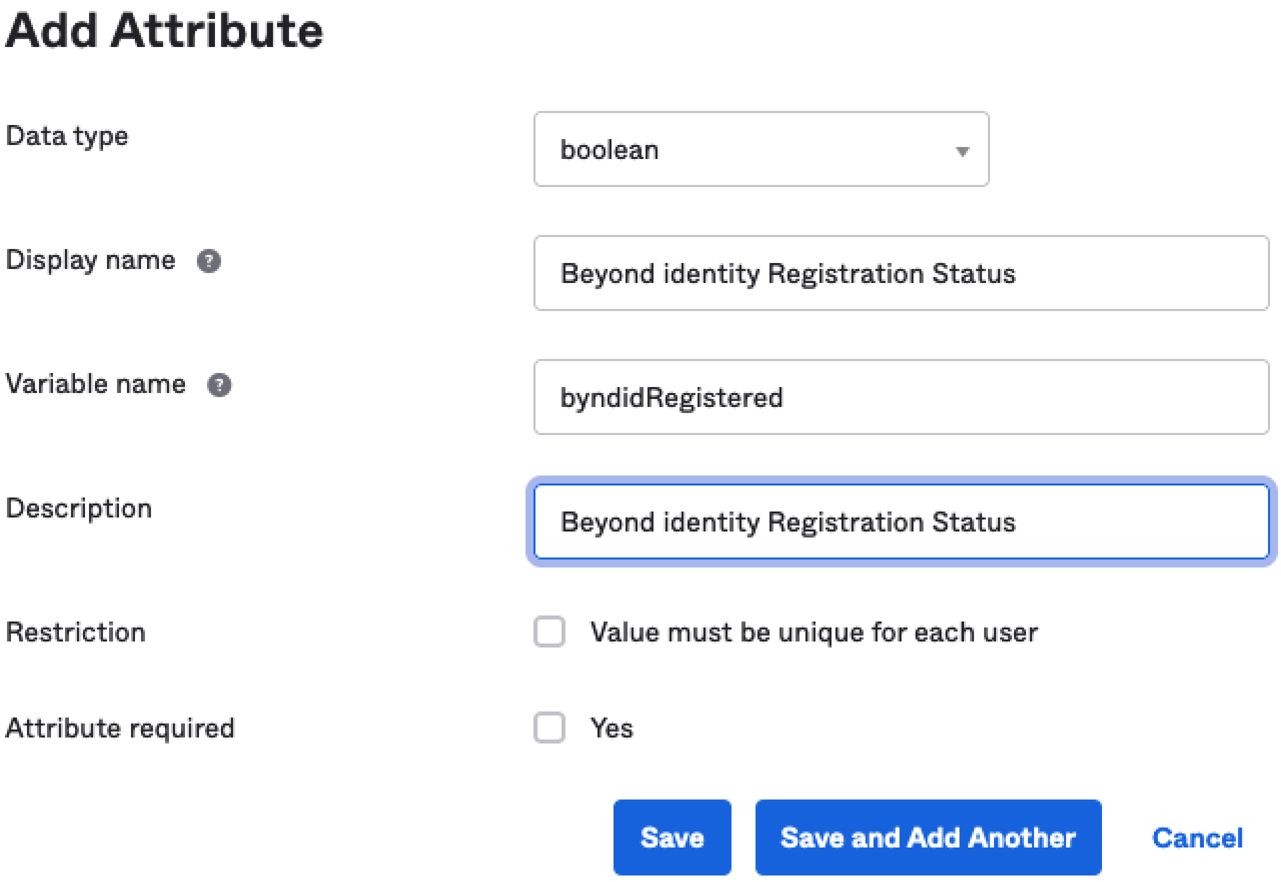
Variable name: user

Profile source priority: Update profile sources configuration

Attributes

6. Select the fields as shown in the following image. Then click **Save**.

- Data Type: **Boolean**
- Display Name: **Beyond Identity Registration Status**
- Variable Name: **byndidRegistered**
- Description: **Beyond Identity Registration Status**



Add Attribute

Data type: boolean

Display name: Beyond identity Registration Status

Variable name: byndidRegistered

Description: Beyond identity Registration Status

Restriction: □ Value must be unique for each user

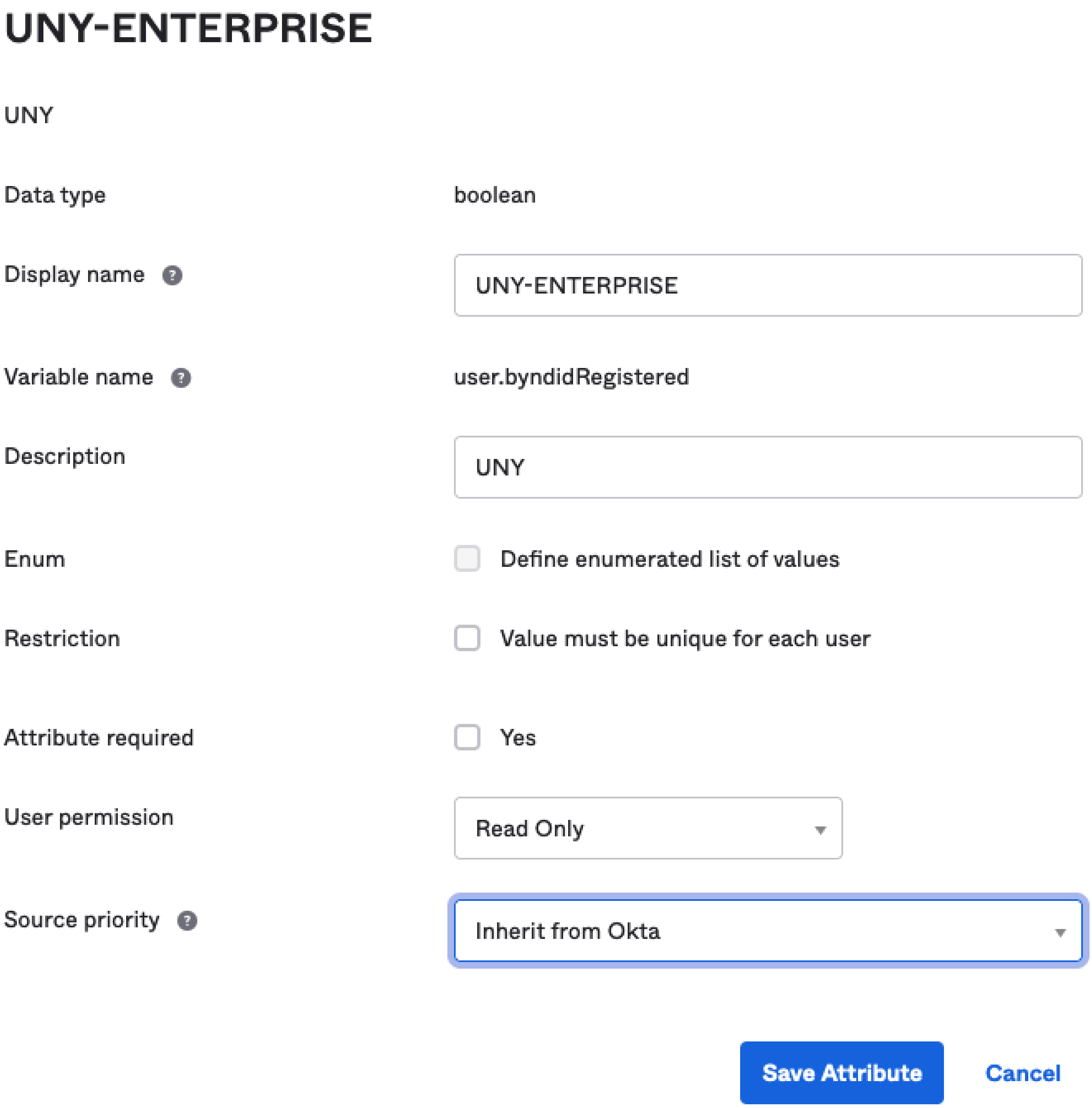
Attribute required: □ Yes

7. If you have multiple profile masters (applicable for AD mastered users), perform the following steps.

8. Click on the edit button for the **byndidRegistered** attribute in Okta profile.

9. For the **Source Priority** field select **Inherit from Okta** from the drop-down menu.

10. Click **Save Attribute**.



UNY-ENTERPRISE

UNY

Data type	boolean
Display name	UNY-ENTERPRISE
Variable name	user.byndidRegistered
Description	UNY
Enum	□ Define enumerated list of values
Restriction	□ Value must be unique for each user
Attribute required	□ Yes
User permission	Read Only
Source priority	Inherit from Okta

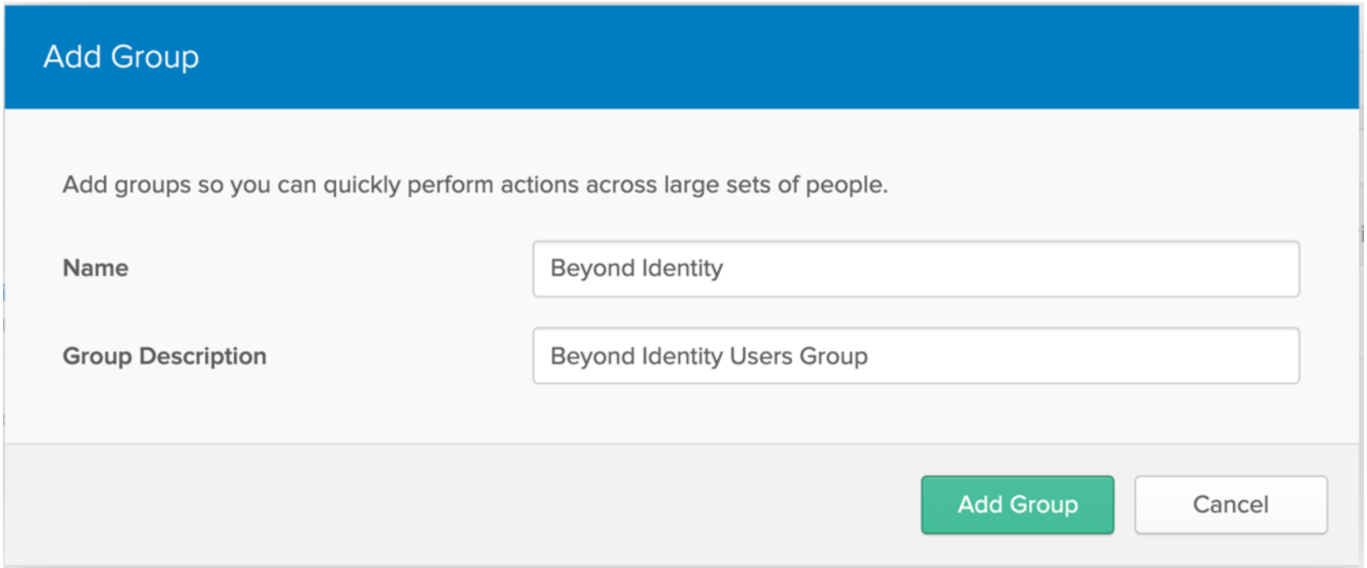
Step 2: Add Beyond Identity User Group

1. Click on **Directory** > **Group**.

2. Click **Add Groups**.

3. Select the fields as shown in the following image. Then click **Add Group**.

- Name: **Beyond Identity**
- Description: **Beyond Identity Users Group**



Add Group

Add groups so you can quickly perform actions across large sets of people.

