Recast

Entra ID Security Groups

Last Modified on 04.14.26

Use the **Entra ID Security Groups** tool to add devices to Entra security groups. This tool can be run on single and multi-selected devices from within Configuration Manager or on single devices in Intune (multi-device selection coming soon!) This tool requires a connection to your Recast Management Server and can only run over a Recast Proxy route.

Prerequisites

- Recast Management Server installed with Recast Proxy
- Service connection from your Recast Management Server to Entra ID (Azure Active Directory)
- Minimum Recast Software version: 5.10.2507.1103
- Minimum Right Click Tools for Intune browser extension version: 2.0.0.6

Recast Permissions

Plugin	Permissions
MicrosoftGraph	AddToEntraGroup GetEntraDevice GetEntraGroups RemoveFromEntraGroup GetDeviceGroupMemberships

Microsoft Permissions

Add the following Microsoft Graph API application permissions to the App registration for your Entra ID service connection.

- Device.Read.All
- Device.Read.Write.All
- Group.Read.All
- Group.Read.Write.All

For more information, see our article on setting up Graph API permissions for Right Click Tools.

Run the Entra ID Security Groups Tool

To run the tool:

1. Right-click on one or more devices.

2. Select **Right Click Tools** > **Console Tools** > **Entra ID Security Groups**.

3. Search for and select one or more Entra security group(s).

4. Click **Add to Selected Security Groups** and confirm that you want to add the device(s) to the group(s).