**SCIM provisioning using Microsoft Entra ID** (formerly known as **Azure Active Directory**) for your **Azure Databricks** account. I'll provide an introduction, steps for configuration, and a conclusion.

**Configure SCIM Provisioning Using Microsoft Entra ID (Azure Databricks)**

Introduction

**SCIM (System for Cross-domain Identity Management)** is a standard protocol that enables automated user provisioning and de-provisioning across different applications. In this guide, we'll set up SCIM provisioning for your Azure Databricks account using Microsoft Entra ID. This allows you to synchronize users and groups seamlessly.

Steps for Configuration

Step 1: Prerequisites

Before you begin, ensure the following:

1. Your Azure Databricks account is on the **Premium plan**.
2. You have the **Cloud Application Administrator** role in Microsoft Entra ID.
3. Your Microsoft Entra ID account is a **Premium edition** account (for provisioning groups).

Step 2: Configure Azure Databricks

1. Log in to the **Azure Databricks account console** as an account admin.
2. Click on **Settings**.
3. Navigate to **User Provisioning**.
4. Click **Enable user provisioning**.
5. Copy the **SCIM token** and the **Account SCIM URL**. You'll need these to configure your Microsoft Entra ID application.

Step 3: Configure Microsoft Entra ID

1. In your **Azure portal**, go to **Microsoft Entra ID > Enterprise Applications**.
2. Set up a **SCIM provisioning connector** using the copied token and URL.
3. Ensure that any existing SCIM connectors that sync identities directly to your workspaces are **disabled** when enabling the account-level SCIM connector.

Conclusion

By following these steps, you'll be able to provision users and groups from Microsoft Entra ID to your Azure Databricks account. Remember that provisioning is separate from authentication and conditional access configurations. Authentication is handled automatically by Microsoft Entra ID using the OpenID Connect protocol flow.

For more details, refer to the official [Azure Databricks documentation](https://learn.microsoft.com/en-us/azure/databricks/administration-guide/users-groups/scim/aad).

Happy provisioning! 🚀.

Certainly! Below is a guide on configuring **SCIM provisioning using Microsoft Entra ID** (formerly known as **Azure Active Directory**) for your **Azure Databricks** account and workspace. I'll provide an introduction, steps for configuration, and a conclusion.

**Configure SCIM Provisioning Using Microsoft Entra ID (Azure Databricks)**

Introduction

**SCIM (System for Cross-domain Identity Management)** is a standard protocol that enables automated user provisioning and de-provisioning across different applications. In this guide, we'll set up SCIM provisioning for both your Azure Databricks account and individual workspaces using Microsoft Entra ID. This allows you to synchronize users and groups seamlessly.

Steps for Configuration

Step 1: Prerequisites

Before you begin, ensure the following:

1. Your Azure Databricks account is on the **Premium plan**.
2. You have the **Cloud Application Administrator** role in Microsoft Entra ID.
3. Your Microsoft Entra ID account must be a **Premium edition** account to provision groups. Provisioning users is available for any Microsoft Entra ID edition.
4. You must be an **Azure Databricks account admin**.

Step 2: Configure Azure Databricks

1. Log in to the **Azure Databricks account console** as an account admin.
2. Click on **Settings**.
3. Navigate to **User Provisioning**.
4. Click **Enable user provisioning**.
5. Copy the **SCIM token** and the **Account SCIM URL**. You will use these to configure your Microsoft Entra ID application.

Step 3: Configure Microsoft Entra ID

1. In your **Azure portal**, go to **Microsoft Entra ID > Enterprise Applications**.
2. Set up a **SCIM provisioning connector** using the copied token and URL.
3. Ensure that any existing SCIM connectors that sync identities directly to your workspaces are **disabled** when enabling the account-level SCIM connector.

Conclusion

By following these steps, you'll be able to provision users and groups from Microsoft Entra ID to both your Azure Databricks account and individual workspaces. Remember that provisioning is separate from authentication and conditional access configurations. Authentication for Azure Databricks is handled automatically by Microsoft Entra ID using the OpenID Connect protocol flow.

For more details, refer to the official [Azure Databricks documentation](https://learn.microsoft.com/en-us/azure/databricks/administration-guide/users-groups/scim/aad).

Happy provisioning! 🚀.

Source(s)

1. [Configure SCIM provisioning using Microsoft Entra ID (formerly Azure ...](https://learn.microsoft.com/en-us/azure/databricks/administration-guide/users-groups/scim/aad)

2. [Sync users and groups from your identity provider - Databricks](https://bing.com/search?q=Configure+SCIM+provisioning+using+Microsoft+Entra+ID+for+Azure+Databricks+account+and+workspace)

3. [Sync users and groups from your identity provider - Databricks](https://docs.databricks.com/en/administration-guide/users-groups/scim/index.html)

4. [Sync users and groups from your identity provider - Databricks](https://docs.gcp.databricks.com/en/administration-guide/users-groups/scim/index.html)

5. [Microsoft Entra on-premises app provisioning to Azure Databricks with ...](https://learn.microsoft.com/en-us/entra/identity/saas-apps/azure-databricks-with-private-link-workspace-provisioning-tutorial)