Manage User/Group Scopes

Last Modified on 11.18.24

A User/Group Scope limits a user or user group to running actions against the subset of users or devices included in the scope. You can add, edit, or remove scopes on the **Permissions** page in your Recast Management Server.

Add or Edit a User or User Group Scope

To add or edit a scope for an existing user or group:

1. On the **Permissions** page, click the Edit icon to the right of the user or group.

2. Under Assigned Roles, select a role, such as Administrators.

3. Enable the **Limit this user to specific objects** option.

4. Select a **Service Connection**.

5. Select the objects against which the user or group can run actions. For example, you can choose specific Configuration Manager collections and/or Active Directory OUs.

   NOTE: You must apply the scope separately for each service connection.

6. Click **Save**.

User/Group Scope Notes

- A scope that creates a subset of users will not impact actions related to devices.
- A scope that creates a subset of devices will not impact actions related to users.
- If a user or user group is included in multiple User/Group scopes, the user's/group's limiting rules will be an aggregate of all the applied scopes.

Remove a User or User Group Scope

To remove a user or group scope:

1. On the **Permissions** page, click the Edit icon to the right of the user.

2. Under Assigned Roles, select a role.

3. Disable the **Limit this user to specific objects** option.

4. Click **Save**.