

Dremio Cloud V

On this page

Okta

Overview

This topic describes how to configure Okta as an enterprise identity provider (IdP).

To configure Okta as an enterprise IdP, you must register <u>Dremio as an application in the Okta organization</u> and <u>add Okta as a provider in Dremio</u>. Once that is done, you may configure <u>Okta to use SCIM</u> for secure user provisioning.

Prerequisites

- Your SCIM API service must be connected to Okta
- To register Dremio as an application in the Okta portal, you must be an Okta administrator, or possess explicit permissions to register an application in Okta.
- You must also be a Dremio admin to configure an enterprise IdP
- To configure Okta as an IdP, you will need items as described from the Okta application and security-API section:
 - Client ID
 - Client Secret
 - Issuer URL

Requirements

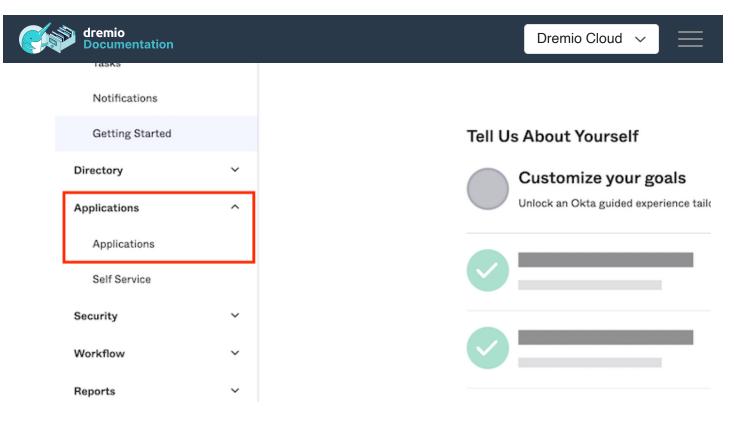
Version: SCIM 2.0+

Okta Configuration

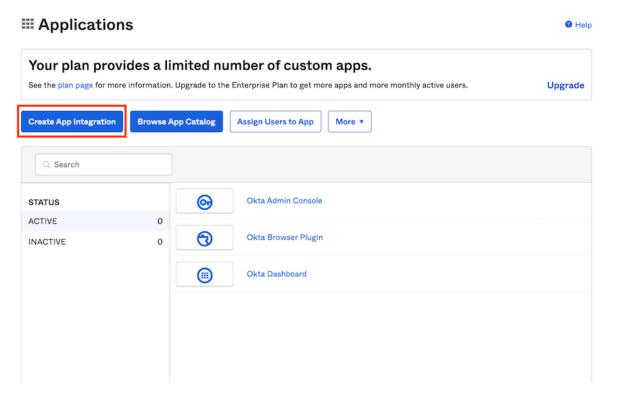
In the Okta organization, perform the following steps to register an Okta application:

1. Using the left navigation menu, go to **Applications** > **Applications**.





2. On the **Applications** page, click **Create App Integration**.



3. From the Create a new app integration page, select OIDC - OpenID Connect under Signin method.



Dremio Cloud ~



Sign-in method

Learn More 🖸



Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

O SAML 2.0

XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

O SWA - Secure Web Authentication

Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

O API Services

Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

Web Application

Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

Single-Page Application

Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

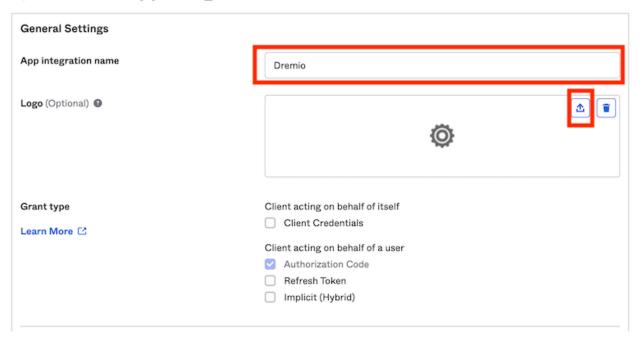
Native Application

Desktop or mobile applications that run natively on a device and redirect users

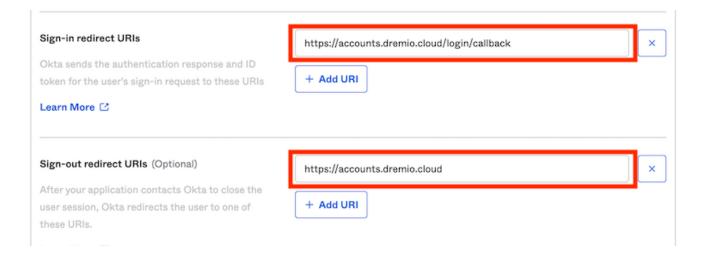


- 4. For the **Application type**, select **Web Application**.
- 5. Click Next.
- 6. From the **New Web App Integration** page, enter a value for **App integration name**.

