Recast

Entra ID Setup for Patching

Last Modified on 2026-10-07

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

Create the Entra ID App Registration for Right Click Tools Patching

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 **Single tenant only – <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 for Right Click Tools Patching

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).

Add API Permissions for Right Click Tools Patching

Recast

Add API Permissions for Right Click Tools Patching

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.

Exclude RCT Patching from a Multi Admin Approval Access Policy

Intune Multi Admin Approval (MAA) access policies require that a second administrative account approve changes before they take effect. As of June 2026, Multi Admin Approval applies to API calls made by automation via the Microsoft Graph API.

If you're deploying or updating applications in Intune environments and want to avoid MAA enforcement, you'll need to exclude the RCT Patching app registration from the applicable access policy.

To exclude RCT Patching from an access policy:

1. In the Intune Admin Center, navigate to **Tenant administration** > **Multi Admin Approval**.

2. On the **Access policies** tab, open the policy to edit.

3. On the **Exclusions** tab, select the Add (+) button under **Apps**.

4. In the **Select apps to exclude** window, search for your RCT Patching app registration by its **Application (client) ID**.

5. Click the checkbox next to Right Click Tools Patching. The application will move to the **Selected** list.

6. Click **Select**. RCT Patching will appear under **Display name** on the **Exclusions** tab.

7. Click **Review + submit for approval**, then enter **Business justification** details, and submit the request.

Your request to exclude RCT Patching will display with a **Needs review** status until approved by a second policy approver.
