Add Azure AD Tenant

Last Modified on 07.12.24

Azure AD integration allows Privilege Manager to target management rules directly to Azure AD groups and devices. When you create dynamic Azure AD groups for your devices and then create Privilege Manager management rules for this Azure AD group, your Azure AD connected devices will automatically receive your management rules when devices are joined to Azure AD and dynamic group memberships have been updated.

You can add multiple Azure AD tenants to a single Privilege Manager environment.

> **NOTE:** Azure AD integration can only be used to manage native Azure AD joined devices. Hybrid Azure AD devices joined to both on-premises AD and Azure AD must be managed as on-premises AD devices.

Creating Azure AD App Registration

You need to create an Azure AD App Registration for the target tenant and you need to have permissions to register new Azure AD Apps. If you do not have permissions to create Azure AD App Registration, send these instructions to someone with the required permissions to receive the following information when this step is completed: **Directory ID** (also known as tenant ID), **Application ID** (also known as Client ID) and **Client Secret**.

1. Open https://portal.azure.com and navigate to **App registrations.**
2. Select **New registration**.
3. Specify the **Name** for the application (for example Recast Privilege Manager) and click **Register.**
4. After the app is registered, click **Certificates & secrets**.
5. On the **Client secrets** tab, add a **New client secret**.
6. Add a **description** for the secret (for example Privilege Manager service), choose when the secret **Expires** and click **Add**.

   DO NOT navigate away from the page before completing the next step!

> **NOTE:** You must create a new client secret before the current one expires and then change the client secret from the Privilege Manager management portal to Azure AD directory.

1. **Copy** the client secret value to a clipboard and save the value to a secure location (if you need to access client secret later). You are not able to see the client secret after you have navigated away from the page. Privilege Manager management portal will not show you the client secret as well and you will need to specify the client secret always

when you modify your Azure AD directory in Privilege Manager (for example if you want to change the display name of the Azure AD tenant in Privilege Manager).

2. On the **API permissions** page, **Add a permission**.
3. On the Microsoft APIs tab, click **Microsoft Graph**.
4. Click **Application permissions**.
5. Under **Select permissions**, enter **Device.Read.All**.
6. Expand the **Device** section and select **Device.Read.All**.
7. Replace the permissions with '**GroupMember.Read.All**'.
8. Expand the **GroupMember** section and select **GroupMember.Read.All**.
9. Replace the permissions with '**User.Read.All**', expand the **User** section, and select **User.Read.All.**
10. Click **Add permissions**.
11. Verify that you have added **three** permissions where the type is **Application** and the permission values have **Device.Read.All**, **Group.Read.All** and **User.Read.All** and then click **Grant admin consent for <your tenant name>**. Confirm by selecting **Yes**.
12. Click **Overview** and take note of the **Application (client) ID** and **Directory (tenant) ID**. The **Client secret** was noted earlier. These values are required when configuring Recast Privilege Manager.

Privilege Manager configuration

After the Azure AD App Registration is done and you have the **Application (client) ID**, **Directory (tenant) ID** and **Client secret** available you can continue to add your Azure AD tenant to Privilege Manager.

- Open your Privilege Manager Portal and add the new Azure AD.
- Create management rules that target Azure AD groups or devices.

Client update

Make sure that your endpoints are using Privilege Manager client version **3.1.5014** or later.