Name: Beyond Identity

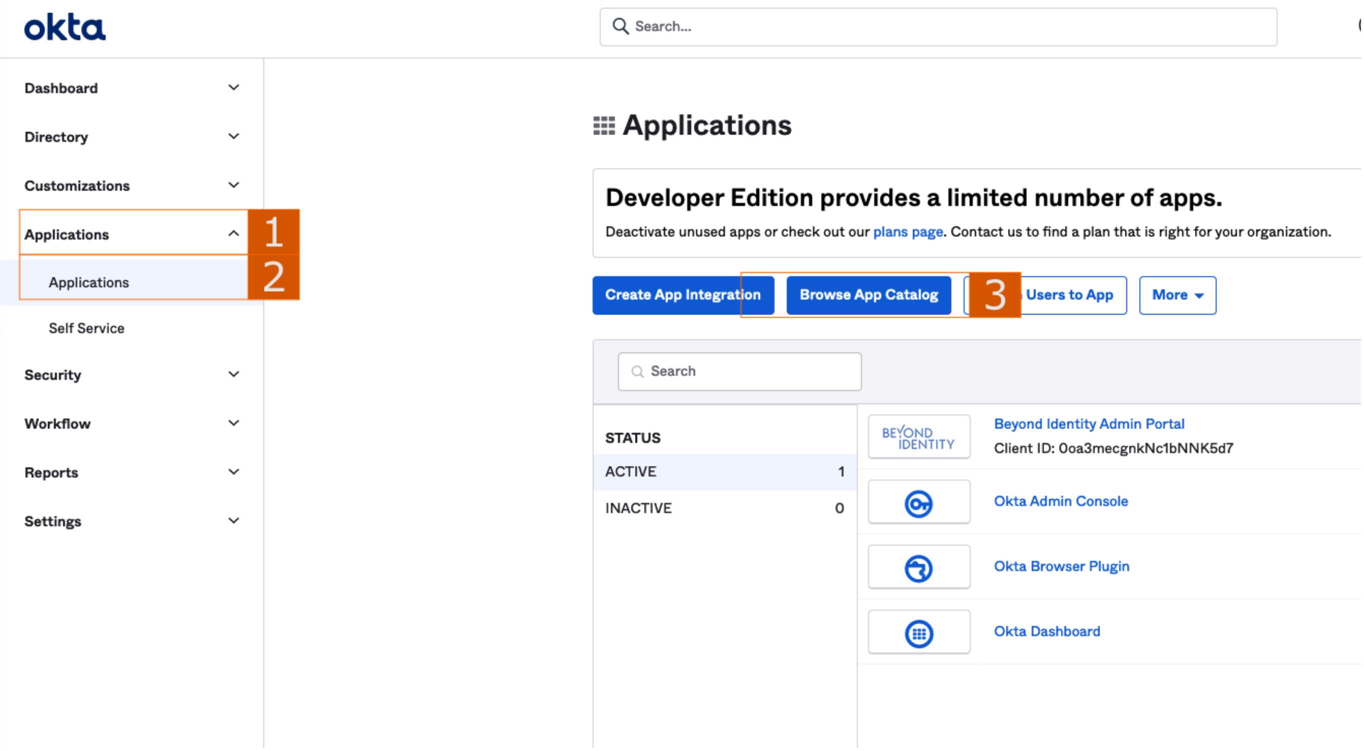
Group Description: Beyond Identity Users Group

Step 3: Set up the Beyond Identity Admin Application in Okta

1. Click **Applications > Browse App catalog**.

2. In the Search window, enter **Beyond Identity Admin**.

3. Select the **Beyond Identity Admin Portal** app and click **Add**.



Applications

Developer Edition provides a limited number of apps.

Deactivate unused apps or check out our plans page. Contact us to find a plan that is right for your organization.

STATUS	
ACTIVE	1
INACTIVE	0

Beyond Identity Admin Portal
Client ID: 0oa3mecgnkNc1bNNK5d7

Okta Admin Console

Okta Browser Plugin

Okta Dashboard

4. Under **General Settings**, update the **Application Label** field with **Beyond Ideneity Admin Portal**. Then click **Done**.

5. In the **Assignment** tab, assign **Admins** to this application.

6. In the **Sign On** tab, click **Edit**, and update the following with the information provided by Beyond Identity:

- Org ID
- Client ID
- Client Secret

Step 4: Setup Admin Portal Access

1. Provide the **Client ID** and **Client Secret** assigned to the admin UI application in Okta to Beyond Identity SE. The Beyond Identity team will collect and configure this value.

2. **Beyond Identity Field Team:** Configure the following fields through Beyond Identity Support Console while updating the Admin Console Configuration.

- Name: **Okta OIDC Integration**
- Client ID: *Use the value recorded in the previous step*
- Client Secret: *Use the value recorded in the previous step*
- Issuer: https://<*okta-tenant-id*>.okta.com (Provided by the customer as Login URL) **TIP** For custom domain names, replace <*okta-tenant-id*>.okta with your domain. For example, *sso.*<*domain*>.com.
- Token Field: **sub**
- Token Field Lookup: **external_id**

After provisioning, the customer should log in and confirm that the admin has access to Beyond Identity Console.

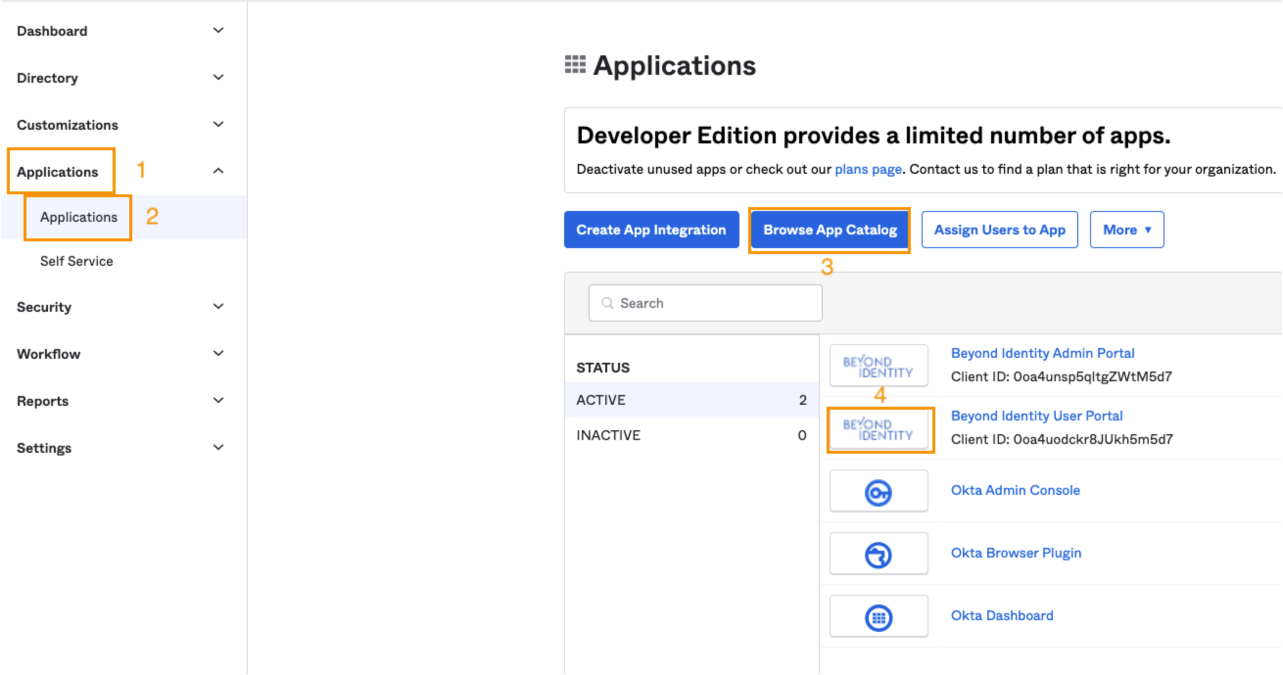
Step 5: Setup Beyond Identity User Portal Application in Okta

1. Click **Applications > Browse App Catalog**.

2. In Search window, enter **Beyond Identity User**.

3. Select **Beyond Identity User Portal** app.

4. Click **Add**.



Developer Edition provides a limited number of apps.

Deactivate unused apps or check out our plans page. Contact us to find a plan that is right for your organization.

Client ID: 0oa4unsp5qltgZWtM5d7

Client ID: 0oa4uodckr8JUkh5m5d7

5. A dialog displays the general settings and the application label. Click **Done**.

6. In the Assignment Tab, click **Assign** and from the drop-down the select **Assign to Groups**.

7. Click **Assign** for the Beyond Identity group.

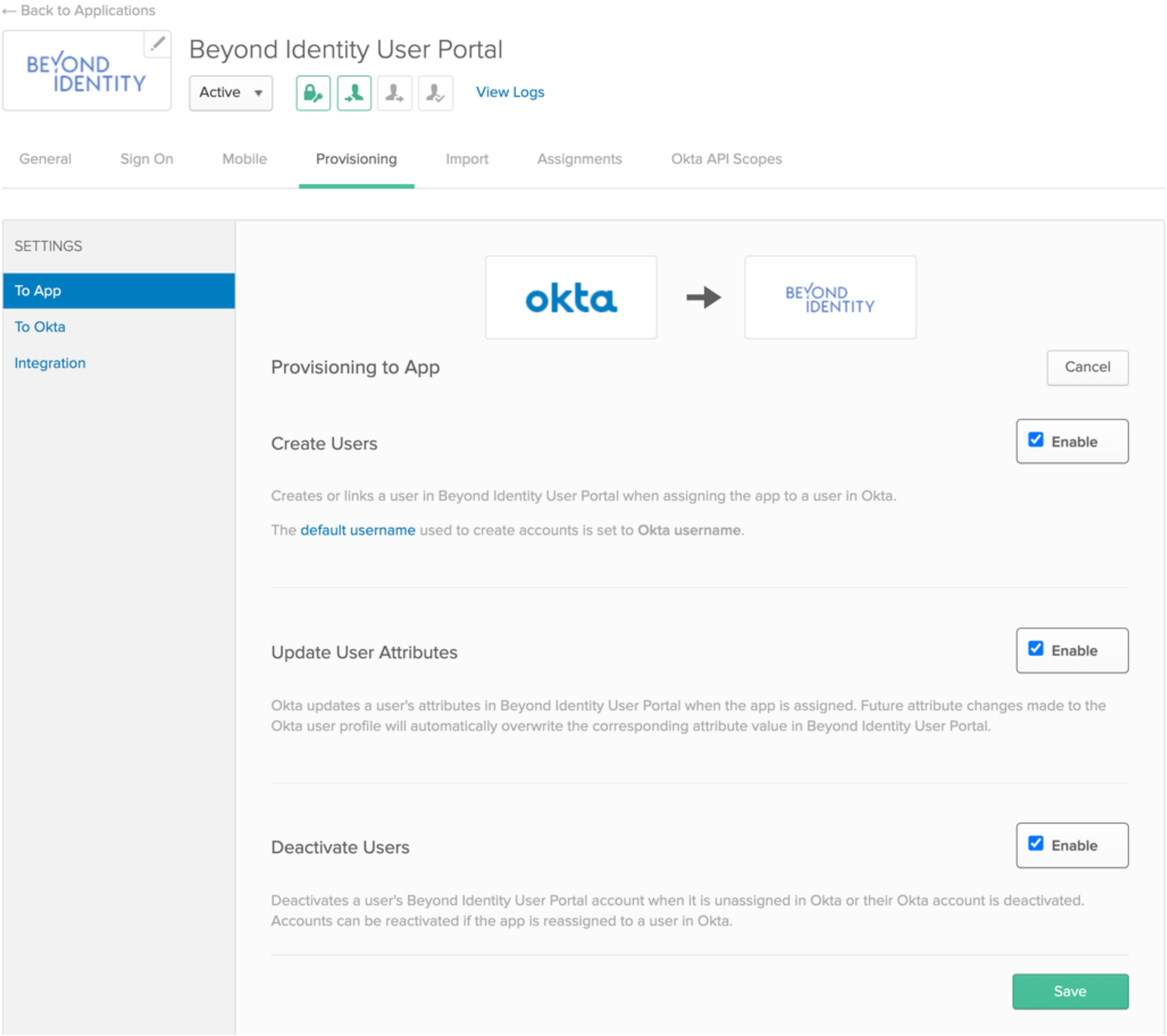
8. In the **Sign On** tab, click **Edit**, update **Org ID** with the information provided by Beyond Identity.

