On this page

External Token Providers

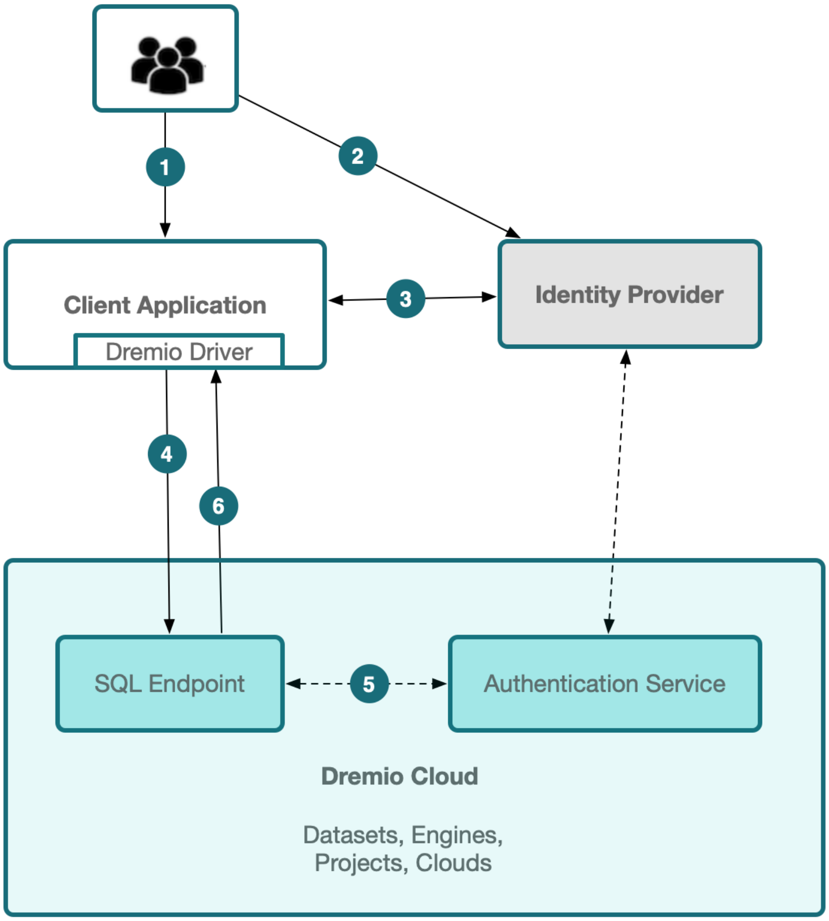
You can use a JSON Web Token (JWT) issued by your identity provider (IdP) to establish ODBC/JDBC connections to Dremio Cloud. The IdP can be any provider that can generate a JWT.

Overview

External token providers enable client applications to use a JWT issued by an IdP in order to authenticate to Dremio's SQL interface. This enables you to integrate Dremio into client applications without having to authenticate both the IdP and Dremio.

To use this feature, the Dremio administrator configures an external token provider in the Dremio organization. This step enables Dremio to validate that the JWT is actually issued by the IdP and received by Dremio, which sets up Dremio to trust the external IdP.

The following figure illustrates an example of the authorization process for a JWT:



2. The user is redirected to the IdP to log in and authenticate.
3. The user accesses the report/dashboard in the client application that uses a Dremio data source. If the user allows the client application to access Dremio, the IdP issues a JWT to the client application for that user.
4. The client application sends a ODBC/JDBC connection request using the Dremio driver and using the JWT as the password and an empty username.
5. Dremio's SQL interface sends the credentials to Dremio's Authentication Service for validation. Dremio's Authentication Service validates that the JWT was actually issued by a valid external token provider and the audience in the JWT is Dremio. The authentication service then returns the user information (extracted from the JWT) to the SQL interface.
6. Dremio's SQL interface creates a stateful connection for the user. The client application can use this connection to issue queries on behalf of the user, and the connection is closed when the token expires.

