

INTEGRATION GUIDE FOR AUTH0



INTRODUCTION

This guide provides information on how to:

- Set up Beyond Identity as a passwordless authentication solution for your Auth0 Workforce environment.
- Set up Auth0 to use Beyond Identity as an Identity Provider (Enterprise Connection).

PREREQUISITES

Ensure that you have an Auth0 account with admin privileges.

BEYOND IDENTITY CONFIGURATION

Information to provide to the Beyond Identity Field Team:

Your Company Name	
Your Auth0 tenant URL or configured custom domain. e.g. https://[your-domain].auth0.com The best way to find your full tenant URL is under Applications > click into any application > under Settings copy the 'Domain' field.	
Beyond Identity Admin Portal Application credentials SSO Client Id SSO Client Secret	
Beyond Identity User Portal Application credentials SSO Client Id SSO Client Secret	This will be updated by 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 will receive from the Beyond Identity Field Team

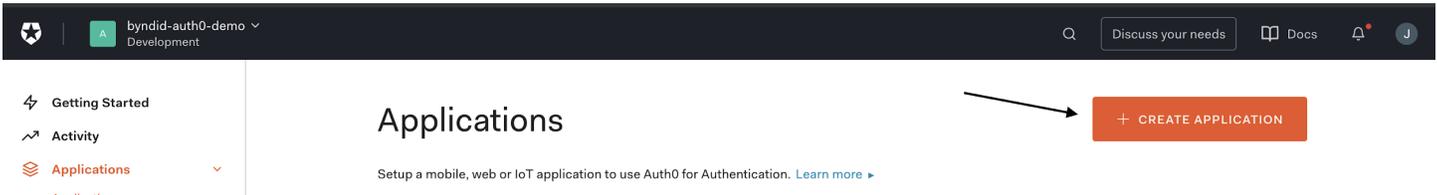
Beyond Identity IdP endpoint URLs:	
Issuer	https://auth.byndid.com/v2
Authorization endpoint	https://auth.byndid.com/v2/authorize
Token endpoint	https://auth.byndid.com/v2/token
JWKS endpoint	https://auth.byndid.com/v2/.well-known/jwks.json
(For Enterprise OIDC) Client ID	[From Beyond Identity Console]
(For Enterprise OIDC) Client Secret	[From Beyond Identity Console]
Beyond Identity Org ID	[From Beyond Identity SE]
Event Hook API Bearer Token	[From Beyond Identity SE]
SCIM API endpoint	https://api.byndid.com/scim/v2/Users https://api.byndid.com/scim/v2/Groups

AUTH0 CONFIGURATION

To configure Beyond Identity as the IdP in Auth0, follow the steps below. Once these steps are taken, you will be ready to enable Beyond Identity for test users.

Step 1: Setup Beyond Identity Admin Application in Auth0

1. Click on **Applications > Applications > Create Application**



2. Call the application “Beyond Identity Admin Portal”, Choose “Regular Web Application” and click ‘Save’

Create application [X]

Name *

Beyond Identity Admin Portal

You can change the application name later in the application settings.

Choose an application type

- Native**
Mobile, desktop, CLI and smart device apps running natively.
e.g.: iOS, Electron, Apple TV apps
- Single Page Web Applications**
A JavaScript front-end app that uses an API.
e.g.: Angular, React, Vue
- Regular Web Applications**
Traditional web app using redirects.
e.g.: Node.js, Express, ASP.NET, Java, PHP
- Machine to Machine Applications**
CLIs, daemons or services running on your backend.
e.g.: Shell script

CREATE **CANCEL**

3. In the ‘Settings’ Tab scroll down and record the “Domain” for your tenant and also record the “Client ID” and “Client Secret” assigned to Application. Beyond Identity team will collect and use those values to configure access into the Beyond Identity Admin Portal.



Beyond Identity Admin Portal

REGULAR WEB APPLICATION Client ID E8RyiyAWT9Yq9FA1nQI7rHwPeKRbVdM

Basic Information

Name *	<input type="text" value="Beyond Identity Admin Portal"/>	
Domain	<input type="text" value="byndid-auth0-demo.us.auth0.com"/>	
Client ID	<input type="text" value="E8RyiyAWT9Yq9FA1nQI7rHwPeKRbVdM"/>	
Client Secret	<input type="password" value="....."/>	

The Client Secret is not base64 encoded.

