Connect Okta Sign-in and Youverse Face Authentication

How to add a second-factor to Okta log in with Youverse face authentication

Youverse

Overview

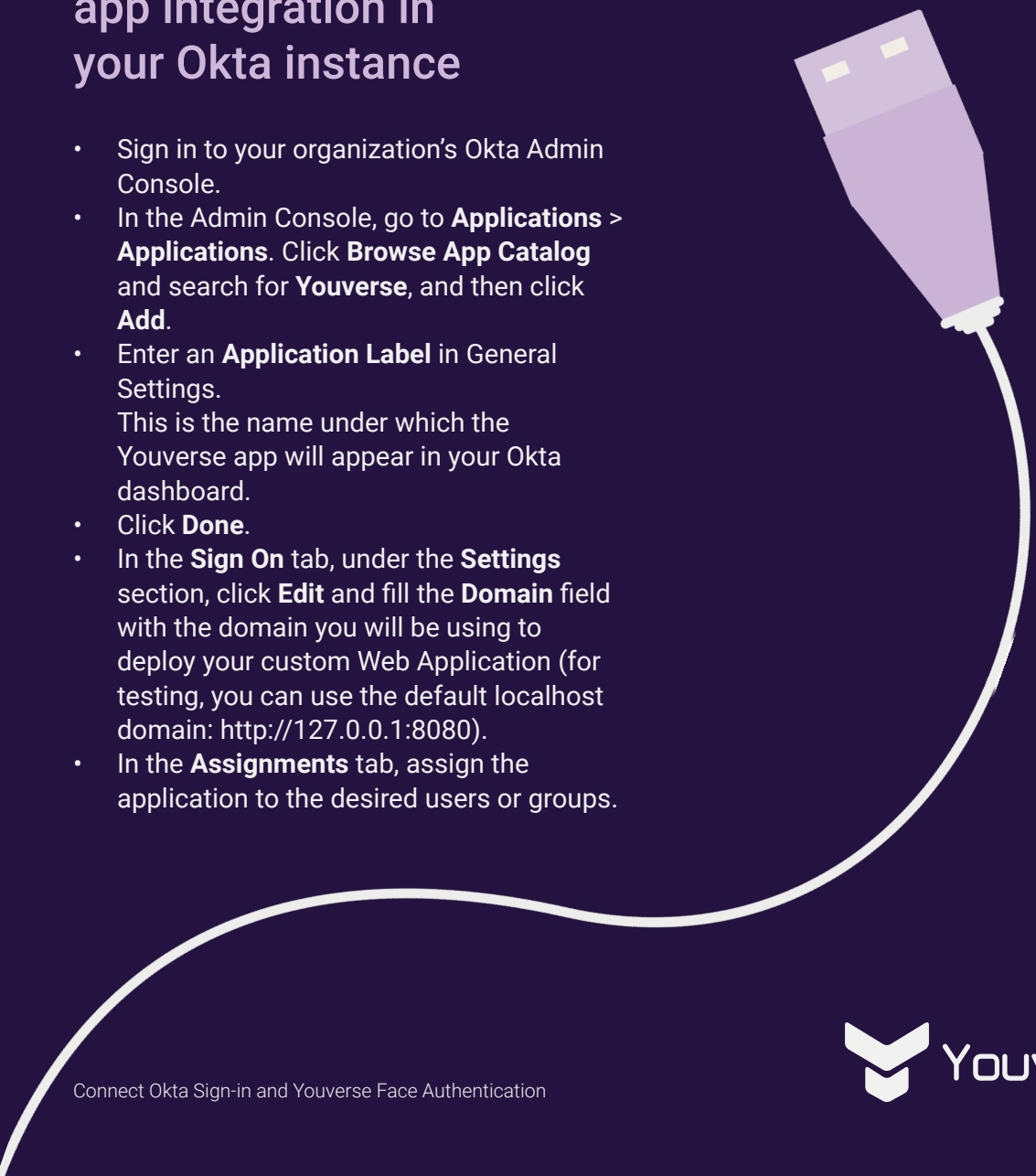
The integration guide will help you configure a custom Web Application using the Okta Sign-in Widget and Youverse Face Authentication APIs to demonstrate how to add a second-factor authentication to an Okta login flow, enhancing security and privacy while providing a seamless user experience.

