



# Remove Permanent Administrator Permissions

Last Modified on 03.17.25

When **Remove current permanent admin permissions** is enabled, Privilege Manager will add the configured users and groups to local Administrators group. All other users and groups will be removed from Administrators group.

By default, Privilege Manager will add built-in Administrator and Temporary Administrator (if configured in Temporary Admin step) to local Administrators group. You can add additional users or groups to Administrators group by clicking **Add Group Rule**

## Default configuration



## Remove current permanent admin permissions

By default, all users and domain groups will have their current permanent administrator permissions removed and replaced with temporary administrator permissions. You can add a group rule to change the users or domain groups that will retain permanent administrator permissions on target devices.

Remove current permanent admin permissions

[+ Add Group Rule](#)

Drag a column header and drop it here to group by that column

Actions	Local Group	Member	Active	Valid until
	Administrators	Temporary Administrator	True	Indefinitely
	Administrators	Administrator	True	Indefinitely

1 - 2 of 2 items

Step 4 of 4

[Previous](#) [Done](#)

If **Remove current permanent admin permissions** option is unchecked, Privilege Manager won't create any Group Rules during the initial setup.

**NOTE:** You can also add, remove or edit the policies used by target devices by going to the **Group Rules** page after the initial setup.

Once you've completed the default configuration steps, click **Done**.

Specified devices will receive your configured rules, the Recast Management Server navigation panel will display the **Agents**, **Reports**, and **Configuration** sections in Privilege Manager, and the [Target Groups](#) page will open.