4. *Optional step* - Add the Beyond Identity logo to the “Application Logo” field:
“<https://byndid-public-assets.s3-us-west-2.amazonaws.com/logos/beyondidentity.png>”
5. Scroll down again to the Application URIs section and enter the following values:
 - a. Application Login URI = <https://admin.byndid.com/login>
 - b. Allowed Callback URLs = <https://admin.byndid.com/auth/callback>

Application URIs

Application Login URI	<input type="text" value="https://admin.byndid.com/login"/>
	<small>In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's /authorize endpoint. Learn more</small>
Allowed Callback URLs	<input type="text" value="https://admin.byndid.com/auth/callback"/>
	<small>After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (https://) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol https:// .</small>

6. Scroll all the way down and click ‘Save Changes’ - all the other settings should be left as default.

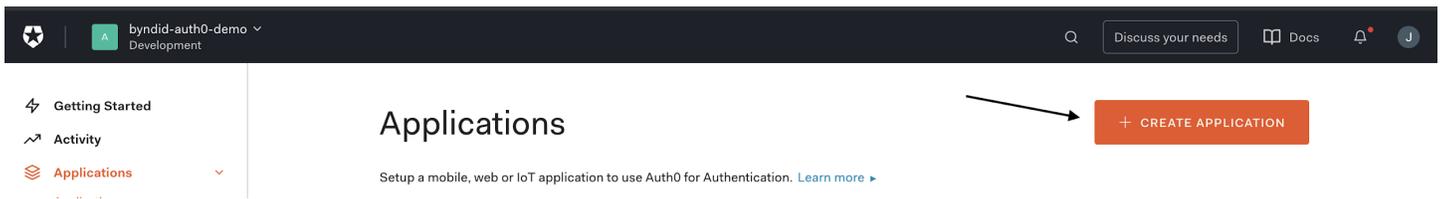
Step 2: Setup Admin Portal Access

1. Provide “Client ID” and “Client Secret” assigned to Admin Application in Auth0 (as per Step 1) to Beyond Identity SE. Beyond Identity team will collect and configure those values at the backend.

Step 3: Setup Beyond Identity User Portal Application in Auth0

prerequisites - you will require a beyond identity tenant name which will be provided by your beyond identity SE

1. Click on **Applications > Applications > Create Application**



2. Call the application “Beyond Identity User Portal”, Choose “Regular Web Application” and click ‘Save’

×

Create application

Name *

You can change the application name later in the application settings.

Choose an application type



Native

Mobile, desktop, CLI and smart device apps running natively.

e.g.: iOS, Electron, Apple TV apps



Single Page Web Applications

A JavaScript front-end app that uses an API.

e.g.: Angular, React, Vue



Regular Web Applications

Traditional web app using redirects.

e.g.: Node.js, Express, ASP.NET, Java, PHP



Machine to Machine Applications

CLIs, daemons or services running on your backend.

e.g.: Shell script

CREATE

CANCEL

- In the 'Settings' Tab scroll down and record the "Domain" for your tenant and also record the "Client ID" and "Client Secret" assigned to Application. These values will be needed in the next step to configure access into the Beyond Identity User Portal.

[← Back to Applications](#)



Beyond Identity User Portal

REGULAR WEB APPLICATION Client ID `cNSk3ztchTE6CS3Dha3thPs2q0IGdGPY`

[Quick Start](#) [Settings](#) [Addons](#) [Connections](#)

Basic Information

Name *	Beyond Identity User Portal	
Domain	byndid-auth0-demo.us.auth0.com	
Client ID	cNSk3ztchTE6CS3Dha3thPs2q0IGdGPY	
Client Secret	<div style="background-color: #eee; border: 1px solid #ccc; height: 1.2em; width: 100%; display: flex; align-items: center;"> </div>	 

The Client Secret is not base64 encoded.

4. *Optional step* - Add the Beyond Identity logo to the “Application Logo” field:

“<https://byndid-public-assets.s3-us-west-2.amazonaws.com/logos/beyondidentity.png>”
5. Scroll down again to the Application URIs section and enter the following values:
 - a. Application Login URI = https://user.byndid.com/auth-user/?org_id=<beyond-identity-tenant-name>
 - b. Allowed Callback URLs = <https://user.byndid.com/auth-user/callback>
6. Scroll all the way down and click ‘Save Changes’ - all the other settings should be left as default.