9. Copy the **Client ID** and **Client Secret**. You'll use this later in the configuration.

10. In the **Provisioning** tab, click **Configure API Integration > Enable API Integration**.

11. In the API token field, paste the API token provided by Beyond Identity, and click **Test API Credentials**. Then click **Save** after you see the *Beyond Identity User Portal was verified Successfully*.

12. In the **Provisioning to App** section, click **Edit**, and enable the following. Then click **Save**.
    - Create Users
    - Update User Attributes
    - Deactivate Users



Provisioning to App

Create Users ☑ Enable

Creates or links a user in Beyond Identity User Portal when assigning the app to a user in Okta.

The default username used to create accounts is set to Okta username.

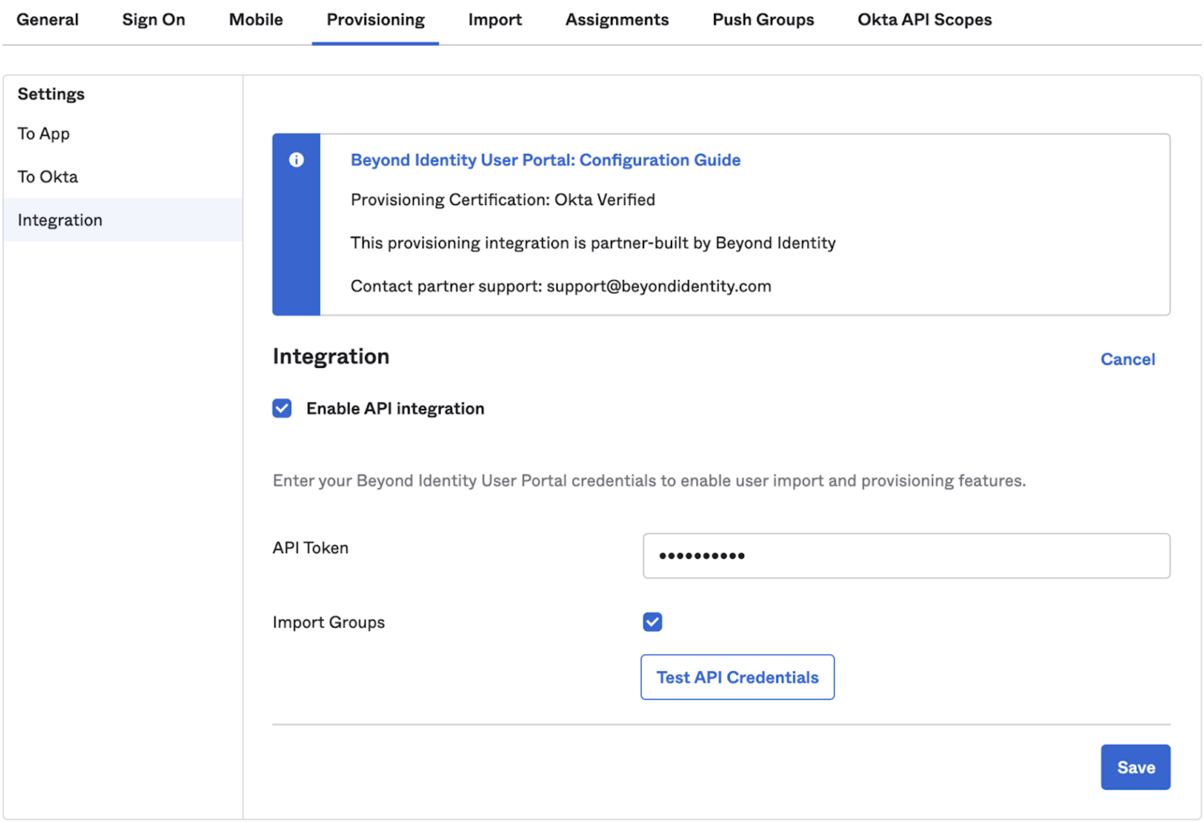
Update User Attributes ☑ Enable

Okta updates a user's attributes in Beyond Identity User Portal when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Beyond Identity User Portal.

Deactivate Users ☑ Enable

Deactivates a user's Beyond Identity User Portal account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

13. For Okta production instances, in the **Provisioning** tab, click **Edit > Integration**, select the **Import Groups** checkbox. Then click **Save**.



Beyond Identity User Portal: Configuration Guide

Provisioning Certification: Okta Verified

This provisioning integration is partner-built by Beyond Identity

Contact partner support: support@beyondidentity.com

Integration

☑ Enable API integration

Enter your Beyond Identity User Portal credentials to enable user import and provisioning features.

API Token: ••••••••••

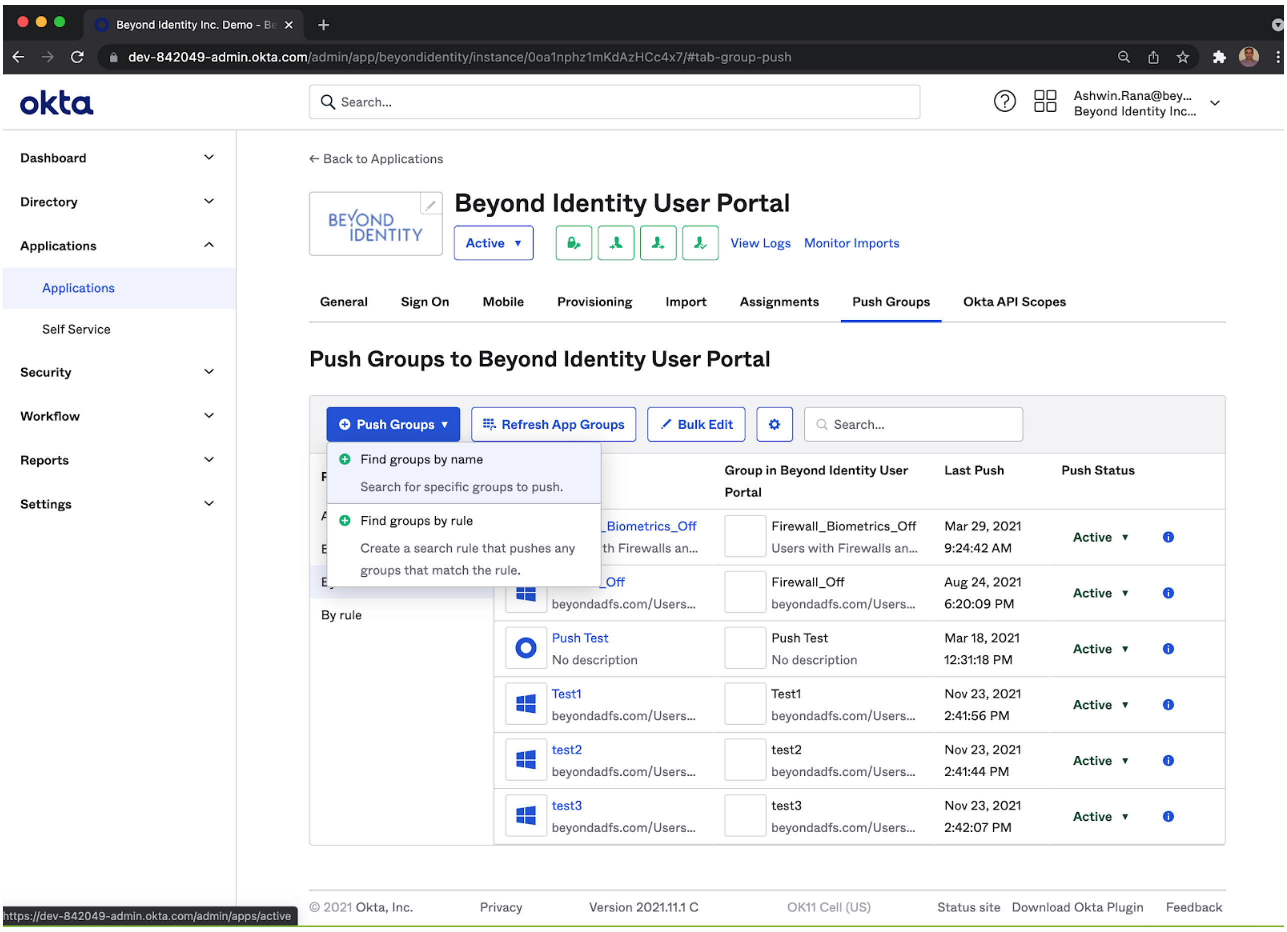
Import Groups: ☑

14. Sync groups with Beyond Identity:

    1. Click the **Push Groups** tab.

    2. Select the **Push Groups** drop-down menu.

    3. Select **Find groups by name** to define which groups are synced with Beyond Identity.



Beyond Identity User Portal

Push Groups to Beyond Identity User Portal

	Group in Beyond Identity User Portal	Last Push	Push Status
_Biometrics_Off th Firewalls an...	Firewall_Biometrics_Off Users with Firewalls an...	Mar 29, 2021 9:24:42 AM	Active ▾
_Off beyondadfs.com/Users...	Firewall_Off beyondadfs.com/Users...	Aug 24, 2021 6:20:09 PM	Active ▾
Push Test No description	Push Test No description	Mar 18, 2021 12:31:18 PM	Active ▾
Test1 beyondadfs.com/Users...	Test1 beyondadfs.com/Users...	Nov 23, 2021 2:41:56 PM	Active ▾
test2 beyondadfs.com/Users...	test2 beyondadfs.com/Users...	Nov 23, 2021 2:41:44 PM	Active ▾
test3 beyondadfs.com/Users...	test3 beyondadfs.com/Users...	Nov 23, 2021 2:42:07 PM	Active ▾