Benefits of External JWTs

- JWTs are provided by an OIDC IdP. OIDC is a commonly used open authentication protocol that extends OAuth 2.0 via an identity layer though which an end user confirms their identity via authentication from their preferred authorization server.
- You can typically pick your preferred OIDC IdP to generate a JWT.
- JWTs reduce the threat of security incidents by removing direct access to these tokens. Typically, such tokens are centrally managed and inaccessible by users.
- Tokens may be generated with short expiration periods of minutes or hours, making these tokens even more secure as they cannot be easily leaked or misused.

Understanding JWT Claim Values

The following sections offer additional context regarding the values required to correctly enable the external token provider functionality. Each of these sections will reference the following example declaration from the JWT Claims Set of a JWT, as provided by Internet Assigned Numbers Authority (IANA):

Example JWT Claims Set declaration

```
{ "iss": "https://server.example.com", "preferred_username": "user@dremio.com
```

Audience

The **Audience** field identifies the recipient(s) the JWT is intended for, which is typically specific to the application. In order to process the JWT, an audience claim must be included. If the audience is absent, the claim will be rejected outright. The audience claim is identified by the `aud` member, which contains an array of case-sensitive strings, consisting of a `StringOrURI` value. In the event of only a single audience, then one string will be found here, as shown in the example below:

Single audience example

```
"aud": "https://client.example.org",
```

> **Note:**
> For Azure Active Directory, the audience can be the client ID or the resource URI.

User Claim Mapping

The **User Claim Mapping** field identifies the specific user the JWT is being used for, which should consist of their Dremio email address. This is considered a private claim name, but is required from an IdP to identify a user's permissions and access. The field in Dremio is used to identify whatever custom claim is attached to usernames depending on the provider, such as `preferred_username`.

As an example, in Power BI with Azure Active Directory, the user claim is `upn`, which is a basic claim in v1.0 access tokens. If you are using a different Token Provider with a user claim other than `upn`, specify that user claim in the **User Claim Mapping** field.

Issuer URL

The **Issuer URL** identifies the original entity that issued the JWT, which is typically application-specific. The issuer may be identified by the `iss` member, a case-sensitive string containing a single `StringOrURI` value. This is required for Dremio.

From the example above, an issuer would appear as:

Issuer example

Note:
A given issuer URL and audience can only be used by one external token provider and one organization.

JWKS URL

The **JWKS URL** field is specifically used when a proof-of-possession key is provided as a reference rather than a value. This is done using the `jku` member, which is a URI referring to a resource for JSON-encoded public keys. These keys are represented as a JWK Set (JWKS), which includes the key.

From the example above, consider the following claim:

Claim example

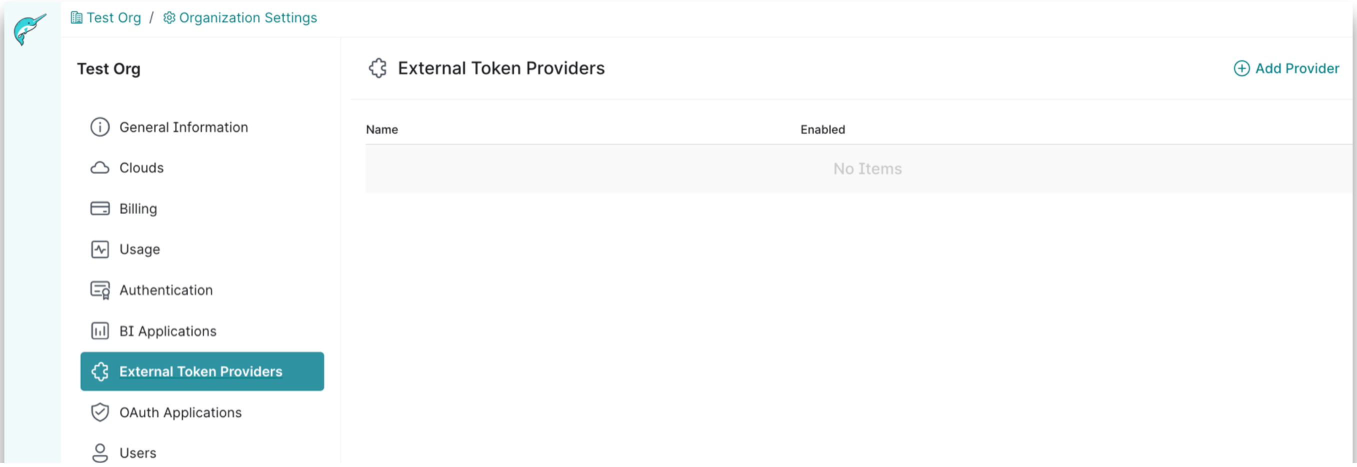
```
"cnf":{ "jku": "https://keys.example.net/pop-keys.json", "kid": "2015-08-28"
```

