Device Warranty Plugin for Security Copilot

Last Modified on 10.16.25

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.
- $7.\ Under\ \textbf{CopilotGateway},\ grant\ the\ \textbf{CopilotGateway}. \textbf{Connect}\ permission.$
- 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.

Add Recast Device Warranty Plugin

To add the Device Warranty Plugin to your Microsoft Security Copilot instance:

- 1. On the Security Copilot webpage, click Sources (located near the Submit Prompt button in the chat textbox).
- 2. Scroll to the Custom section and click Upload Plugin.
- 3. Click Security Copilot plugin.
- 4. Enable Upload as a link.
- 5. Paste the following link into the link textbox: https://cpgwprod.recastsoftware.com/.well-known/manifest
- 6. As the File type, select 'yaml'.
- 7. Click Add.

Use Recast Device Warranty Plugin

Once you add the Recast Device Warranty plugin to Security Copilot, you can enter prompts in the chat textbox. Prompts that relate to device warranties should automatically map to the Recast Device Warranty plugin.

Prompts to Try

- What is my Recast Management Server version?
- When does the warranty expire for [device name]?
- What does the warranty cover for [device name]?
- Show me all device warranties expiring within the next week

NOTE: The plugin is currently forward-looking, returning results for warranties that have not yet expired.

Results

For some prompts, Security Copilot will return a summary of results. To see all the details, you can view the content in full-screen mode. There is also an option to **Export to Excel**.



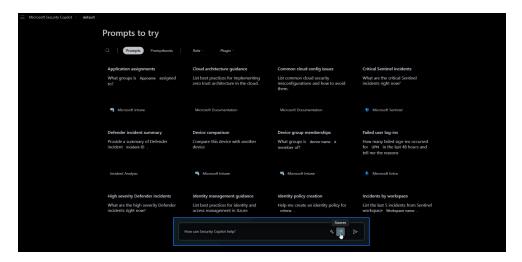
TROUBLESHOOTING TIP: If the plugin reports that it can't find a Recast Management Server connected for your tenant, testing the Copilot Gateway service connection from RMS should resolve the issue.

View/Edit Device Warranty Plugin Settings

After adding the Recast Device Warranty plugin to your Security Copilot instance, you'll find it listed under your available plugins.

To view or edit Recast Device Warranty plugin settings:

1. On the Microsoft Security Copilot webpage, click the Sources button in the chat textbox at the bottom of the page.



- 2. On the Manage sources > Plugins tab, scroll down to the Custom section to see the Recast Device Warranty plugin.
- 3. Click the Settings cog.