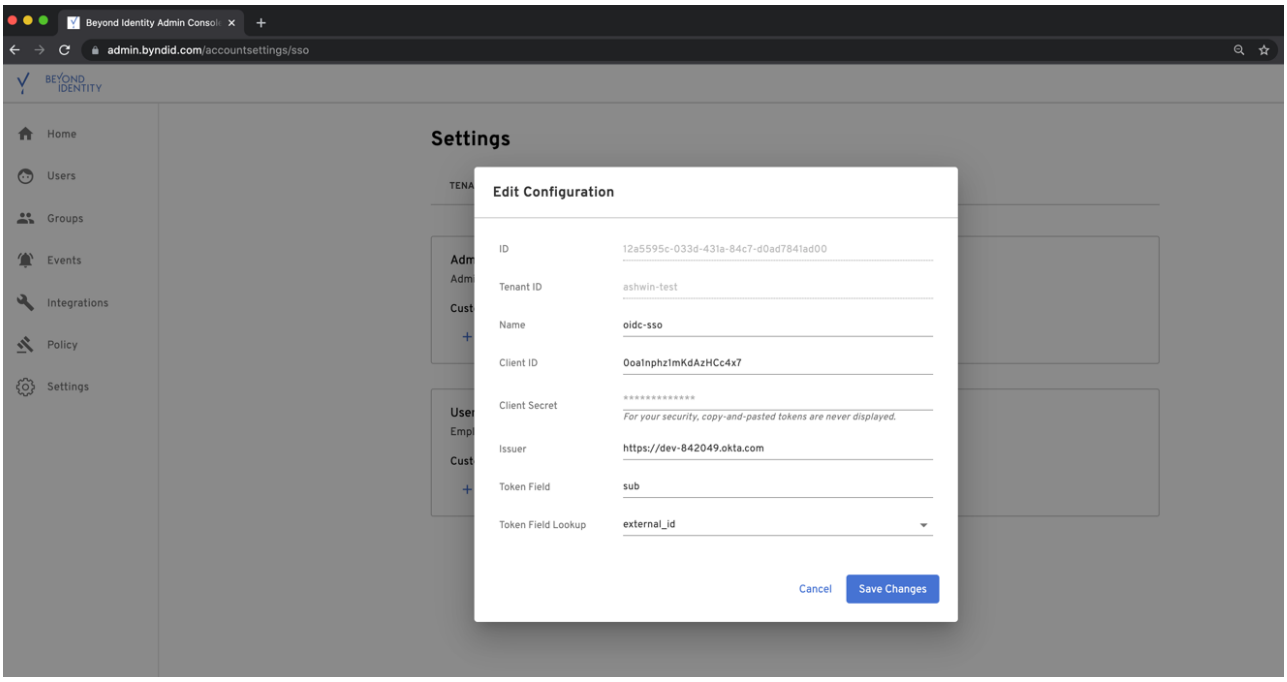
Beyond Identity configuration

Step 1: Set up the Beyond Identity User Console Authentication

1. Log into the Beyond Identity Admin Console and click **Settings > Console Login> User Console SSO Integration**.

2. Click **Add OIDC SSO** and configure the following fields for the User Console SSO Integration. Then click **Save Changes**.

   - Name: **Okta OIDC Integration**
   - Client ID: *Use the value recorded in the previous step*
   - Client Secret: *Use the value recorded in the previous step*
   - Issuer: https://<*okta-tenant-id*>.okta.com (Provided by the customer as Login URL) **TIP** For custom domain names, replace <*okta-tenant-id*>.okta with your domain. For example, *sso.<domain>*.com.
   - Token Field: **sub**
   - Token Field Lookup: **external_id**



Edit Configuration

ID	12a5595c-033d-431a-84c7-d0ad7841ad00
Tenant ID	ashwin-test
Name	oidc-sso
Client ID	0oa1nphz1mKdAzHCc4x7
Client Secret	************* *For your security, copy-and-pasted tokens are never displayed.*
Issuer	https://dev-842049.okta.com
Token Field	sub
Token Field Lookup	external_id

Cancel Save Changes

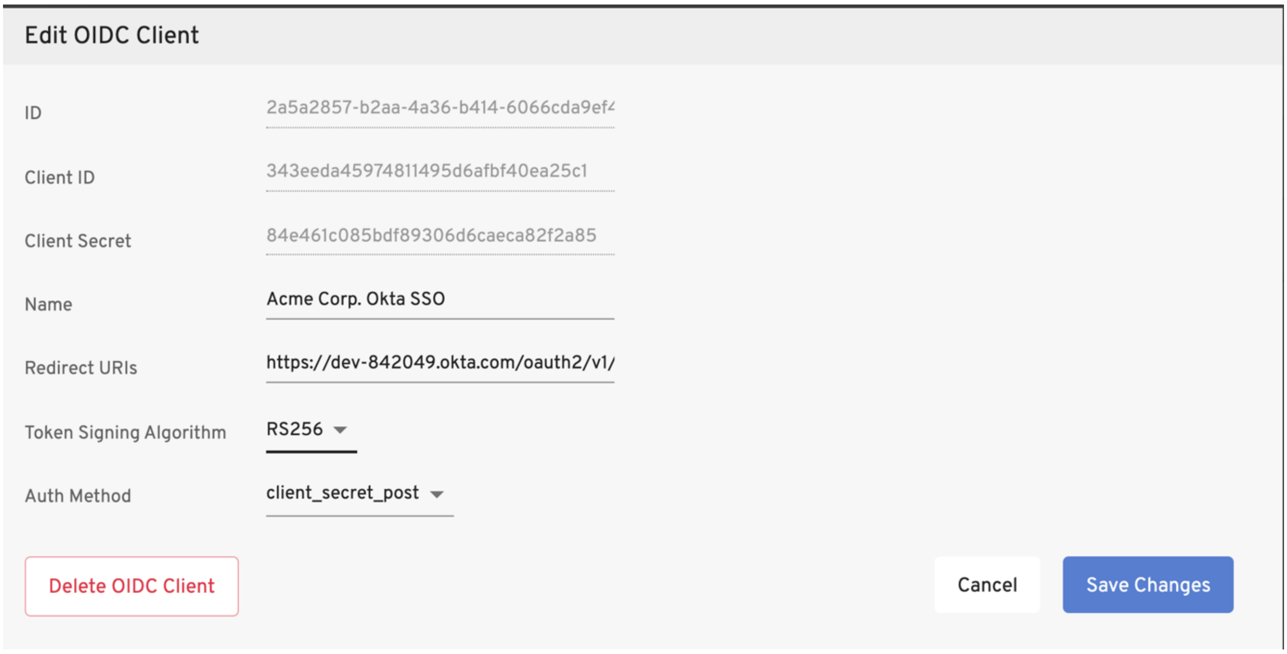
Step 2: Setup Beyond Identity Console for User Authentication

1. Log into the Beyond Identity Admin Console and click the **Integrations** tab, and click **OIDC**.

2. Click **Add OIDC Client**, and enter the following information. Then click **Save Changes**.

   - Name: **Okta SSO**
   - Redirect URIs: https://<*okta-tenant-name*>.okta.com/oauth2/v1/authorize/callback **TIP** You can add multiple Redirect URIs using a comma between the URLs.
   - Token Signing Algorithm: **RS256**
   - Auth Method: **Client_secret_post**

3. Select the OIDC created above and copy the **Client ID** and **Client Secret** values. You'll use these values in the next step.

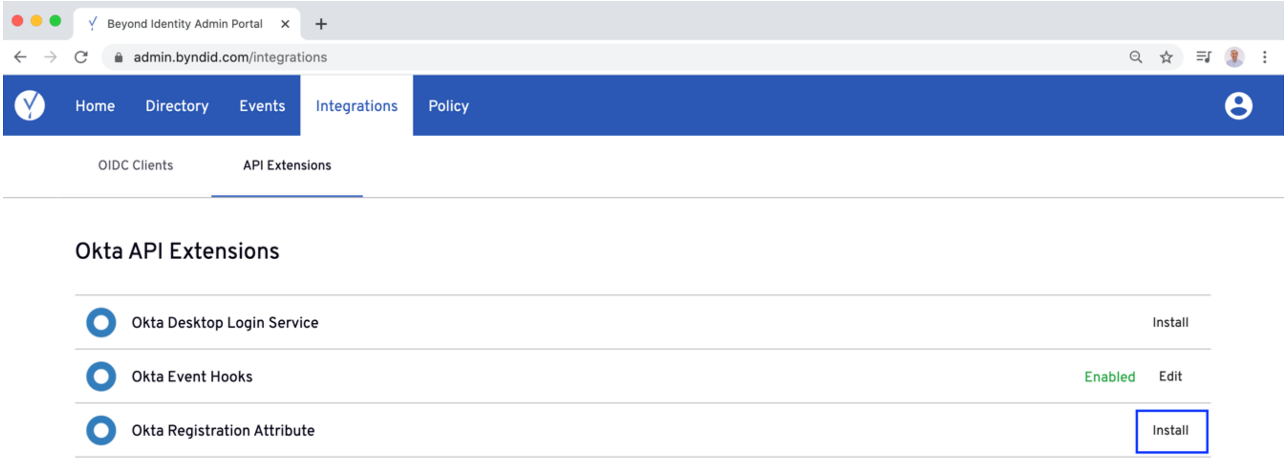


Edit OIDC Client

ID	2a5a2857-b2aa-4a36-b414-6066cda9ef4
Client ID	343eeda45974811495d6afbf40ea25c1
Client Secret	84e461c085bdf89306d6caeca82f2a85
Name	Acme Corp. Okta SSO
Redirect URIs	https://dev-842049.okta.com/oauth2/v1/
Token Signing Algorithm	RS256
Auth Method	client_secret_post

Delete OIDC Client Cancel Save Changes

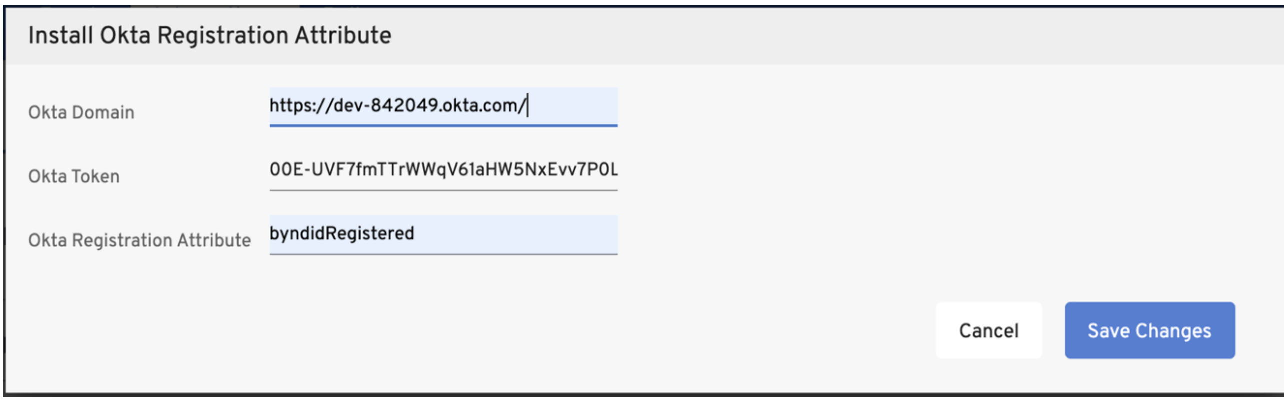
4. Click the **Integrations** tab, click **API Extensions**, and click **Install** for the Okta Registration Attribute.



Okta API Extensions

Okta Desktop Login Service	Install
Okta Event Hooks	Enabled Edit
Okta Registration Attribute	Install

5. Enter the following information for your tenant. Then click **Save Changes**.
   - Okta Domain
   - Okta API Token
   - Okta Registration Attribute Enter **byndidRegistered** or the value chosen by your organization mentioned earlier in this guide.



