Initial Setup

Last Modified on 10.25.23

The first time you expand the Privilege Manager section in the Recast Management Server interface, you'll only see one option, **Setup**.

Clicking on **Setup** opens the **Default Configuration** workflow that will guide you through choosing devices that will use Privilege Manager, adding the temporary administrator function, setting up passwords, and removing current permanent admin permissions.

Choose Devices

As a first step, you'll select the devices which will follow the Privilege Manager rules you set up.

Options:

- **All agents** includes all devices where Recast Agent is installed and licensed for Privilege Manager.
- **Specify target devices** allows you to select a set of devices.

  To specify target devices:

  1. Click **Add Target**.

  2. In the side panel that opens, you can choose to specify a target based on devices in Active Directory (domains, OUs, groups, single agents, single devices) or Azure Active Directory (tenants, groups, single agents, single devices).

Before attempting to connect to third-party services, ensure that Recast Proxies are in place on the Service Connections page.

Add Temporary Admin

By enabling temporary administrator functionality, you can grant selected users admin privileges for a specific amount of time just when needed.

To implement the temporary admin function:

1. Confirm that the **Implement temporary administrator functionality** option is enabled.

2. Enter the **Display name** and **Login name** to be used on target devices for the temporary user account.

NOTE: On the **Self Service Rules** page, you can give specific users or domain groups self-service capabilities on devices.

Randomize Passwords

You can choose to randomize the password on the built-in Administrator account, or on a custom account you have already created on the target devices.

Options:

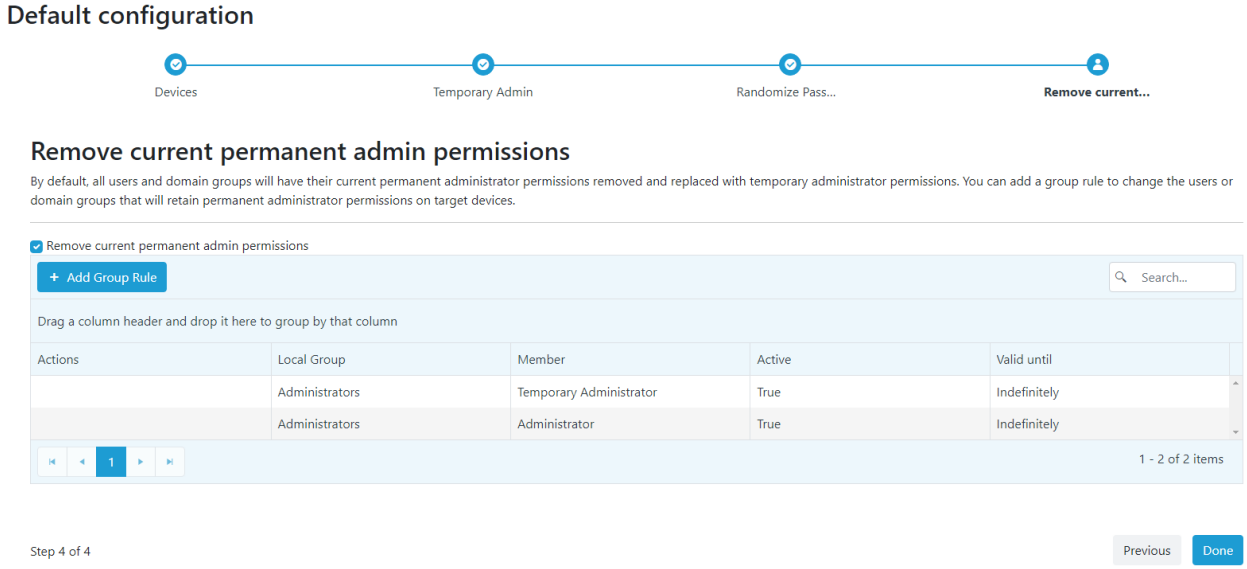
- Randomize local admin account password (default)
- Use built-in Administrator account
- Use custom local account

NOTE: You can skip this step if using LAPS for password management.

Remove Permanent Permissions

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**



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.