**Configuring SCIM Provisioning Using Microsoft Entra ID**

Prerequisites

* Ensure your **Azure Databricks account** is on the **Premium plan**.
* You must have the **Cloud Application Administrator** role in **Microsoft Entra ID**.
* Your **Microsoft Entra ID** account should be a **Premium edition** account to provision groups (user provisioning is available for any edition).
* As an **Azure Databricks account admin**, you'll need access to the Azure Databricks account console.

Steps

1. **Configure Azure Databricks**:

* Log in to the **Azure Databricks account console**.
* Click on **Settings**.
* Navigate to **User Provisioning**.
* Click **Enable user provisioning**.
* Copy the **SCIM token** and the **Account SCIM URL**. You'll use these to configure your **Microsoft Entra ID application**.

1. **Microsoft Entra ID Configuration**:

* In your **Azure portal**, go to **Microsoft Entra ID > Enterprise Applications**.
* Set up a **SCIM provisioning connector** using the copied token and URL.
* If you already have SCIM connectors syncing identities directly to your workspaces, **disable those connectors** when enabling the account-level SCIM connector.
* Remember that provisioning configuration is separate from authentication and conditional access policies.

---

Feel free to customize this document further based on your specific environment and requirements. If you have any questions, don't hesitate to ask!

# Configuring SCIM Provisioning Using Microsoft Azure AD

## Introduction

System for Cross-domain Identity Management (SCIM) is an open standard protocol for automating the exchange of user identity information between identity domains, or IT systems. Microsoft Azure Active Directory (Azure AD) is a cloud-based identity and access management service provided by Microsoft. In this document, we will outline the steps to configure SCIM provisioning using Microsoft Azure AD, specifically focusing on using Microsoft Entra ID.

## Prerequisites

1. \*\*Microsoft Azure AD\*\*: You must have access to Microsoft Azure AD with administrative privileges.

2. \*\*Microsoft Entra ID Account\*\*: Access to Microsoft Entra ID with necessary permissions to configure applications and integrations.

3. \*\*Access to SCIM-compliant application\*\*: Ensure the application you want to provision users to supports SCIM provisioning.

## Steps to Configure SCIM Provisioning

### 1. Log in to Microsoft Azure Portal

1. Go to [Microsoft Azure Portal](https://portal.azure.com) and sign in with your administrator credentials.

### 2. Create an Enterprise Application

1. In the Azure Portal, navigate to "Azure Active Directory" > "Enterprise applications".

2. Click on "New application".

3. Search for and select the application you want to configure SCIM provisioning for.

4. Follow the prompts to add the application to your Azure AD.

### 3. Configure Provisioning

1. After adding the application, go to its settings page.

2. Select "Provisioning" from the left-hand menu.

3. Set the provisioning mode to "Automatic".

4. Choose the provisioning connector type as "SCIM".

5. Enter the SCIM endpoint URL provided by the application you want to provision users to.

6. Enter the authentication credentials required to connect to the SCIM endpoint.

7. Test the connection to ensure it's successful.

### 4. Map Attributes

1. Once the connection is established, map the attributes between Azure AD and the SCIM endpoint.

2. Map user attributes such as username, email, display name, etc., as per the requirements of the target application.

3. Ensure proper mapping to avoid data discrepancies during provisioning.

### 5. Enable Provisioning

1. After mapping attributes, enable provisioning by switching the provisioning status to "On".

2. Save the configuration.

### 6. Verify Provisioning

1. Add or modify users in Azure AD to trigger provisioning.

2. Monitor the provisioning logs in Azure AD to verify that users are successfully provisioned to the target application.

3. Verify in the target application that the users are correctly provisioned with the mapped attributes.

## Conclusion

By following the steps outlined in this document, you can configure SCIM provisioning using Microsoft Azure AD, enabling seamless user provisioning and management across different applications and systems. This integration streamlines identity management processes and ensures consistency and security across your organization.