Set Up Entra ID for Device Warranty Plugin

Last Modified on 08.20.25

For the Recast Device Warranty Plugin for Security Copilot to work with Entra ID, you'll need to complete these tasks within the Microsoft Azure portal:

- Register your Recast Management Server with Microsoft

  NOTE: if you've already created an App registration for Recast applications, such as Privileged Access, there's no need to create a new one.

- Add a claim
- Create a Copilot Gateway App role
- Grant Graph API permissions
- Add client secret
- Configure your application ID URI

Register your Recast Management Server with Microsoft

To create the App registration for your Recast Management Server.

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** as you will need to enter these later in your Recast Management Server.

Add a Claim

To add a claim to the App registration:

1. On the **Token configuration** tab in your app registration, click **Add optional claim**.

2. Select the **Access** radio button.

3. Select 'idtyp' from the listed claims.

4. Click **Add**.

Create a Copilot Gateway App Role

To create an app role for the Copilot Device Warranty Plugin:

1. On the **App roles** tab in your app registration, click **Create app role**.

2. Enter the following values for the app role:

- Display name: CopilotGateway.Connect
- Allowed member types: Applications
- Value: CopilotGateway.Connect
- Description: Allows the application to connect to Recast Copilot Gateway

3. Enable the **Do you want to enable this app role?** checkbox.

4. Click **Apply**.

Grant Graph API Permissions

To add required API permissions for the Copilot Device Warranty Plugin:

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. Grant the following permissions:

Application permissions	Device.Read.All
	User.Read.All
	OnPremDirectorySynchronization.Read.All

5. Click **Add a permission** again.

6. On the **APIs my organization uses** tab, search for your app registration.

7. Under **CopilotGateway**, grant the **CopilotGateway.Connect** permission.

8. Click **Add permissions**.

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

Add Client Secret

To add the 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**, choose when the secret **Expires,** and click **Add**.

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 the client secret value to set up your Recast Management Server and connect to Copilot Gateway.

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 Copilot Gateway .

Configure Your Application ID URI

To configure your application ID URI:

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