RECAST SOFTWARE

# Set Up Entra ID for Privilege Manager

Last Modified on 04.23.25

Privilege Manager allows you to automatically target management rules at your Entra ID groups and devices. You can add multiple Entra ID tenants for a single Privilege Manager environment.

**NOTE**: You can only use this Entra ID integration to manage native Entra ID-joined devices. Hybrid Entra ID devices, joined to both on-premises Active Directory and Entra ID, must be managed as on-premises AD devices.

For Privilege Manager to function with Entra ID, you'll need to set up the following items within the Microsoft Azure portal:

- Create the Entra ID App Registration for Privilege Manager
- Add client secret
- Grant the application API permissions

## Create the Entra ID App Registration

To create the app registration:

1. Log into https://portal.azure.com using your Azure credentials with full admin rights.

2. Search for **App registrations**.

3. On the **App registrations** page, click **New registration**.

4. Give the application a meaningful display **Name**. You can change the name later.

5. As the **Supported account type**, select **Accounts in this organizational directory only (Recast Software only - Single tenant)**.

6. Click **Register**.

7. In the **Overview** pane that opens, copy the **Application (client) ID** and **Directory (tenant) ID**. You'll need to enter these later in your Recast Management Server.

## Add Client Secret

1. On the **App registrations** page, under **Manage**, click **Certificates & secrets**.

2. On the **Client secrets** tab, add a **New client secret**.

3. Add a client secret **Description** (ex. Privilege Manager service), choose when the secret **Expires,** and click **Add**.

> **NOTE**: You must create a new client secret before the current one expires and change the client secret for your Recast Management Server service connection to Entra ID.
>
> **TIP**: Schedule a support ticket, task or calendar entry before the expiry time to perform these actions.

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

4. Copy the client secret value to a clipboard and save it to a secure location, as you cannot see the client secret after navigating away from the page. You will need to specify the client secret if you modify Entra ID details in Privilege Manager, such as editing the display name of the Entra ID tenant.

## Add API Permissions for the Application

To add API permissions:

1. On the **App registrations** page, under **Manage**, click **API Permissions**.

2. Select **Add a permission**.

3. On the **Microsoft APIs** tab, click **Microsoft Graph**.

4. Add the following permissions:

| | |
|---|---|
| Application permissions | GroupMember.Read.All |
| | Device.Read.All |
| | User.Read.All |

5. Click **Grant admin consent for [Tenant Name]** and confirm the selection.

Once the Entra ID App Registration is done and you have recorded the **Application (client) ID**, **Directory (tenant) ID** and **Client secret**, you can then add a service connection from your Recast Management Server to Entra ID for Privilege Manager.