Step 4: Setup Beyond Identity User Portal Authentication

1. Once logged into Beyond Identity Admin UI, click on Account Settings.

The screenshot shows the 'Account Settings' page for 'Auth0 Beyond Identity Demo'. The 'USER ACTIVITY' section shows 0 active users, with 0 authentications (2 failed attempts) and 1 device added. The 'DEVICE ACTIVITY' section shows 1 active device. A table below lists device types and their OS platform and authenticator version distributions:

Device Type	OS Platform	Authenticator Version
1 DEVICE W/ PASSCODE SET	Android: 0%, macOS: 100%	2.28.0: 100%
1 DEVICE W/ BIOMETRICS SET	iOS: 0%, Windows: 0%, Unknown: 0%	
1 DEVICES W/ SECURE ENCLAVE		

2. Click on “User Portal” tab and click on Edit.

The screenshot shows the 'User Portal' configuration page. The 'User Portal' tab is selected, and the 'Edit' button is visible. The configuration fields are:

- SSO Issuer: <https://byndid-auth0-demo.us.auth0.com/>
- SSO Client ID: cN8a3ubnTEc530a3mPz3p0G6PY
- SSO Client Secret: *****

3. Update SSO Issuer, Client Id, and Client Secret fields from the previous step.

SSO Issuer is same as Auth0 domain URL.

SSO Client ID and SSO Client Secret is collected during Step 3.3

Edit User Portal Access	
SSO Issuer	<input type="text" value="https://byndid-auth0-demo.us.auth0.c"/>
SSO Client ID	<input type="text" value="cNSk3ztchTE6CS3Dha3thPs2q0IGdGI"/>
SSO Client Secret	<input type="text" value="u7_4AMbrqVklcpeH8Zogh5plT94QL0"/>

[Cancel](#) [Save Changes](#)

Step 5: Setup Beyond Identity Service for User Authentication:

1. Once logged into Beyond Identity Admin UI, click on “Integrations” tab and then click on OIDC Clients.
2. Click on “Add OIDC Client” and complete the following fields:
 - a. Name = “Auth0 SSO” or similar
 - b. Redirect URL = “<https://<auth0 domain>.auth0.com/login/callback>” - replacing <auth0 domain> with your Auth0 domain URL or configured custom domain.
For example - <https://byndid-auth0-demo.us.auth0.com/login/callback>
 - c. Leave Token Signing Algorithm and Auth Method as default
3. Click ‘Save Changes’

Add OIDC Client	
Name	<input type="text" value="Acme Corp. Auth0 SSO "/>
Redirect URIs	<input type="text" value="https://byndid-auth0-demo.us.auth0.com,"/>
Token Signing Algorithm	<input type="text" value="RS256"/>
Auth Method	<input type="text" value="client_secret_post"/>

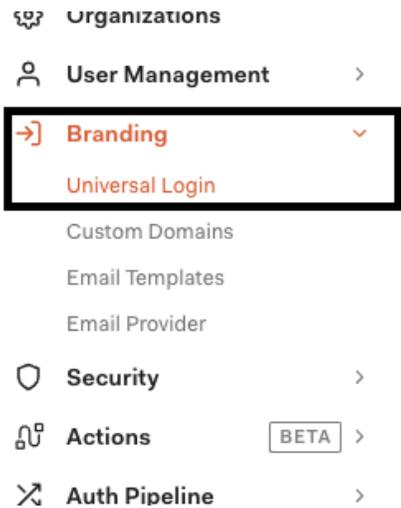
[Cancel](#) [Save Changes](#)

4. Click on the newly created OIDC Client configuration and write down Client ID and Client Secret Value (see below screenshot). You will be using these values in the next step.

Edit OIDC Client	
ID	d55db62d-b798-454f-a925-e83bc02fc7
Client ID	e4061fc404b29439778171afdd765b54
Client Secret	fb75df136c0a0c84c2e359cf8ee1347e
Name	Acme Corp. Auth0 SSO
Redirect URIs	https://byndid-auth0-demo.us.auth0.com,
Token Signing Algorithm	RS256 ▾
Auth Method	client_secret_post ▾
<div style="display: flex; justify-content: space-between; align-items: center;"> Delete OIDC Client Cancel Save Changes </div>	

Step 6: Enable New Login Experience required for OIDC connections

1. In the Auth0 Management Dashboard, on the left hand-navigation window click 'Branding' and then 'Universal Login' on the expanded sub-menu.