Install Okta Registration Attribute

Okta Domain	https://dev-842049.okta.com/
Okta Token	00E-UVF7fmTTrWWqV61aHW5NxEvv7P0L
Okta Registration Attribute	byndidRegistered

Step 3: Configure Beyond Identity as the Identity Provider

1. In the main Okta menu, select **Security > Identity Providers**.

2. In the Identity Providers tab, click **Add Identity Provider**.

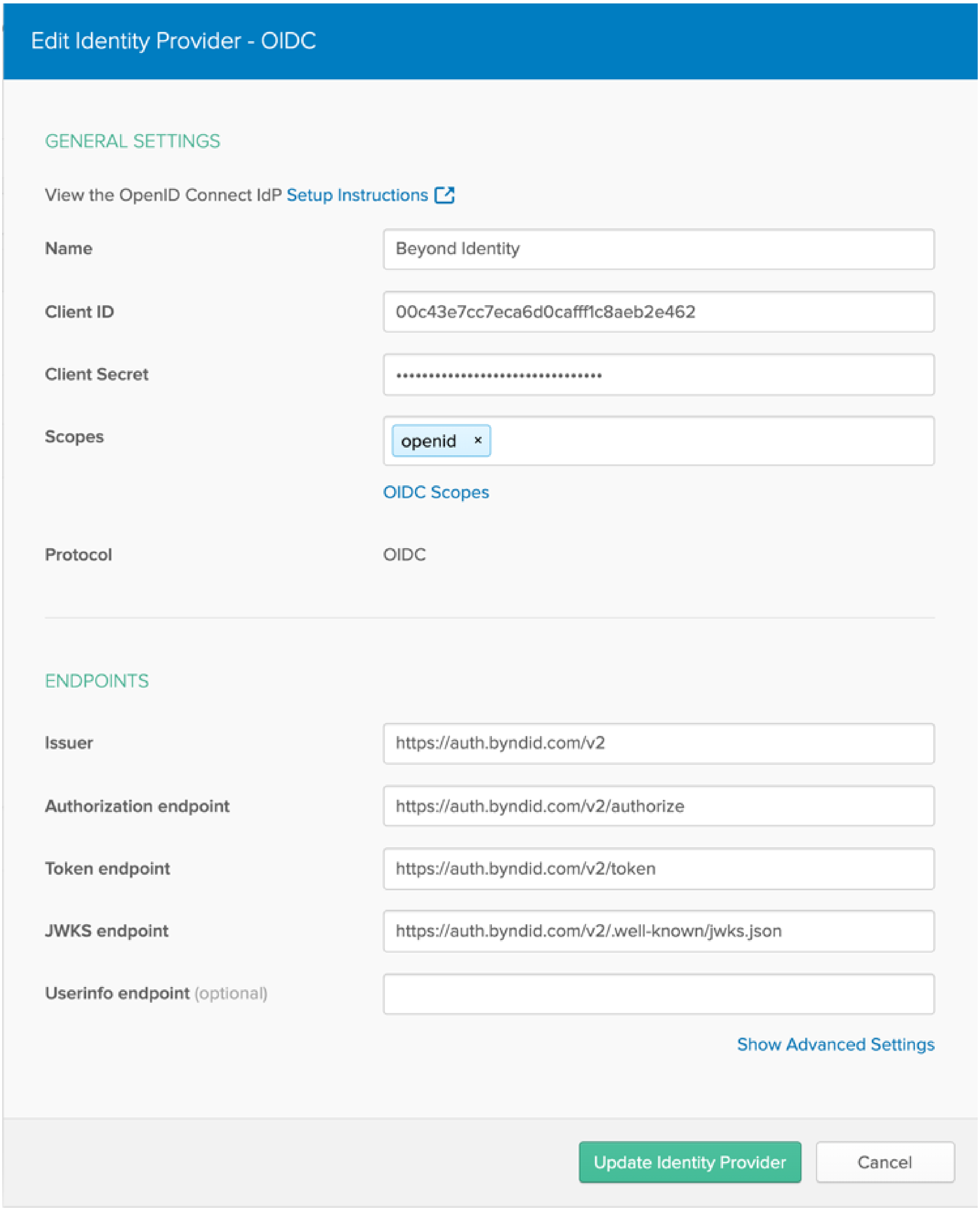
3. Select **Add OpenID Connect IdP**. **NOTE** This option will not be available in Okta until it's enabled or the ticket mentioned earlier gets resolved.

4. Enter the following information.
   - Name: **Beyond Identity**
   - Client ID: *From the Beyond Identity Admin Console*
   - Scopes: **openid**Remove any additional scopes listed.

- Issuer: **https://auth.byndid.com/v2**
- Authorization endpoint: **https://auth.byndid.com/v2/authorize**
- Token endpoint: **https://auth.byndid.com/v2/token**
- JWKS endpoint: **https://auth.byndid.com/v2/.well-known/jwks.json**

5. Click **Show Advanced Settings**, enter the following information, and click **Update Identity Provider**.

    - IdP Username: **idpuser.externalId**
    - Match Against: **Okta Username**
    - Account Link Policy: *Leave as the default option*
    - Auto-link: *Leave as the default option*
    - If no match is found: **Redirect to Okta Sign-in Page**



Edit Identity Provider - OIDC

GENERAL SETTINGS

View the OpenID Connect IdP Setup Instructions

Name: Beyond Identity

Client ID: 00c43e7cc7eca6d0cafff1c8aeb2e462

Client Secret: ••••••••••••••••••••••••••••••••

Scopes: openid ×

OIDC Scopes

Protocol: OIDC

ENDPOINTS

Issuer: https://auth.byndid.com/v2

Authorization endpoint: https://auth.byndid.com/v2/authorize

Token endpoint: https://auth.byndid.com/v2/token

JWKS endpoint: https://auth.byndid.com/v2/.well-known/jwks.json

Userinfo endpoint (optional):

6. (Optional) If you don't have SCIM cabability enabled, you can

Step 4: (Optional) Set up Event Hooks in Okta

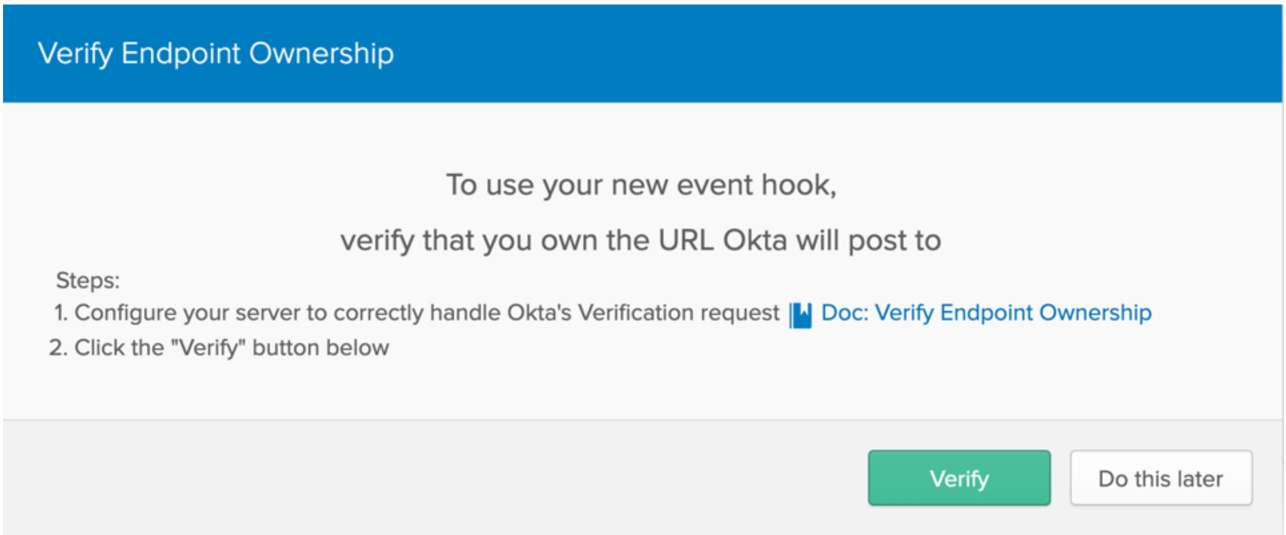
The Event Hooks configuration is only required if you do not have SCIM capability enabled for your Okta tenant due to licensing restrictions.

1. In Okta Admin Portal, Click on **Workflow > Event Hooks**.

2. Select **Create Event Hook** and update the following information. Then click **Verify**.

- Name: **Beyond Identity Provisioning flow**
- URL: **https://api.byndid.com/okta_events**
- Authentication field: **Authorization**
- Authentication Secret: *The Bearer token provided by the Beyond Identity*.
- Subscribe to events:
  - **User Added to Group**
  - **User Removed from Group**
  - **User suspended**
  - **User unsuspended**

3. Click **Save & Continue**. Then click **Verify**.



Verify Endpoint Ownership

To use your new event hook,

verify that you own the URL Okta will post to

Steps:
1. Configure your server to correctly handle Okta's Verification request Doc: Verify Endpoint Ownership
2. Click the "Verify" button below

Step 5: (Optional) Set up Event Hooks in Beyond Identity

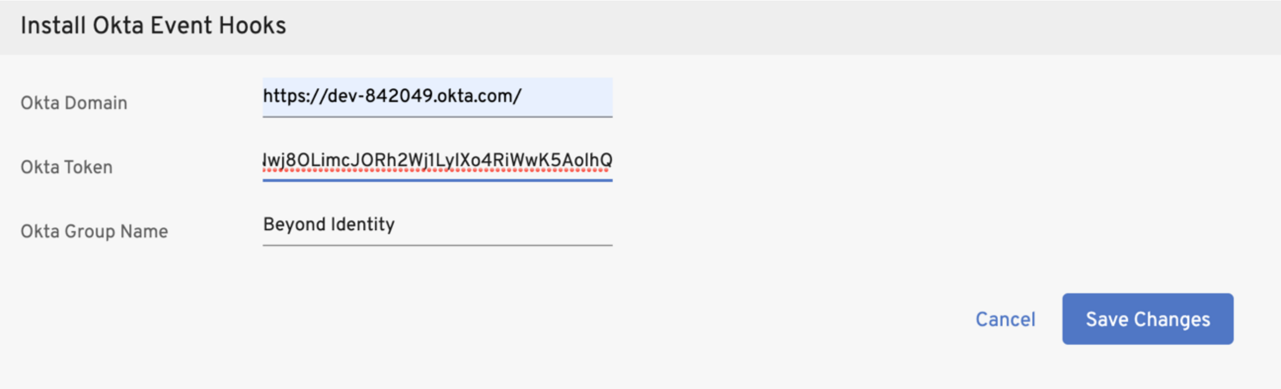
The Event Hooks configuration is only required if you do not have SCIM capability enabled for your Okta tenant due to licensing restrictions. Following changes are required in Beyond Identity Admin UI to enable Okta Event Hooks.