Ready? Follow the steps.

Prerequisites

- An Okta account.
- A Youverse account. If you do not already have one, you can sign up here. To get a free trial license please e-mail us at support@youverse.me.
- A Python developer enviroment.

Install the Youverse app integration in your Okta instance



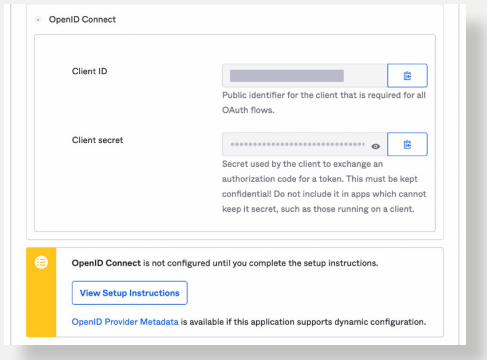
- Sign in to your organization's Okta Admin Console.
- In the Admin Console, go to **Applications** > **Applications**. Click **Browse App Catalog** and search for **Youverse**, and then click **Add**.
- Enter an **Application Label** in General Settings.
  This is the name under which the Youverse app will appear in your Okta dashboard.
- Click **Done**.
- In the **Sign On** tab, under the **Settings** section, click **Edit** and fill the **Domain** field with the domain you will be using to deploy your custom Web Application (for testing, you can use the default localhost domain: http://127.0.0.1:8080).
- In the **Assignments** tab, assign the application to the desired users or groups.

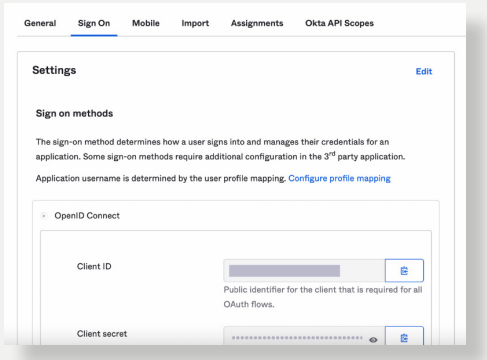
Youverse

Configure the Web Application

The following steps cover the configuration and deployment of a sample application that enables you to test your Youverse and Okta integration.

- Clone the example application repository from GitHub integration to a local folder on your system.
- Open a terminal and change to the base directory where you cloned the repository.
- Then install dependencies:
  $ pip install -r requirements.txt
- Copy the *client_secrets.json.dist* to *client_secrets.json*:
  $ cp *client_secrets.json.dist client_secrets.json*
- You now need to gather the following information from the Okta Admin Console:
  - **Client ID** and **Client Secret** - These can be found on the **Sign On** tab of the Youverse app integration that you installed earlier in the Okta Admin Console.
  - **Open ID Connect URLs** - These are the **authorization_endpoint**, **token_endpoint** and **userinfo_endpoint** for your Okta domain that can be found by clicking on **OpenID Provider Metadata** link under the **Sign On** tab.
- Additionaly you need to gather the **Youverse API URL Youverse** and **API Key** from your Youverse account dashboard (or contact support@youverse.me).
- Fill the information that you gathered in the *client_secrets.json* file.





Youverse

If you set a custom domain for this app in the Sign On tab in Okta Admin Console (different than http://127.0.0.1:8080), please update the “redirect_uri” in *client_secrets.json* accordingly.

You are now ready to start testing your new app with Okta login and Youverse Face Authentication as a second-factor!

Test the Web Application

- Launch the app server from a terminal window: *$ python main.py*.
- Now navigate to http://127.0.0.1:8080 in your browser. If you see a home page that prompts you to log in, then things are working.
- Clicking the **Log in** button will redirect you to the Okta hosted sign-in page. Enter the credentials of a valid Okta account and proceed.
- Then a new screen will be displayed to perform the second-factor authentication with Youverse. Just look at your webcam and click the take selfie button.
- After the face authentication, you are logged in to the application.

Additional resources

Okta Hosted Login + Youverse Face Authentication example on Github. Subscribe Youverse Face Authentication here. Choose the Web Plan.

Troubleshooting

If you find any issues or need help with the setup please contact us or join us at our discord community.

Youverse