The `jku` value is used for the **JWKS URL** field in Dremio. However, if multiple keys are used, a “kid” must also be identified in the JRT and found within the referenced JWKS. That key should also contain the same “kid” value.

Viewing External Token Providers

Perform the following steps to view external token providers:

1. From Dremio Cloud, click the Organization (building) icon in the side navigation bar.
2. Click the Settings (gear) icon at the top of the page.
3. On the Organization Settings page, click **External Token Providers** on the left sidebar.



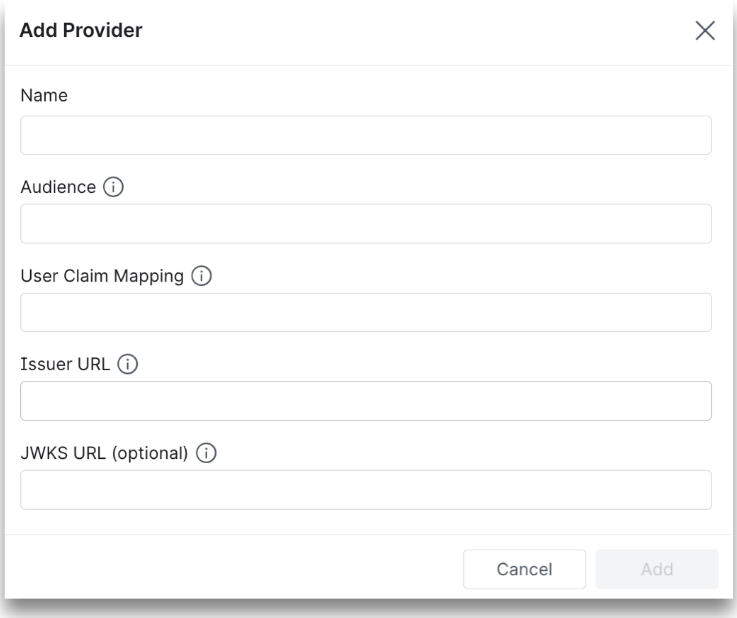
Name	Enabled
No Items	

Adding an External Token Provider

Perform the following steps to add an external token provider:

> **Note:**
> See Understanding JWT Claim Values for claim information.

1. From the Organization Settings page, click **External Token Providers** on the left sidebar.
2. On the External Token Providers page, click **Add Provider** at the top-right corner.
3. In the **Add Provider** dialog, enter the following:



   a. For **Name**, enter a name for the client application.

   b. For **Audience**, enter the value that identifies the intended recipients of the JWT being added.

   c. For **User Claim Mapping**, enter the private claim that maps to the Dremio username.

   d. For **Issuer URL**, enter the URL (using the `https` scheme with no query or fragment component) of the IdP you want to connect to. Dremio will normalize the issuer URL.

