Scopes

Last Modified on 12.16.24

A Recast Scope limits user permissions to a subset of devices or users. Scopes can be configured on the **Permissions** page in your Recast Management Server.

Common Uses

- Route Scope: Runs actions over a specified Recast Proxy or Fast Channel route only when target devices are included in the scope
- User/Group Scope: Limits a user or user group to running actions against a specified subset of users or devices included in a service connection

Scopes are created automatically in the background when a route is created or when a user is assigned a role and associated permissions that only allow them to perform tasks within a limited scope, which may include certain devices, users, AD OUs, or AD groups.

The read-only **Recast Scopes** page displays scopes that have been created in your environment, and indicates whether the scope came from actions taken on the Routes page or the Permissions page.

Manage Route Scopes

A Recast Route Scope allows actions to be run over a specified route only if the target devices are included in the scope. You can add, edit, or remove scopes applied to routes on the **Routes** page in your Recast Management Server.

Add or Edit a Route Scope

To add or edit a scope applied to an existing route:

1. On the **Routes** page, click the Edit icon to the right of the route.
2. In the Edit Route window that opens, enable the **Limit to devices** option.
3. Select a Configuration Manager or Active Directory **Service Connection**.
4. Select the devices to include in the scope.

   NOTE: You must apply the scope separately for each service connection.
5. Click **Submit**.

Remove a Route Scope

To remove a route scope:

1. On the **Routes** page, click the Edit icon to the right of the route.

2. In the Edit Route window, disable the **Limit to devices** option.

3. Click **Submit**.

Manage User/Group Scopes

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**.