

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 [Dremio as an application in the Okta organization](#) and [add Okta as a provider in Dremio](#). Once that is done, you may configure [Okta to use SCIM](#) 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**.



The screenshot shows the Dremio Cloud documentation interface. The sidebar on the left contains a list of navigation items: Tasks, Notifications, Getting Started, Directory, Applications (highlighted with a red box), Self Service, Security, Workflow, and Reports. The main content area on the right is titled 'Tell Us About Yourself' and features a section 'Customize your goals' with two progress bars, each preceded by a green checkmark icon.

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

The screenshot shows the Okta Applications page. At the top, there's a header 'Applications' with a 'Help' link. Below this is a message: 'Your plan provides a limited number of custom apps. See the [plan page](#) for more information. Upgrade to the Enterprise Plan to get more apps and more monthly active users.' with an 'Upgrade' link. Below the message are four buttons: 'Create App Integration' (highlighted with a red box), 'Browse App Catalog', 'Assign Users to App', and 'More'. Below the buttons is a table with a search bar and a list of applications.

STATUS	
ACTIVE	0
INACTIVE	0

	Okta Admin Console
	Okta Browser Plugin
	Okta Dashboard

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

Create a new app integration

×



### Sign-in method

[Learn More](#)

☒ **OIDC - OpenID Connect**

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.

☐ **SAML 2.0**

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

☐ **SWA - Secure Web Authentication**

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

☐ **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 to a non-HTTP callback (for example, iOS, Android, React Native)




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

## New Web App Integration

**General Settings**

**App integration name**

**Logo (Optional)** ⓘ  



**Grant type**  
[Learn More](#) ⓘ

Client acting on behalf of itself

☐ Client Credentials

Client acting on behalf of a user


☒ Authorization Code

☐ Refresh Token

☐ Implicit (Hybrid)


- (Optional) For **Logo**, upload a logo using the **Upload** icon.
- 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.

**Sign-in redirect URIs**  
Okta sends the authentication response and ID token for the user's sign-in request to these URIs  
[Learn More](#) ⓘ



[+ Add URI](#)

**Sign-out redirect URIs (Optional)**  
After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.




[+ Add URI](#)

10. (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).

**Trusted Origins**

**Base URIs (Optional)**

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

[Learn More](#) 

**Assignments**

Controlled access

☒ Allow everyone in your organization to access


☐ Limit access to selected groups

12. 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.

[← Back to Applications](#)



**Dremio**

Active ▾ [View Logs](#)

**General** **Sign On** **Assignments** **Okta API Scopes**

**Client Credentials** [Edit](#)

**Client ID** 00a15f708yPtoKX0D5d7

Public identifier for the client that is required for all OAuth flows.

**Client secret** .....

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

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

**okta**  ? okta-dev-22129329

**Security** **API** [Help](#)

**API** [Add Authorization Server](#)

Name	Audience	Issuer URI	
default	api://default	https://okta.com/oauth2/default	Active

[Show More](#)

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
<b>Client ID</b>	1. From the left sidebar, click <b>Applications</b> .

	<ol style="list-style-type: none"> <li>2. Click your registered application.</li> <li>3. On your registered application page, click the <b>General</b> tab.</li> <li>4. Under <b>Client Credentials</b>, copy the <b>Client ID</b> value.</li> </ol>
<b>Client Secret</b>	<ol style="list-style-type: none"> <li>1. From the left sidebar, click <b>Applications</b>.</li> <li>2. Click your registered application.</li> <li>3. On your registered application page, click the <b>General</b> tab.</li> <li>4. Under <b>Client Credentials</b>, copy the <b>Client Secret</b> value.</li> </ol>
<b>Issuer URL</b>	<ol style="list-style-type: none"> <li>1. From the left sidebar, navigate to <b>Security &gt; API</b>.</li> <li>2. On the <b>API</b> page, click the <b>Authorization Servers</b> tab.</li> <li>3. Copy the <b>Issuer URI</b> from your <b>default</b> authorization server.</li> </ol>

## 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**.
2. Click the **Authentication** tab from the left sidebar. Under the **Enterprise** selection, click **Add Provider**.

The screenshot shows the Dremio Organization Settings page. The left sidebar has 'Authentication' selected. The main content area is titled 'Authentication' and is divided into two sections: 'Standard' and 'Enterprise'.

**Standard Section:**


Provider	Active
Password	<input checked="" type="checkbox"/>
Google	<input checked="" type="checkbox"/>
GitHub	<input checked="" type="checkbox"/>
Microsoft	<input checked="" type="checkbox"/>


**Enterprise Section:**


Provider	Active	Action
<a href="#">+ Add Provider</a>		

3. Using the **Add Provider** dialog, select **Okta**.

The screenshot shows the 'Add Provider' dialog box. The title bar says 'Add Provider' with a close button. The main content area shows 'Step 1: Select a provider'.


 **dremio**  
Documentation

Dremio Cloud 



---

**Step 2: Create an application in Okta**

Copy the redirect URL below and create an application for Dremio 

https://accounts.dremio.cloud/login/callback

---

**Step 3: Enter the required information from Okta**

Issuer URL


Client ID

Client Secret


Cancel


Add


- For **Step 2: Create an application in Okta**, enter the redirect URL from the Dremio application.
- For **Step 3: Enter the required information from Okta**, enter the [required information from Okta](#):
  - 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.





**Organization**


 Projects


 Clouds

 **Authentication**

 BI Applications





 External Token Providers

 Users



 Administrators

**Authentication**

**Standard**

Provider	Active
 Password	<input checked="" type="checkbox"/>
 Google	<input checked="" type="checkbox"/>
 GitHub	<input checked="" type="checkbox"/>
 Microsoft	<input checked="" type="checkbox"/>

**Enterprise**

Provider	Active	Action
 Okta	<input type="checkbox"/>	





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 [Personal Access Tokens page](#).

Once you've generated a token with Dremio, complete the following steps:

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!**
3. 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.
6. 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 [users](#) or [groups](#) access to Dremio and [revoke access](#).

## 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.
2. 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 [Users screen](#).

We recommend [assigning privileges](#) and [roles](#) 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 [role](#) with all group members assigned to the role.

We recommend [assigning privileges](#) 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?