1. Click **Integrations > API Extensions**.

2. Enter the information for the Okta Domain and Okta API Token for your tenant.

3. Update the Okta Group Name to **Beyond Identity** or the value chosen by your organization.

4. Click **Save Changes**.



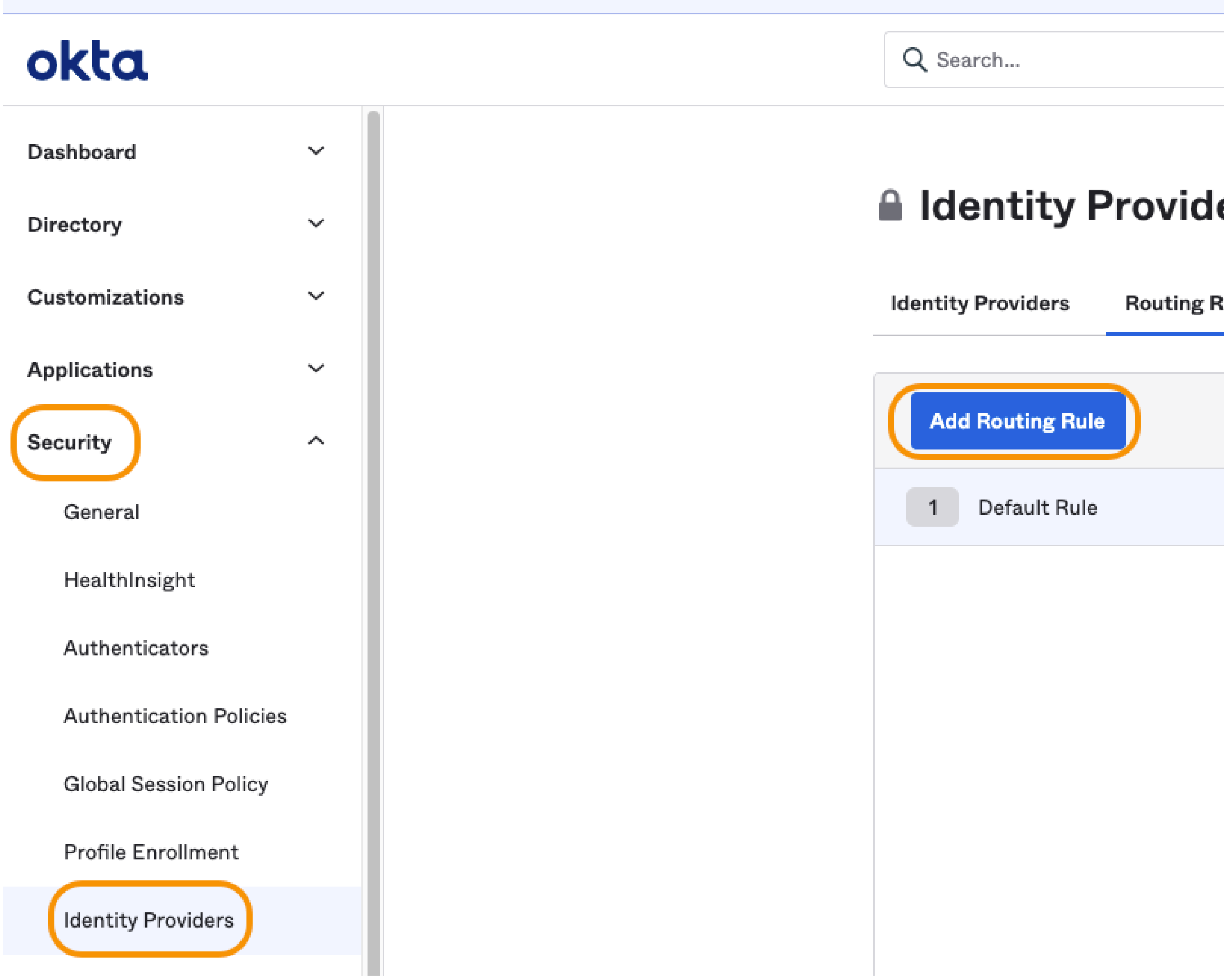
Install Okta Event Hooks

Okta Domain	https://dev-842049.okta.com/
Okta Token	lwj8OLimcJORh2Wj1LylXo4RiWwK5AolhQ
Okta Group Name	Beyond Identity

Step 11: Set up Routing Rules

-

1. Click **Security** > **Identity Providers** > **Routing Rules**.



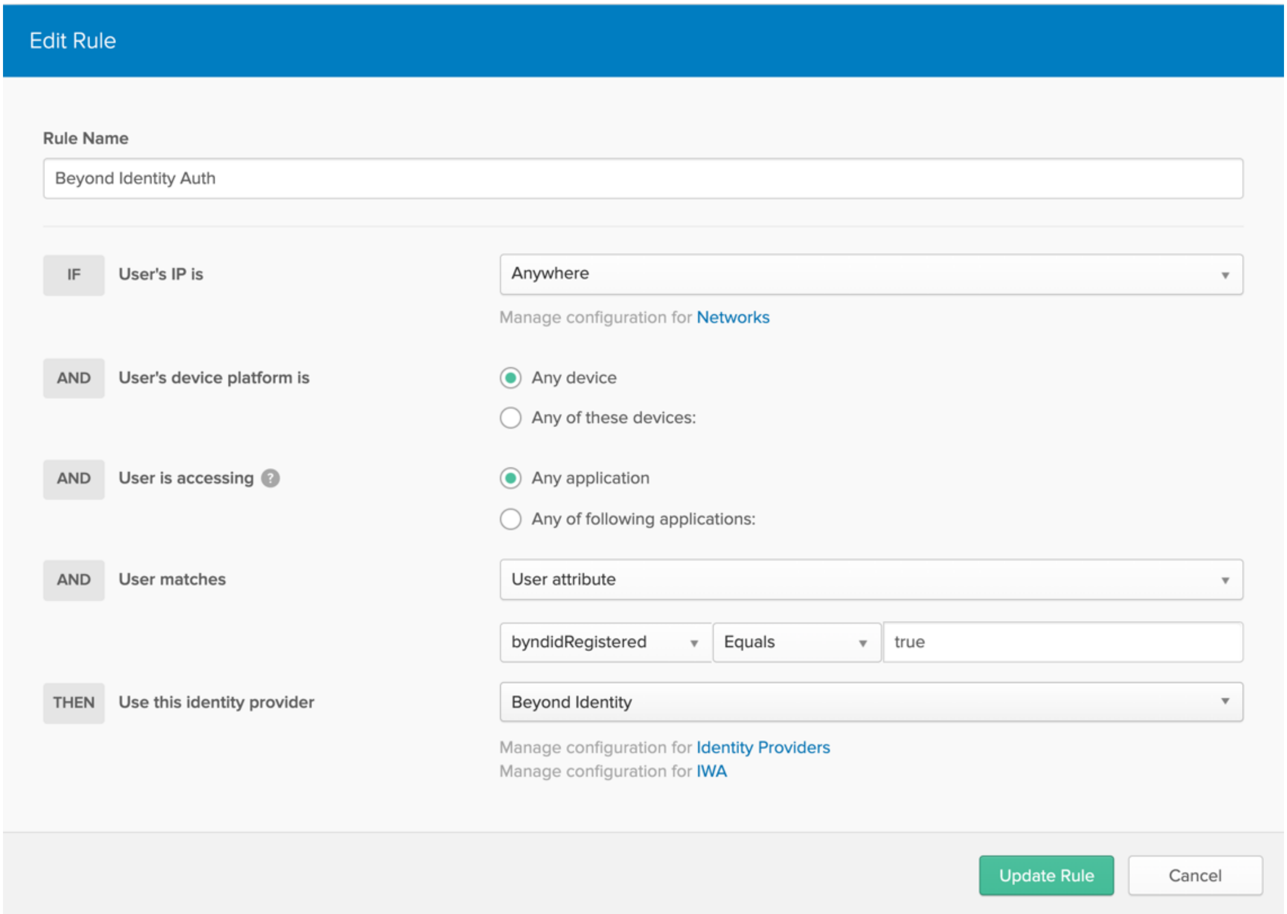
2. Click **Add Routing Rule** and set the following parameters:
   - Rule Name: **Beyond Identity Auth**
   - User IPs: *Leave blank*
   - Device Platform: *Leave blank*
   - Application: *Leave blank*

- User matches: **User Attributes**

  byndidRegistered Equals true NOTE These values are case sensitive, for example, **True** won't work but **true** will.

- Use this identity provider: **Beyond Identity**

3. Click **Save and Activate Rule** to set this as your first rule.



Edit Rule

Rule Name

Beyond Identity Auth

IF	User's IP is	Anywhere Manage configuration for Networks
AND	User's device platform is	● Any device ○ Any of these devices:
AND	User is accessing	● Any application ○ Any of following applications:
AND	User matches	User attribute byndidRegistered · Equals · true
THEN	Use this identity provider	Beyond Identity Manage configuration for Identity Providers Manage configuration for IWA

Set up Test Users

User Enrollment

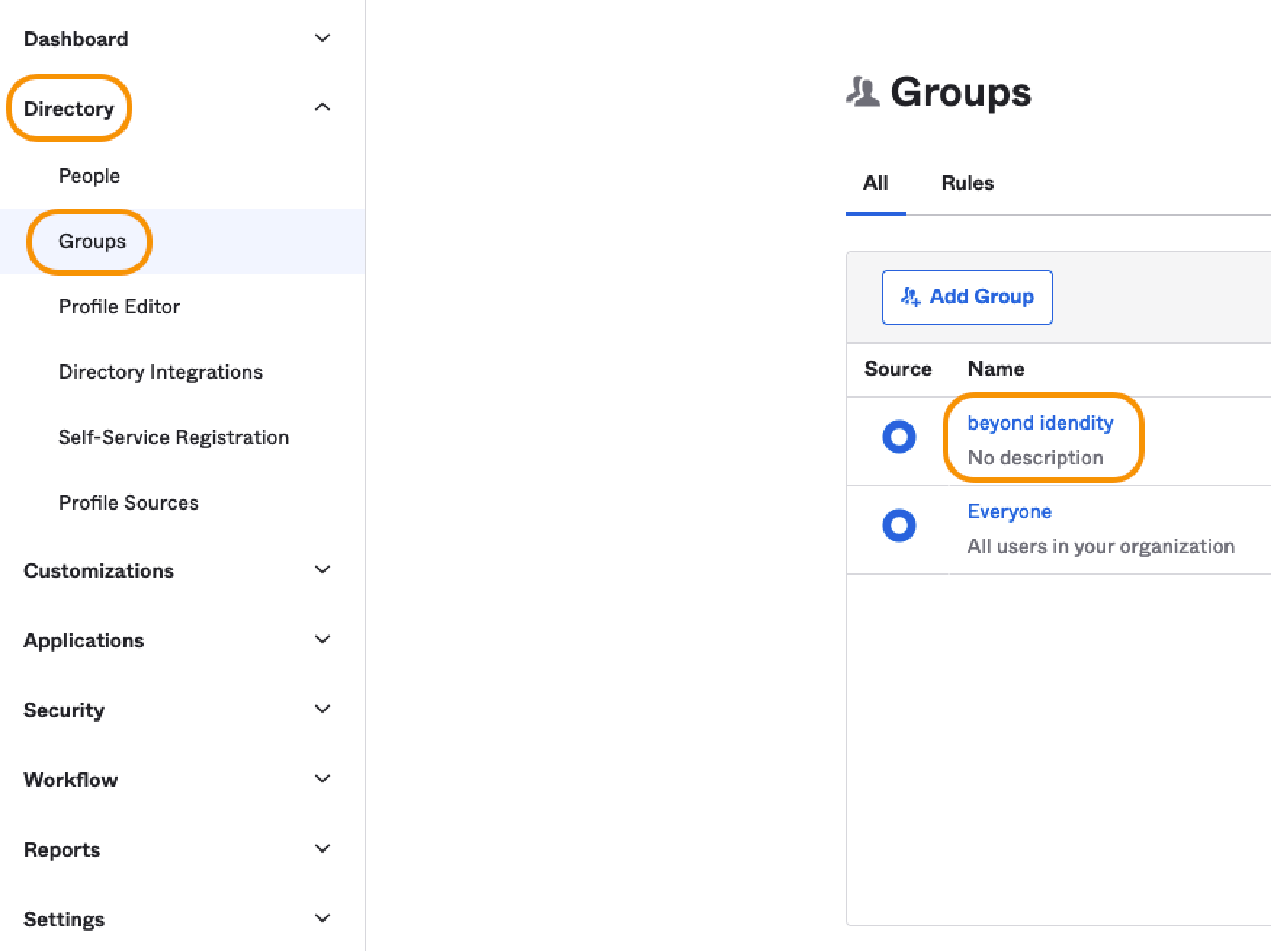
You'll enroll a user in the Beyond Identity experience by assigning them to the **Beyond Identity** group.

