Recast

# Entra ID Setup for Privileged Access

Last Modified on 11.27.25

To create the app registration for Privileged Access:

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. If using **Credential provider** > **Local Account** > **Use alternative credentials with Azure AD**, enable **Allow public client flows**.

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

7. Click **Register**.

8. 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

To add the client secret for Privileged Access:

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. Privileged Access 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 Privileged Access, such as editing the display name of the Entra ID tenant.

---

## Add API Permissions

Recast

To add API permissions for Privileged Access:

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 **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 Privileged Access.

---

## Configure Application ID URI

To configure the Application ID URI for Privileged Access:

1. On the **App registrations** page, under **Manage**, click **Expose an AP**

2. Click to **Add** an application ID URI.

3. In the **Edit application ID URI** side panel that opens, enter the **Application ID URI**.

4. **Save** your changes.

---