Configuring Microsoft Entra ID With OpenID Connect

You can configure user authentication with Microsoft Entra ID as your IdP using OpenID Connect.

Important: The users defined in Entra ID are automatically added to the AtScale Identity Broker when they log in for the first time. All users are added to the `everyone` group, which includes the `query_user` role. If you need to add users to other groups or assign them additional roles, you must do so from within the Identity Broker. For more information, see Managing Users with the Identity Broker.

Prerequisites

This procedure assumes that you have an enterprise application set up for AtScale in Entra ID, and that it is configured with OpenID Connect. For more information, refer to the Microsoft Entra ID documentation.

Additionally, you must be logged in as an admin user.

Procedure

To configure authentication using Microsoft Entra ID with OpenID Connect:

1. In AtScale, open the main menu and select **Security**. The Identity Broker opens.
2. Log in using your AtScale admin username and password.
3. Select the **atscale** realm if it is not already selected.
4. In the left-hand navigation, select **Identity providers**, then click **OpenID Connect v1.0**.
5. On the **Add OpenID Connect provider** page, complete the following fields:

    - **Redirect URI**
    - **Alias**
    - **Display name**

6. In a new browser tab, log in to the Microsoft Entra admin center, locate the OpenID Connect metadata document URL for the AtScale application, and copy it.
   For instructions on locating this information, refer to the Microsoft Entra ID documentation.
7. In the Identity Broker, paste the URL in the **Discovery endpoint** field. The Identity Broker validates the URL and displays a checkmark if it passes.
8. Go back to the Microsoft Entra admin center, locate the **Application (client) ID** for the AtScale application, and copy it.
9. In the Identity Broker, paste the client ID the **Client ID** field.

10. In the Microsoft Entra admin center, locate and copy the client secret for the AtScale application.
11. In the Identity Broker, paste the client secret into the **Client Secret** field.
12. Click **Add**.
13. Click on the newly-added IdP.
14. Scroll down to the **Advanced settings** section and enable the **Store tokens** and **Stored tokens readable** settings.
15. Click **Save**.
16. Test your configuration:

    1. Open a new browser tab and navigate to your AtScale instance. The **Sign in to your account** window appears.
    2. Click the option to log in with Entra ID and enter your credentials.