Recast

Entra ID Setup for Patching

Last Modified on 12.03.25

For Right Click Tools Patching to work with Intune, you'll first need to complete some tasks within the Microsoft Azure portal.

Create Entra ID App Registration

To create the app registration for RCT Patching:

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

To add the client secret for RCT Patching:

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** (for example. Patching 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.

   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. You will not be able to see the client secret after navigating away from the page. You will need to specify the client secret whenever you modify Entra ID details in Patching, for example, if you want to change the display name of the Entra ID tenant).

Recast

Add API Permissions

To add API permissions for RCT Patching:

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**:

DeviceManagementApps.ReadWrite.All	Read and write Intune apps
GroupMember.Read.All	
DeviceManagementConfiguration.Read.All	Required to test an integration
Device.Read.All	Required to test the Azure Active Directory (Entra ID) service connection

5. Click **Grant admin consent for [Tenant Name]**.

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