1. Click **Directory > Groups**.

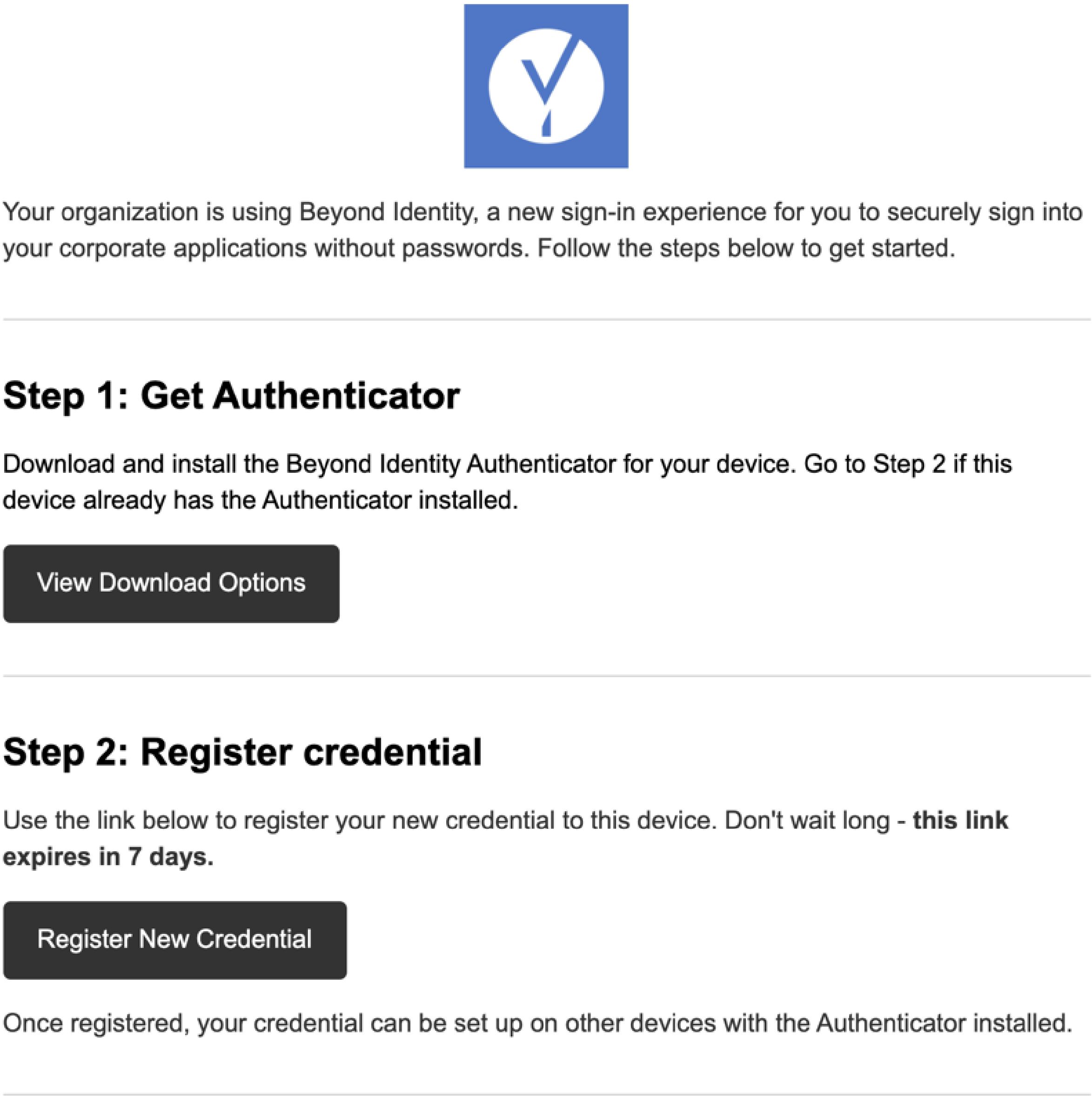
2. Select the **Beyond Identity** group.

3. Click **People Box** and click the user want to add to group.

4. Click **Assing People > Beyond identity User Portal**. Then click **Save**.



Enrolled users will receive an email from Beyond Identity welcoming them to the new Identity Provider.



Your organization is using Beyond Identity, a new sign-in experience for you to securely sign into your corporate applications without passwords. Follow the steps below to get started.

Step 1: Get Authenticator

Download and install the Beyond Identity Authenticator for your device. Go to Step 2 if this device already has the Authenticator installed.

Step 2: Register credential

Use the link below to register your new credential to this device. Don't wait long - **this link expires in 7 days.**

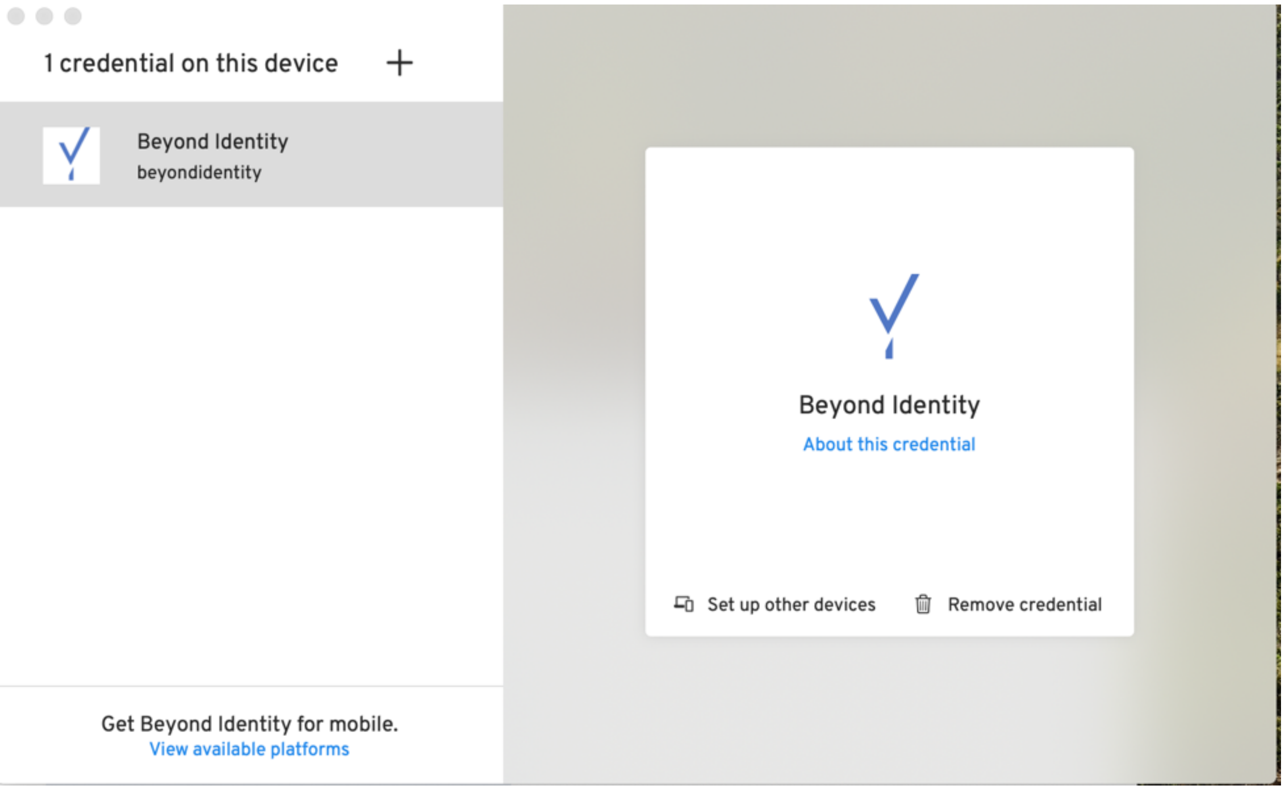
Once registered, your credential can be set up on other devices with the Authenticator installed.

Each enrolled user is prompted to follow the two steps below:

- **Step 1:** Download the Beyond Identity Authenticator to their device. When the user clicks **View Download Options**, the Beyond Identity Authenticator downloads page will open in a browser with all supported platforms displayed. The user should download and install the Beyond Identity Authenticator on their device if they still need to install it.

  Now that the user has the Authenticator installed on their device, they should proceed to Step 2, as there is yet to be a user credential associated with it.

- **Step 2:** Register their Credential in the Beyond Identity IdP. By clicking on Step 2 **Register New Credential**, the user's credential gets enrolled in the Beyond Identity service on the back end. On the front end, when users click Step 2, it takes them to the Beyond Identity Authenticator, where they will see the progress of their credential registration. Once completed, the user will see the credentials in the Authenticator.



1 credential on this device

Beyond Identity
beyondidentity

Beyond Identity
About this credential

Set up other devices
Remove credential

Get Beyond Identity for mobile.
View available platforms

User Authentication (Signing in) workflow

Each enrolled user can visit their Okta instance or any application supported by your SSO to sign into their corporate applications.

1. The Okta application or SSO-supported application will ask the user to enter their username.
2. Once the username is submitted, a prompt to use or open the Beyond Identity app for authentication will display for the user.
3. The user should click affirmatively on the prompt to be signed into their application without using a password. The Beyond Identity app, along with a success notification, displays. **NOTE** For iOS devices, some application sign-in processes will ask the user to exit the Beyond Identity Authenticator to return to their app after successful authentication.