2. In the 'Settings' tab - Select the 'New' Experience.

Universal Login

Create a beautiful universal login page where you can redirect to authenticate your users. [Learn more](#) ▶

[Settings](#) [Login](#) [Password Reset](#) [Multi-factor Authentication](#)

Settings

Experience

The default look and feel for your Universal Login pages. [Learn more](#).

New

New and improved visuals, flows, and functionality enhancing your end user experience.

- ✓ Lightweight and faster
- ✓ No JavaScript required

[Learn More](#) →

Classic

Our existing experience with the look and feel you and your users are familiar with.

- ✓ Based on Lock.js and other JavaScript libraries
- ✓ More comprehensive set of features

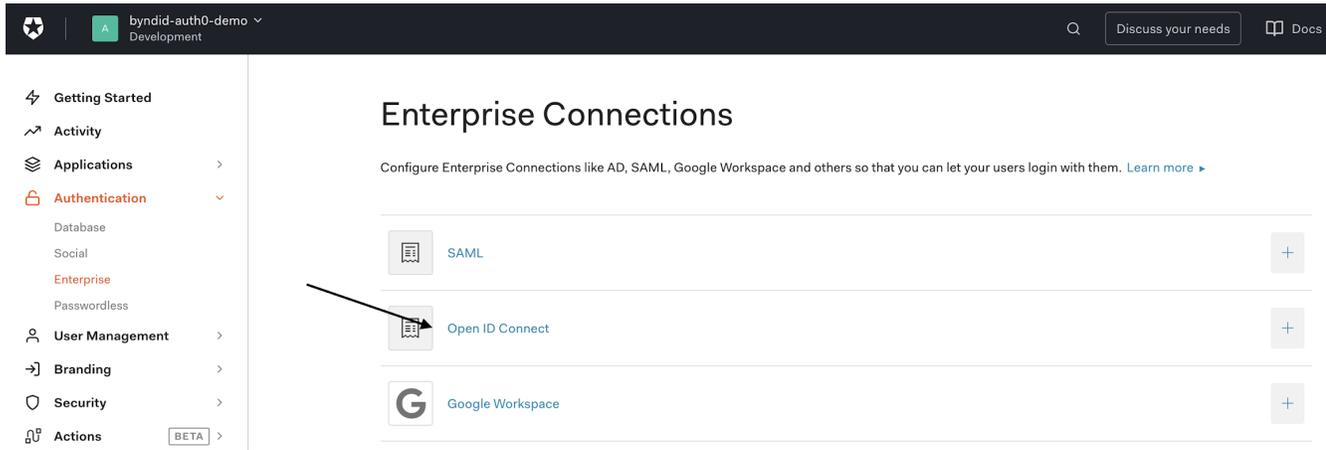
[Learn More](#) →

Please note that the New Universal Login Experience is not yet at feature parity with the Classic Experience. [Learn more](#).

3. Scroll down and click 'Save Changes'

Step 7: Configure Beyond Identity as the Identity Provider in Auth0

1. On the left navigation pane click 'Authentication', the menu will expand, then click 'Enterprise'
2. On the Enterprise Connections page - Click 'Open ID Connect'



3. Then within the Open ID Connect menu click 'Create Connection'
4. Enter the following values:
 - a. Connection Name: "Beyond-Identity"
 - b. Issuer URL: "https://auth.byndid.com/v2"
 - c. Client ID: From Step 5.4
 - d. Client Secret: From Step 5.4



New Open ID Connect Connection

Connection name *

Beyond Identity

This is a logical identifier of the connection. This name cannot be changed.

Issuer URL *

https://auth.byndid.com/v2

Enter the URL of the discovery document of the OpenID Connect provider you want to connect with.

Client ID *

2rHlg2ea4Zo6KI51VaAnhsP1TLisTppIUT

Obtaining the Client ID differs across providers. Please check your provider's documentation.

Client Secret

Dc6BIFEdffHyspbncvaUffffl2DI73HWHqu5dFOwYONh9j2alcrxozk6oy1YRR

Based on the settings provided, we'll use the Authorization Code Flow to connect to the IdP which requires a client secret.

