Connecting To Google G Suite Directory

If you do not want to use AtScale's embedded directory service to manage users and groups, you can configure an AtScale organization to connect to and use Google G Suite Directory.

Before You Begin

Before you can connect AtScale to Google G Suite Directory, you must follow these prerequisite steps:

1. Log into Google Cloud Platform.
2. In the APIs card, click "Go to APIs overview".
3. On the left side of the screen, click **Library**.
4. Search on the term "Admin SDK" and then click the Admin SDK result.
5. Click Enable.
6. On the left side of the screen, click **Credentials**.
7. Click **Create credentials** and select **OAuth client ID**.
8. Set the value of **Authorized JavaScript origins** to the following line:

```
http://<hostname>:10500
```

For hostname, substitute the fully-qualified domain name that is used to connect to AtScale. For the deployment of an AtScale cluster, this is the hostname (e.g. atscaleprod.company.com).

1. Set the value of **Authorized redirect URLs** to the following line:

```
http://<hostname>:10500/login/google/callback/<orgID>
```

   - For hostname, substitute the fully-qualified domain name that is used to connect to AtScale. For the deployment of an AtScale cluster, this is the hostname (e.g. `atscaleprod.company.com`).
   - For orgID, substitute the name of the AtScale organization that you are connecting to G Suite Directory.

Next, you need a Google Cloud service account and a private key in JSON format.

- If you want to create a service account:

  1. Create a Google Cloud service account. (URL)

     1. In the **Create service account** dialog, select **Furnish a new private key** and keep the default JSON format selected.
     2. Select **Enable G Suite Domain-wide Delegation**.

- If you want to use an existing service account:

    1. In Google Cloud Platform, navigate to the list of service accounts that your projects are using.
    2. Click the dots on the right side of the service account's listing and select **Edit**.
    3. Select **Enable G Suite Domain-wide Delegation** and click Save.
    4. Again, click the dots on the right side of the service account's listing and select **Create Key**.
    5. Create a key that is in the JSON format.

Finally, whether you are using a new service account or an existing one, follow these two steps:

1. Delegate domain-wide authority to your service account by following the instructions on this page of the Google Cloud Platform documentation: Performing G Suite Domain-Wide Delegation of Authority.

    - For the client ID, use the client ID that is in the JSON private key that you downloaded when creating the service account.
    - Use the following API scopes:

    ```
    https://www.googleapis.com/auth/admin.directory.group.readonly,
    https://www.googleapis.com/auth/admin.directory.user.readonly
    ```

2. Copy the JSON private key to the filesystem where the AtScale engine is running.

About This Task

You must configure a connection to one external directory service for each AtScale organization. Each organization can connect to a different external directory service.

Note: Using Google BigQuery a data warehouse is not a prerequisite for using G Suite Directory to manage AtScale users and groups. You can use any external directory service that is supported by AtScale, or you can use AtScale's embedded directory service.

Procedure

1. Choose **Security** from the main navigation, select **Setup** under the Directory section.
2. Select **G Suite Directory** as the type of directory service that you want to connect to.
3. Click the **Download Configuration** button to save the current configuration to your hard drive before you make any changes.
4. Specify values for the configuration settings.

Section	Field	Description
General	Name	Specify a unique name for AtScale to use when referring

		to your G Suite Directory.
General	Synchronize group assignments when users log in (strongly recommended)	Select to ensure that any changes to a user's account that are made in G Suite Directory and that affect the user's roles and permissions in AtScale are synchronized with the user's account info cached in AtScale.
Google Settings	Domain	Specify a domain to use from your Google Cloud account.
Google Settings	Email Address of Organization Administrator	Specify the email address of user who has the privileges to manage the Google Cloud account's organizational structure. With this address, AtScale is authorized to read account information of all users within the organization who are associated with AtScale through mappings to AtScale roles and groups.
Google Cloud Service Account Settings	Client ID from JSON Private Key	Specify the client ID that is contained in the JSON private key for the service account.
Google Cloud Service Account Settings	Path to JSON Private Key	Specify an absolute path on the local filesystem to the location of a copy of the JSON private key for the service account.
Google Cloud OAuth Settings	OAuth Client ID	Specify the client ID pertaining to your Google Cloud OAuth credentials.
Google Cloud OAuth Settings	OAuth Client Secret	Specify the secret pertaining to your Google Cloud OAuth client ID.
Optional Settings	Maximum Number of Users to Include in Full Synchronizations with the Directory	When users log into AtScale, their account info is synchronized in AtScale. These individual synchronizations differ from bulk synchronizations, in which multiple user accounts are synchronized at a time. These bulk actions can consume significant amounts of system resources. To limit their duration, you can set a maximum number of user accounts to synchronize.

Optional Settings	Filter for Allowing Matching Users to Log In to AtScale	Specify a filter to restrict access to AtScale to a subset of users. Refer to Google's documentation for syntax and options.

5. Click **Save** and Test Configuration.

Results

- When users log into the AtScale Design Center, they must use their Google account credentials.
- Before users of client BI applications can connect to published AtScale cubes, they must log into the AtScale Design Center, go to their user-account page, and copy the temporary session password from that page. The temporary session password authorizes them to connect to AtScale published cubes, using their Google account ID, for a two-hour session. When a user's session expires, that user must return to the user-account page to obtain another temporary session password.If you want to change the duration for which temporary session passwords are valid, and if you are a super user or an administrator for your AtScale organization, follow these steps:

    1. Choose **Settings** from the main navigation, select **Organization** under the Organization Settings section.
    2. Search the page for the setting **OAuth Session Expiry (minutes)** and click Override to set a new duration in seconds.
    3. Click **Update Settings** at the top of the page.