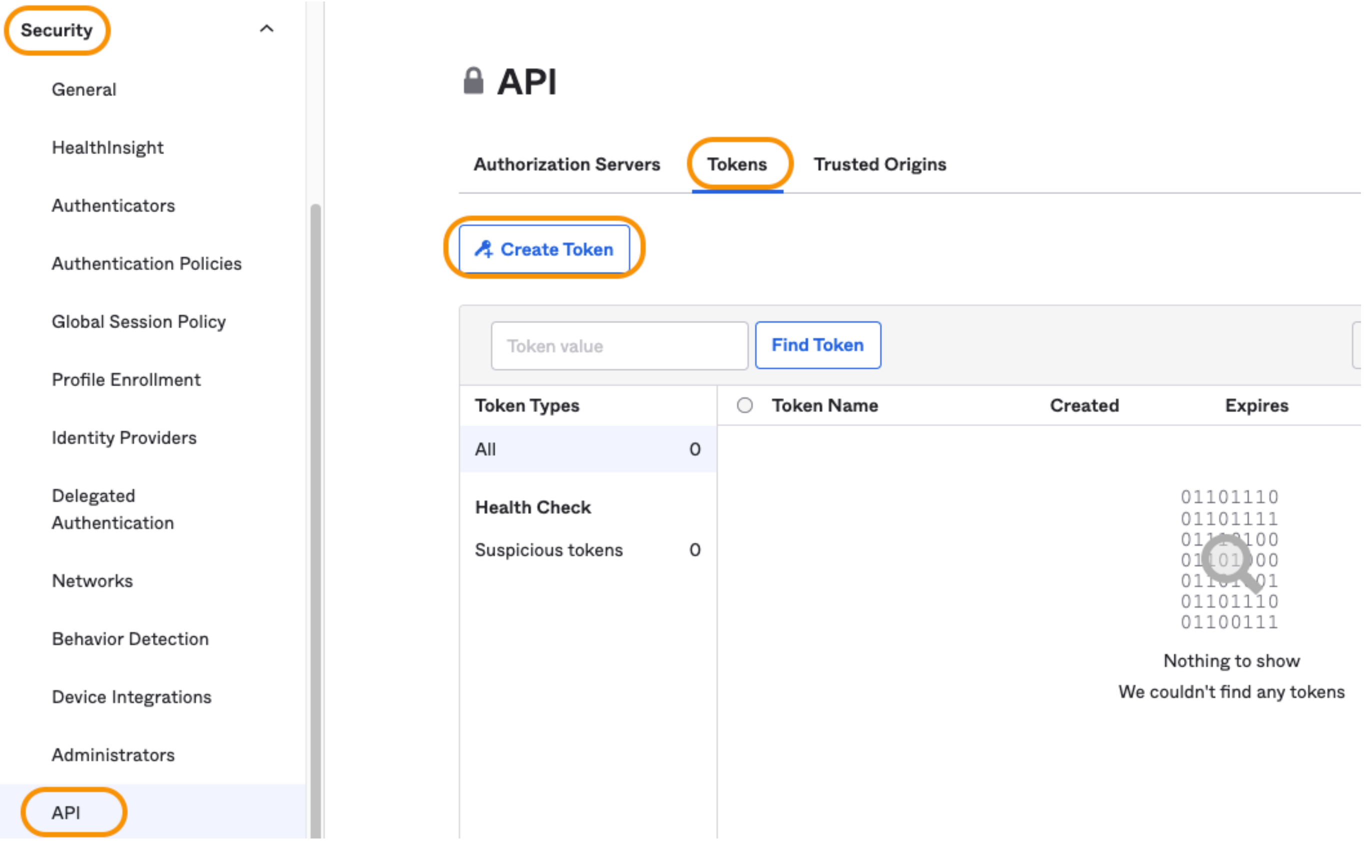
User Deprovisioning

You can de-provision a user from the Beyond Identity experience by removing them from the **Beyond Identity** group.

1. Click **Directory > Groups**.
2. Select the **Beyond Identity** group.
3. Click **Manage People** and, under the **Members** column, click the minus (-) next to the user you want to remove from the group.
4. Click **Save**.

Create a Token in Okta

The following image is an example of an administrator view in Okta and illustrates the actions listed below:



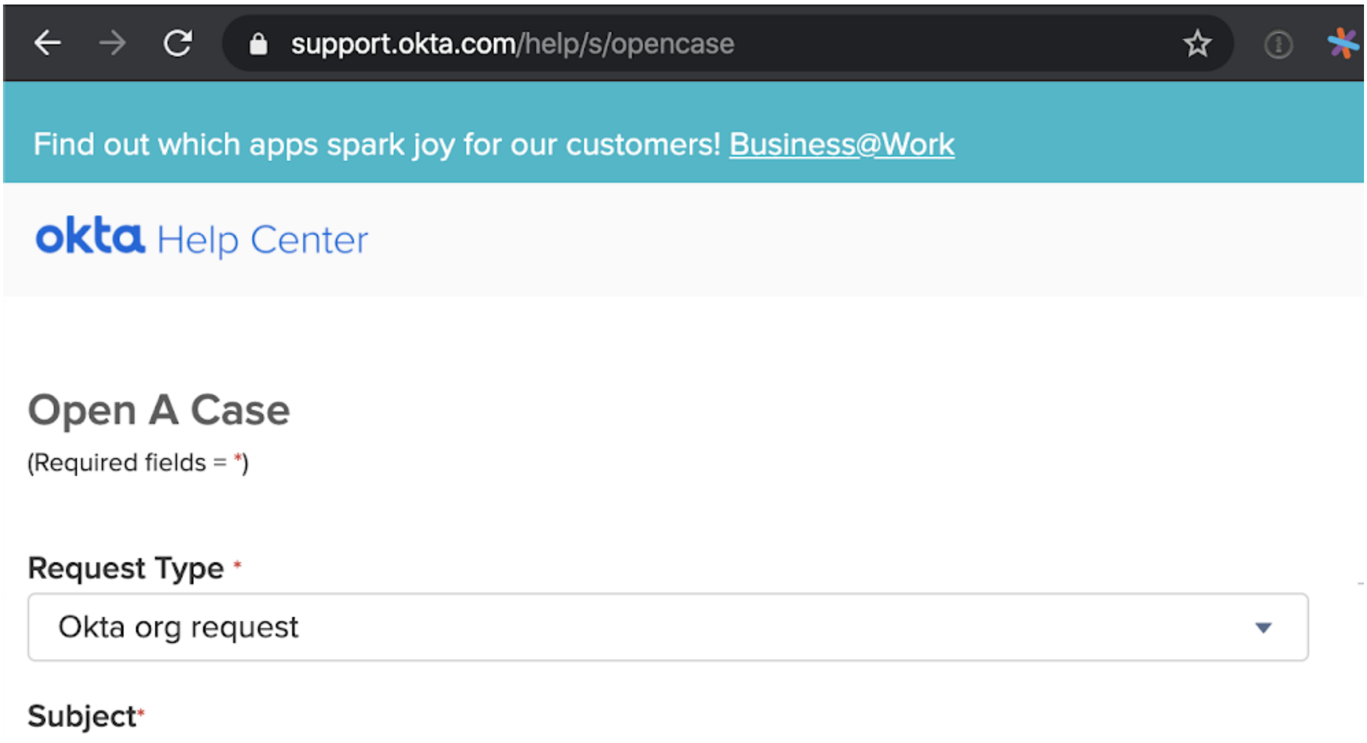
Nothing to show

We couldn't find any tokens

1. Sign into the Okta portal as an administrator.
2. In the main menu bar for Okta, select **Security**.
3. Select **API** from the **Security** drop-down list.
4. Select the **Tokens** tab, click **Create Token**, and enter the name for the token. For example, **Beyond Identity**.

Open a Ticket to Enable OpenID Connect IDP Connections in Okta

The following is an example of how to open a case with Okta requesting them to enable OpenID IDP Connections in Okta Sandbox and Production environments.


support.okta.com/help/s/opencase
Find out which apps spark joy for our customers! Business@Work
okta Help Center

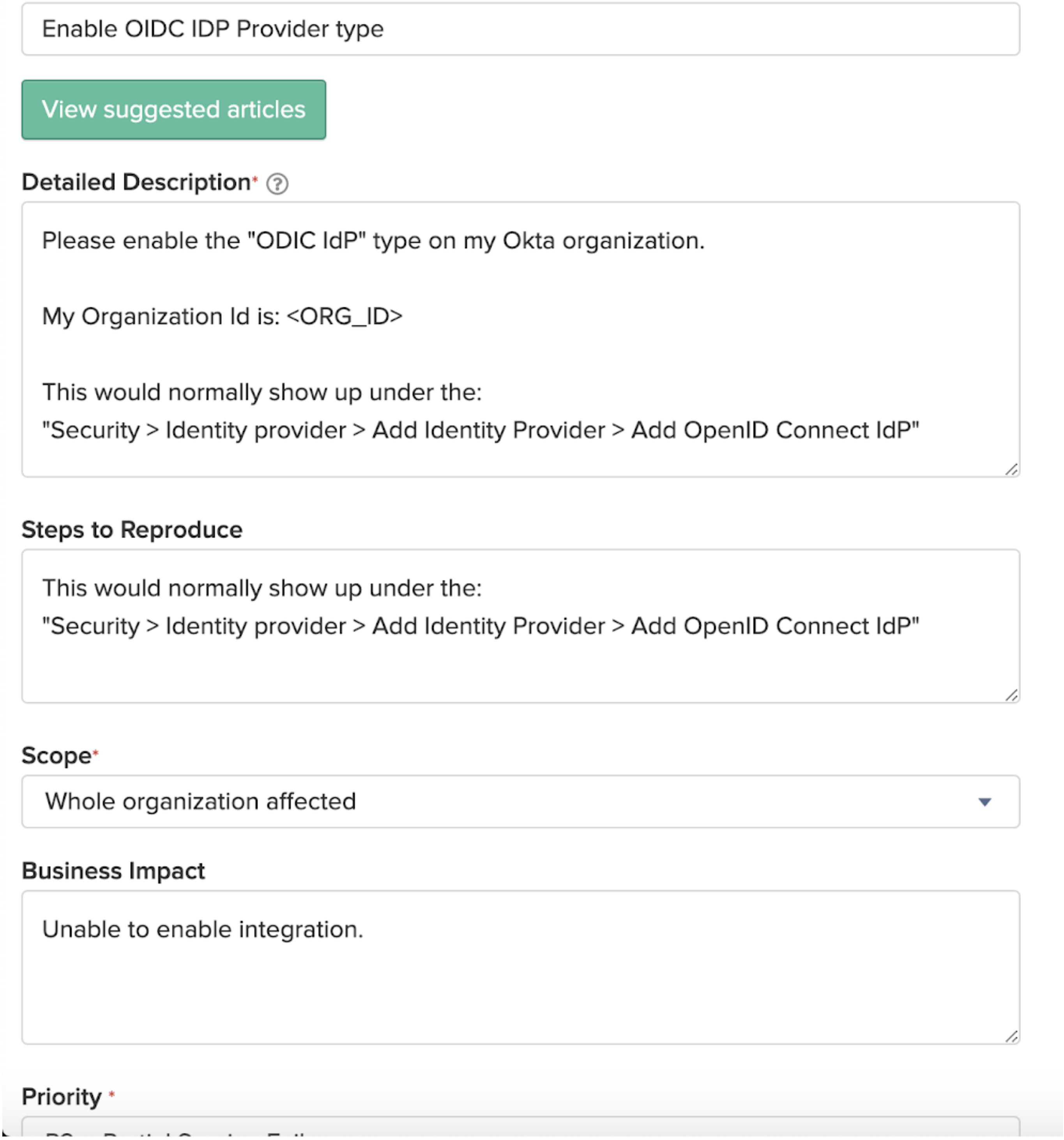
Open A Case

(Required fields = *)

Request Type *

Okta org request

Subject*



Enable OIDC IDP Provider type

Detailed Description*

Please enable the "ODIC IdP" type on my Okta organization.

My Organization Id is: <ORG_ID>

This would normally show up under the:
"Security > Identity provider > Add Identity Provider > Add OpenID Connect IdP"

Steps to Reproduce

This would normally show up under the:
"Security > Identity provider > Add Identity Provider > Add OpenID Connect IdP"

Scope*

Whole organization affected

Business Impact

Unable to enable integration.

Priority *

1. Navigate to Okta's Open Case Center.
2. Create a case with the following information:
   - Request Type: **Okta org request**
   - Subject: **Enable OIDC Provider Type**
   - Detailed Description: (see example below) *Please enable the "ODIC IdP" type on my Okta organization.*
     My Organization Id is: <ORG_ID>
     This would normally show up under:
     "Security > Identity provider > Add Identity Provider > Add OpenID Connect IdP"
   - Steps to reproduce: (see example below) *This would normally show up under:*
     "Security > Identity provider > Add Identity Provider > Add OpenID Connect IdP"
   - Scope: **Whole organization affected**

- Business impact: (see example below) *Unable to enable integration*
- Priority: **P3 - Non-critical issue**
- Okta org: Select from the list the organizations where Beyond Identity will be integrated.
- Case email: Your own email
- Phone number: Your phone number
- Add contact to team: <Can be left empty>
- Add attachment: <Not required>