Callback URL

You may need to configure the OIDC Issuer with this callback URL:
https://byndid-auth0-demo.us.auth0.com/login/callback

Advanced

Sync user profile attributes at each login



ENABLED

CREATE

5. Click 'Create'

6. On the 'Settings Tab' under 'Issuer URL' click 'Show Issuer Details' and complete with the following values:

Beyond Identity IdP endpoint URLs:	
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

Advanced Settings

Issuer	<input type="text" value="https://auth.byndid.com/v2"/>
Authorization Endpoint	<input type="text" value="https://auth.byndid.com/v2/authorize"/>
Token Endpoint	<input type="text" value="https://auth.byndid.com/v2/token"/>
JWKS URL	<input type="text" value="https://auth.byndid.com/v2/well-known/jwks.json"/>

7. Scroll down to ‘Scopes’ and enter “**openid**”

Scopes	<input type="text" value="openid"/>
--------	-------------------------------------

List of scopes to request from the Issuer. Must contain at least openid and be separated by a space.

Callback URL	You may need to configure the OIDC Issuer with this callback URL: <input type="text" value="https://byndid-auth0-demo.us.auth0.com/login/callback"/>
--------------	---------------------------------------------------------------------------------------------------------------------------------------------------------

Advanced

Sync user profile attributes at each login ENABLED

[SAVE CHANGES](#)

8. Click “Save Changes”

9. Now scroll back up and click on the next tab along ‘Login Experience’

[← Back to Open ID Connect](#)



Beyond Identity

OPEN ID CONNECT Identifier `con_JenciSj3iQQSA2i1`

[Settings](#) [Login Experience](#) [Applications](#)

10. Under this tab, find the section called ‘Connection button’ and check (enable) the checkbox field labelled ‘Display connection as a button’

11. Enter the ‘Button display name’ as “Beyond Identity”

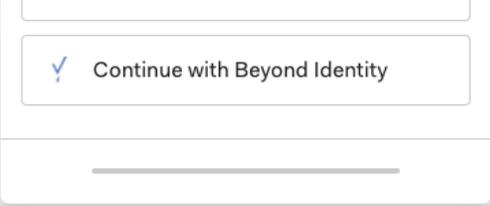
12. Add the following url for the ‘Button Logo URL’ -

<https://byndid-public-assets.s3-us-west-2.amazonaws.com/logos/beyondidentity.png>

Connection button

If you want to display a button for this connection in the login page, you can configure the display name and the logo URL.

Display connection as a button



ⓘ Your connection button preview

Button display name

Beyond Identity

Button logo URL

<https://byndid-public-assets.s3-us-west-2.amazonaws.com/logos/beyondidentity.png>

Image will be displayed as a 20x20px square.

SAVE

13. Scroll down and click ‘Save’

Step 8: Enable the Beyond Identity Connection in Auth0

1. Lastly, on the Applications tab within the OIDC connection - enable this connection for the Beyond Identity Admin and User portal applications which were created in Step 1 and 3.

[← Back to Open ID Connect](#)



Beyond Identity

OPEN ID CONNECT Identifier con_1JEtTIXnbqRUMpZ3

[Settings](#) [Login Experience](#) [Applications](#)

Applications using this connection.

	auth0-sso-dashboard GENERIC	<input type="checkbox"/>
	Beyond Identity Admin UI Login REGULAR WEB APPLICATION	<input checked="" type="checkbox"/>
	Beyond Identity User Portal UI Login REGULAR WEB APPLICATION	<input checked="" type="checkbox"/>

Step 9: Check Auth0 callback URL is correct in Beyond Identity OIDC integration

1. In the Auth0 management dashboard, under the 'Settings' tab of the Beyond Identity OIDC connection just created in Step 7, make a note of the 'Callback URL' as below.

Callback URL You may need to configure the OIDC Issuer with this callback URL:
`https://byndid-auth0-demo.us.auth0.com/login/callback`

2. In Beyond Identity Admin UI, click on "Integrations" tab and then click on OIDC Clients. Find the OIDC client created in Step 5 and click 'Edit'.
3. Ensure that the 'Redirect URI' value matches with the value in Auth0 connection (Step 9.1). If the values do not match, update the value with the Callback URL extracted in Step 9.1 and Save Changes.

