Manage Route Limiting Rules

Last Modified on 03.28.25

A route limiting rule (previously known as a route scope) allows actions to be run over a specified route only if the target devices are within the defined limits. Adding a route limiting rule can be especially helpful where the environment includes multiple domains with varying trust levels.

You can limit a Recast Proxy Route to devices in one or more of the following:

- Active Directory - domain, OU, group
- Configuration Manager - site, device collection

Add or Edit a Route Limiting Rule

To add or edit a limiting rule 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.

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

5. Click **Submit**.

Route Limiting Rule Notes

Fast Channel Route

- You must configure a limiting rule for a Fast Channel route.
- You can only apply a limiting rule to a ConfigMgr service connection.
- You cannot apply multiple limiting rules concurrently.
- You can only run actions on devices that are Fast Channel-capable, meaning that Recast Agents are deployed to the devices.

Proxy Route

- Limiting rules set up for the proxy account user apply.
- If a device is included in multiple proxy route limiting rules, the device's limiting rules will be an aggregate of all the applied limiting rules.

Remove a Route Limiting Rule

To remove a route limiting rule:

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**.