New Web App Integration

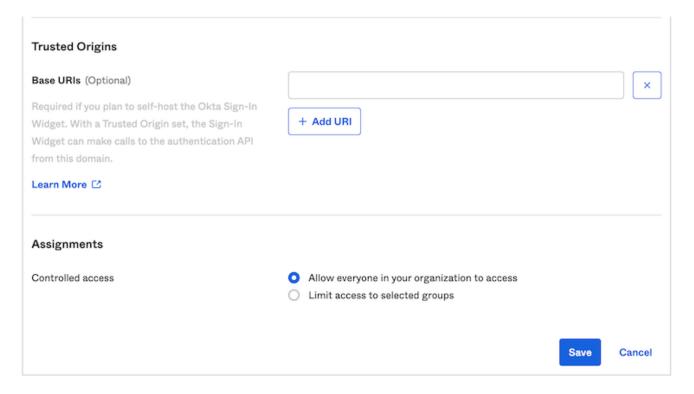


- 7. (Optional) For Logo, upload a logo using the Upload icon.
- 8. For **Grant type**, under **Client acting on behalf of a user**, check the **Authorization Code** box.
- Under Sign-in redirect URIs, enter https://accounts.dremio.cloud/login/callback to specify each sign-in redirect URI for your application. This overwrites the default local sign-in redirect URI. This URL can also be retrieved from the Dremio Add Provider dialog.





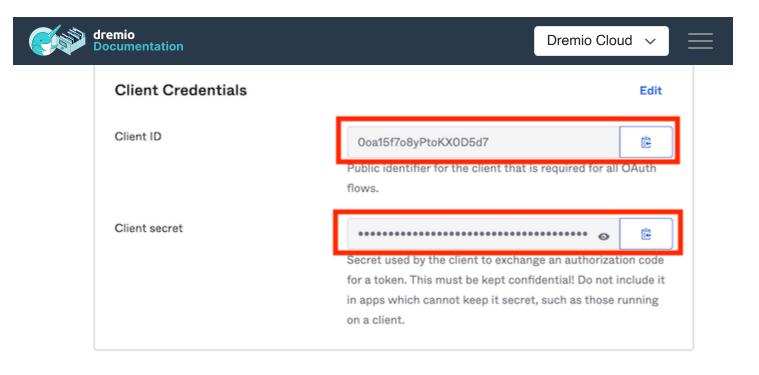
- (Optional) For Sign-out redirect URIs, click + Add URI, and enter https://accounts.dremio.cloud to specify the sign-out redirect URI. This overwrites the default local sign-out redirect URI.
- 11. (Optional) Under **Trusted Origins**, enter the base URI for **Base URIs** (but only if you plan to self-host the Okta sign-in widget).



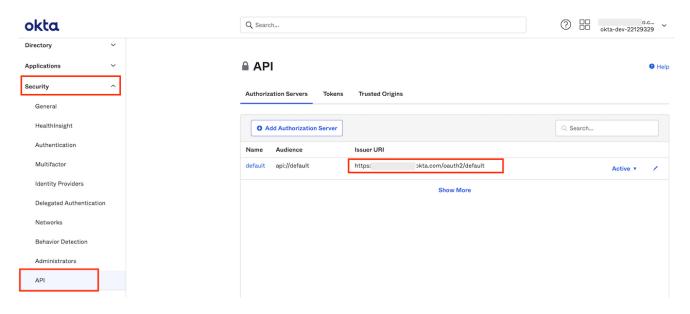
- Under Assignments, select Allow everyone in your organization to access for Controlled access.
- 13. Click Save.

Your registered application page will display. You now need the following values to configure the IdP within Dremio:

- 1. From your registered application page, select **General > Client Credentials**.
- 2. Copy the **Client ID** and **Client Secret** values. They are needed later to configure Okta in Dremio.