Edit OIDC Client

ID dc65470b-0b7d-4db8-86a6-3a06801173c

Client ID 2ce433ada7684812e32817ab12a10a2a

Client Secret c5302413d1bb75d9876df7c19834cia4

Name Auth0 OIDC connection

Redirect URIs <https://byndid-auth0-demo.us.auth0.com>,

Token Signing Algorithm RS256 ▼

Auth Method client_secret_post ▼

Delete OIDC Client

Cancel

Save Changes

Setting up test users

User Provisioning

Before your users can start authenticating with Beyond Identity, they need to be provisioned in the Beyond Identity Directory. As Auth0 does not support SCIM, users need to manually provisioned using the Beyond Identity admin portal or using the Beyond Identity REST API. Please see admin portal video tutorial here which shows navigating to the directory area of the admin portal - <https://www.beyondidentity.com/resources/beyond-identity-admin-console-overview>

1. In the Admin portal under the 'Directory' tab click Add User'
2. Enter the following values:
 - a. External ID: `oidc|Beyond-Identity|<email_address>`
 - b. Email: `<email_address>`
 - c. Username: `<email_address>`
 - d. Display Name: `<Full Name>`
3. Click ' Save Changes'
4. The user will now be sent a welcome email to the email address supplied above. See User Enrollment section.

Note: The External ID format above must be adhered to as this will be the user ID of the user in Auth0.

User Enrollment

1. Enrolled (provisioned) user will receive an email from Beyond Identity welcoming them to the new Identity Provider.
 - a. See image below for reference:



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.

[View Download Options](#)

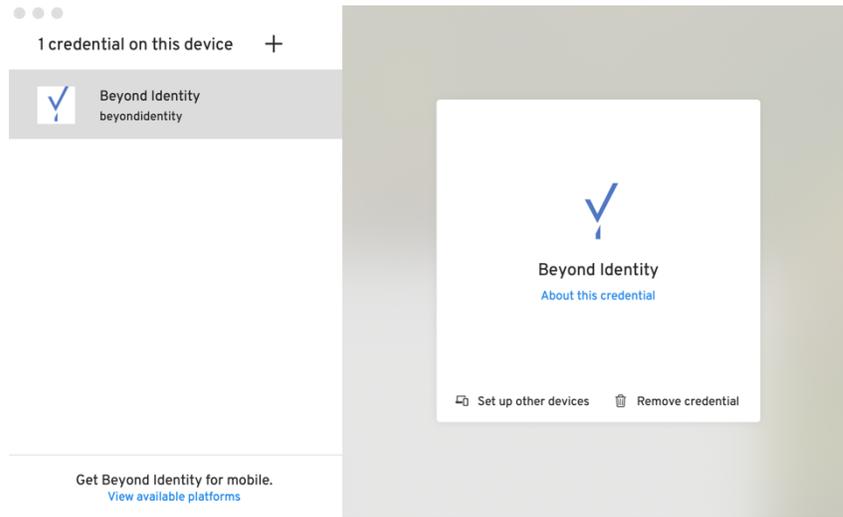
Step 2: Register credential

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

[Register New Credential](#)

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

2. Each enrolled user will be asked to follow the two steps below:
 - a. Step 1: Download the Beyond Identity Authenticator to their device.
 - i. 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 have not already.
 - ii. Now that the user has the Authenticator installed on their device, they should proceed to Step 2 as there is not yet a user credential associated with the Authenticator on that device.
 - b. Step 2: Register their Credential in the Beyond Identity IdP.
 - i. By clicking on Step 2 “**Register New Credential**”, the user’s credential will get enrolled in the Beyond Identity service on the back end. On the front end, users who click Step 2 will be taken to the Beyond Identity Authenticator where they will see the progress of their credential registration. Once completed, the user will see a credentials in the Authenticator.
 - ii. See example image below:



User Authentication (Signing in)

1. Each enrolled user can visit any application supported by the SSO to passwordlessly sign into the corporate applications.
2. The SSO-supported application will ask the user to enter their username.
3. Once the username is submitted, a prompt to use or open the Beyond Identity app for authentication will display for the user.
4. The user should click affirmatively on the prompt to be signed into their application, without the use of a password. The Beyond Identity app along with a success notification will display.
 - a. Note: For iOS devices, some application sign-in processes will ask the user to exit out of the Beyond Identity Authenticator to return to their app after successful authentication.

User Deprovisioning

To deprovision a user from the Beyond Identity experience, manually delete users from Beyond Identity Admin Portal.