



Limiting Rules

Last Modified on 03.28.25

Limiting Rules Overview

Limiting rules are created automatically in the background when a route is created or when a user or user group is assigned a role granting permissions that only allow them to perform tasks within the defined limits, which may narrow permissions to certain devices, users, AD OUs, or AD groups.

Limiting Rule Types

[User/Group Limiting Rule](#) - Limits a user or group to running actions against a specified subset of users or devices

[Route Limiting Rule](#) - Runs actions over a specified Recast Proxy or Fast Channel route only if the target devices are within the bounds of the limiting rule

To better understand why and how to use limiting rules, watch Marty Miller's [Limiting Rules in Recast Management Server](#) video on the Recast Software YouTube channel.

Manage User/Group Limiting Rules

A user or user group limiting rule (previously known as a scope) restricts a user or user group to running actions against a specified subset of users or devices. This type of limiting rule can be used, for example, to give a Help Desk group permission to run actions against only workstation devices.

You can limit a user/group to running actions against one or more of the following:





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

Add or Edit a User or User Group Limiting Rule

To add or edit a limiting rule for an existing user or group:

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

Recast Users

Name	Identifier	Is Group	Actions
Administrators	0-1-0-07-00000000-0000-0000-0000-00000000-0000	True	 
Low Permission User	0-1-0-07-00000000-0000-0000-0000-00000000-0000	False	 

2. In the **Role Assignments** window that opens, under Assigned Roles, select a role.
3. Enable the **Limit this user to specific objects** option.
4. Choose a Configuration Manager or Active Directory **Service Connection**.

Assigned Roles

LAPS

Limit this user to specific objects:

Service Connection:

Choose a service connection

Save

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 limiting rule separately for each service connection.

6. Click **Save**.

User/Group Limiting Rule Notes

- A limiting rule that creates a subset of users will not impact actions related to devices.
- A limiting rule that creates a subset of devices will not impact actions related to users.
- If a user or group is included in multiple user/group limiting rules, the user's/group's limiting rules will be an aggregate of all the applied limiting rules.
- If multiple limiting rules are set for a user or group, only one limiting rule needs to be true in order for the validation to pass. For example, if a user is in the limiting rule group, limiting rules applied to the group will also apply to the user.
- Recast Builder actions are permissioned separately. If an action is a **Device Action Type** or **User Action Type**, the device or user value must pass validation. If the action is a **Generic Action Type**, it will remain without a limiting rule.

Remove a User or User Group Limiting Rule

To remove a user or group limiting rule:

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**.

Manage Route Limiting Rules

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**.
-