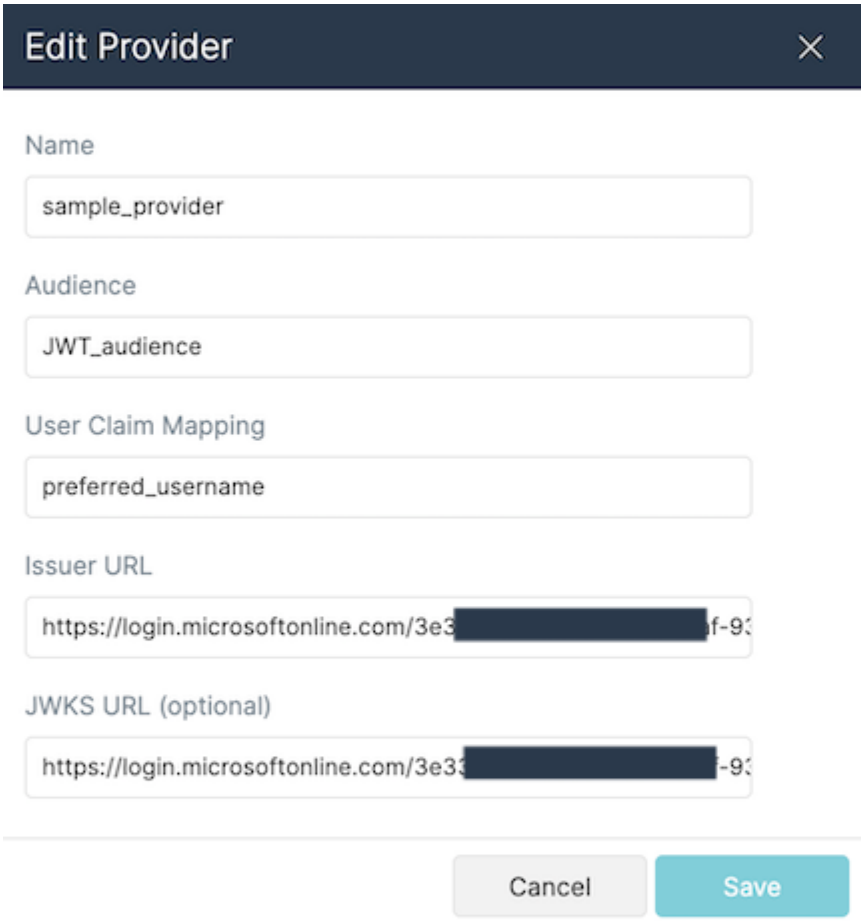
   e. (Optional) For **JWKS URL**, enter the URL of the IdP's JSON Web Key Set document. If not provided, Dremio will retrieve it from {issuerUrl}/.well-known/openid-configuration.

4. Click **Save**.

All parameters are optional in an edit operation. Perform the following steps to edit an external token provider:

> **Note:**
> See Understanding JWT Claim Values for additional information.

1. From the Organization Settings page, click **External Providers** on the left sidebar.
2. From the External Token Providers page, click the **Edit** icon for the external token provider that you want to edit.
3. From the **Edit Provider** dialog, enter a name for the client application for **Name**.



Edit Provider

Name: sample_provider

Audience: JWT_audience

User Claim Mapping: preferred_username

Issuer URL: https://login.microsoftonline.com/3e3[redacted]

JWKS URL (optional): https://login.microsoftonline.com/3e3[redacted]

4. For **Audience**, enter the value that identifies the intended recipients of this JWT that is being added.

   > **Note:**
   > For Azure Active Directory, the audience can be the client ID or the resource URI.

5. For **User Claim Mapping**, enter the claim of the external JWT that maps to the Dremio username.

> **Note:**
> A given issuer URL and audience can only be used by one external token provider and one organization.

7. (Optional) For **JWKS URL**, enter the URL of the IdP's JSON Web Key Set document. If not provided, Dremio will retrieve it from {issuerUrl}/.well-known/openid-configuration.
8. Click **Save**.

Deleting an External Token Provider

Perform the steps below to delete an external token provider:

1. From the Organization Settings page, click **External Providers** on the left-hand sidebar menu.
2. From the External Token Providers page, click the **Delete** icon for the external token provider that you wish to delete.
3. Confirm that you wish to delete the external token provider.

Was this page helpful? Yes No