3. From the left sidebar, navigate to **Security** > **API**.

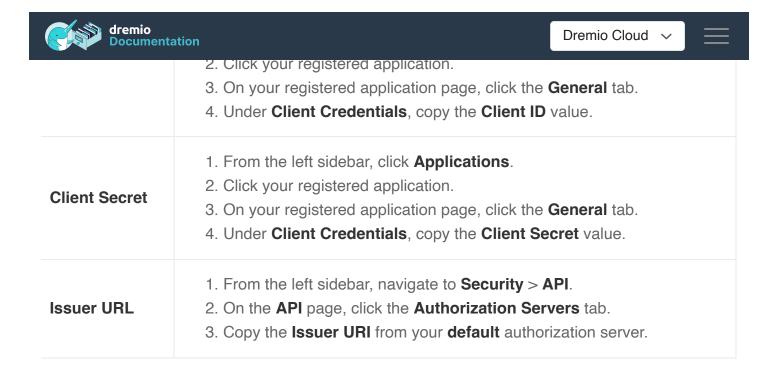


4. From the **API** page, select the **Authorization Servers** tab and copy the **Issuer URI** from your **default** authorization server. This is likewise needed later to configure Okta with Dremio.

Okta Properties Required for Dremio Configuration

Obtain the following properties from the Okta organization:

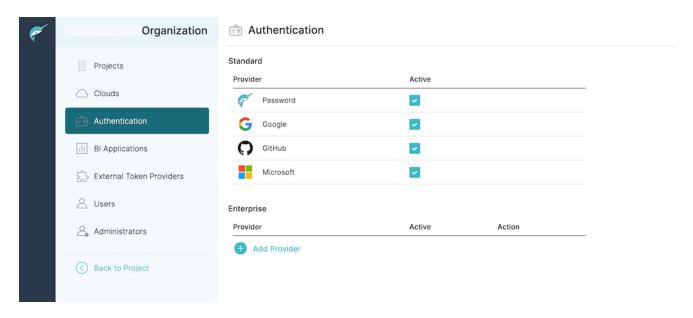
Property	Tracing the Property in the Organization
Client ID	1. From the left sidebar, click Applications .



Dremio Configuration

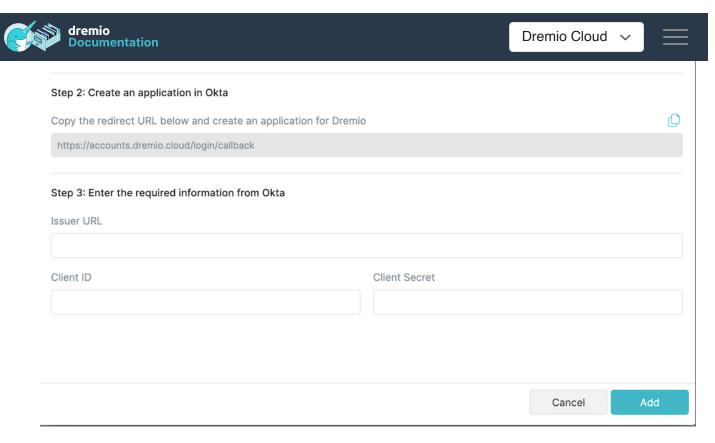
Perform the following steps from Dremio:

- 1. Click the **Settings** (gear) icon from the bottom-left corner of the screen and then select **Organization Settings**.
- Click the Authentication tab from the left sidebar. Under the Enterprise selection, click Add Provider.

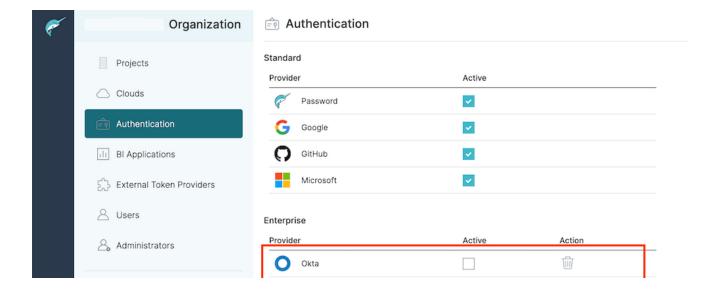


3. Using the Add Provider dialog, select Okta.





- 4. For **Step 2: Create an application in Okta**, enter the redirect URL from the Dremio application.
- 5. For **Step 3: Enter the required information from Okta**, enter the <u>required information from Okta</u>:
 - For Issuer URL, enter the issuer URL.
 - For Client ID, enter the client ID.
 - For Client Secret, enter the client secret.
- Click Add. Okta is now listed under the Enterprise section. However, it is not enabled by default.





