Connecting To Azure Active Directory

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. Here you can find how to use it to manage users and groups in AtScale.

> Consider that with Azure AD configured as identity provider, users would be able to use basic authentication only with the Power BI and Excel business intelligence tools .

Prerequisites

- Your users are configured in Azure AD.
- Your user account in AtScale is assigned to the Organization Admin or Super User role. For details, see Assigning Individual Users to Roles.
- In AtScale, obtain the organization details:

    1. Go to Settings > Global Settings > Organizations, choose the organization you need. You would be now on the Organization Settings page.
    2. Copy the part of the browser URL between org and settings, without the slashes. This is the organization ID you need. Here is an example: `21989ba3-2182-4234-4ba5-457855404bbf`

       Note there is a difference between the name of an organization and its ID. For details, see Rename an Organization.

    3. Obtain the Design Center IP/hostname and port displayed on the page. For example, `atscale.example.com` and `10500`.
    4. Do this for each organization for which you want to use Azure AD.

Setting Up Azure

Before you can connect AtScale, you must follow these prerequisite steps in Azure:

1. Create an application for the AtScale connection; for details, see Register an application.
2. Go to Overview and copy the application (client) ID and the Directory (tenant) ID. They would later be used when setting up AtScale.
3. Go to API permissions and enable the following permissions for Microsoft Graph; for details, see Add permissions to access Microsoft Graph:

    - Application permissions: `GroupMember.Read.All`, `User.Read.All`
    - Delegated permissions: `GroupMember.Read.All`, `User.ReadBasic.All`

4. Go to Certificates & secrets and add a client secret. Note the following:

- The procedure is described in Add a client secret.
- The secret value is available only on secret creation, so you need to copy it at this point.
- It would later be used when setting up AtScale.

5. Go to Authentication and add the redirect URIs for your AtScale Design Center instances:

   - Choose the "Web" type.
   - Enter the address in the following format, using using the organization details you obtained from AtScale: `https://<Design Center IP>:<Design Center Port>/login/oauth/callback/<organization id>`

     For example: `https://atscale.example.com:10500/login/oauth/callback/21989ba3-2182-4234-4ba5-457855404bbf`

   - The procedure is described in Add a redirect URI.

6. Go to Expose an API and add a scope (for example, `user_impersonation`):

   - The procedure is described in Add a scope. See also Scopes and permissions in the Microsoft identity platform.
   - Store the scope, it would later be used when setting up AtScale.
   - In Authorized client applications, add a client application, using the application (client) ID of the application you have created.

7. Go to API permissions > Add a permission > My APIs and add your application. For details, see Configure a client application to access a web API.

Setting Up AtScale

After the Azure application is configured, you need to log in to AtScale and do the following:

1. Choose Security from the main navigation, select Setup under the Directory section.
2. Select Azure Active Directory as the type of directory service that you want to connect to.
3. For Name, specify a unique name for AtScale to use when referring to this directory; it is recommended to keep the Synchronize group assignments when users log in option selected.
4. Enter the details you obtained from Azure (see the section above): tenant ID, engine client ID, engine client secret, and API scope.
5. Optionally, set the maximum number of users to include in full synchronizations with the directory; enter an integer, 1 or more.
6. Save the directory.

Next Steps

After Azure AD is configured you need to do map directory groups to AtScale roles; make sure the Design Center User and Runtime Query User roles are mapped. For details, see Assigning Roles to Directory Groups.

Optionally, you can sync part of the users by going to Security > Directory > Synchronize, creating a new synchronization filter, and choosing the Sync Now button. Consider the details provided in Bulk Synchronization of User Accounts to AtScale.

After you have some users synchronized, you can go to Security > Users to verify they are available and the roles assigned to them are correct.

Result

With Azure AD configured, you can do the following:

- The synchronized users would log in to AtScale's Design Center using their Azure account. Instead of entering user name and password, they would simply choose the Log in with Microsoft button and select the account they want to use.
- You can start using token-based authentication for BI clients.