Dremio Cloud ~

7. To activate the Okta enterprise IdP, select the checkbox under the **Active** column.

Okta is now configured as an authentication IdP and will display as an option for users logging in on Dremio.

Configuring SCIM

Okta may be configured to use SCIM for secure user and group provisioning in Dremio. This is accomplished through the following steps, as described below. Once you've configured Okta with SCIM, you may assign selective access to Dremio for your users or groups, or revoke access, as described below.

Adding SCIM as an App

- 1. From the Okta interface, navigate to the **Applications** page.
- 2. Click Browse App Catalog and search for SCIM.
- 3. Select SCIM 2.0 Test App (Header Auth) and then click **Add** from the app's page.
- 4. Enter an **Application label** and then click **Next**.
- 5. From the **Sign on Methods** page, click the **Secure Web Authorization** radio button and then the **Administrator sets username**, user sets password.
- 6. Click Done.

Configuring SCIM

- 1. From the SCIM application interface in Okta, click on the *Provisioning* tab.
- 2. Select the *Integration* tab and then click **Configure API Integration**.
- 3. Click Enable API Integration.
- 4. Enter the URL to your Dremio server in the Base URL field with the following format:

Base URL format

https://scim.dremio.cloud/scim/v2/

Generating Access Tokens

Dremio personal access tokens (valid for up to 180 days) with the format bearer {PAT} may be used when configuring Okta with SCIM. To obtain this, please refer to the <u>Personal Access Tokens</u> <u>page</u>.

Dremio Cloud V

to you ve generated a tener with Bronne, complete the following ctope

- 1. From the **Integration** tab in the Okta interface, in the **API Token** field enter the text bearer (including a space after the word) and then paste the token value provided from Dremio.
- 2. Click **Test API Credentials** to verify that Okta can access your instance of Dremio. A green message should appear at the top of the screen saying the API was verified successfully!
- Click Save.
- 4. Navigate to the *Provisioning* tab, and then the *To App* sub-tab.
- 5. Click the **Edit** button to the right of the **Provisioning to App** header.
- Select the Enable checkbox for Create Users, Update User Attributes, and Deactivate Users. Make any other selections as desired.
- 7. Click Save.

SCIM is now fully configured, which means users added from Okta will automatically provision in Dremio. You may now grant <u>users</u> or <u>groups</u> access to Dremio and <u>revoke access</u>.

Assigning User Access

To assign or grant users access to Dremio, perform the following steps:

- 1. From the Okta interface, navigate to the *Assignments* tab.
- Click the Assign drop-down from the top-left corner of the screen and select Assign to People.
- 3. Locate the desired users by scrolling or using the search bar.
- 4. Click the **Assign** button next to the desired user.
- 5. Scroll down and click Save and Go Back.

That user is now granted access to Dremio and an account is automatically created in the service. They may log in immediately and administrators may view their account from the <u>Users screen</u>.

We recommend <u>assigning privileges</u> and <u>roles</u> to manage their access to objects in Dremio.

Assigning Group Access

To assign or grant groups of users access to Dremio, perform the following steps:

- 1. From the Okta interface, navigate to the **Assignments** tab.
- 2. Click the **Assign** drop-down at the top-left corner of the screen and select **Assign to Groups**.
- 3. Click **Push Groups > Push Groups** to push an Okta group to Dremio.

All users associated with the group will be synchronized in Dremio. The group will also synchronize with Dremio as a <u>role</u> with all group members assigned to the role.



Dremio Cloud V

We recommend <u>assigning privileges</u> to manage role members' access to objects in Dremio.

Revoking Access

If you wish to revoke a user or group's access to Dremio:

- 1. From the SCIM app in the Okta interface, navigate to the Assignments tab.
- 2. Click the **Delete** (X) button on the far right of the desired user's row.

The deleted user(s) may no longer log in on Dremio. However, this does not automatically delete their account, and must be manually removed.

Was this page helpful?



