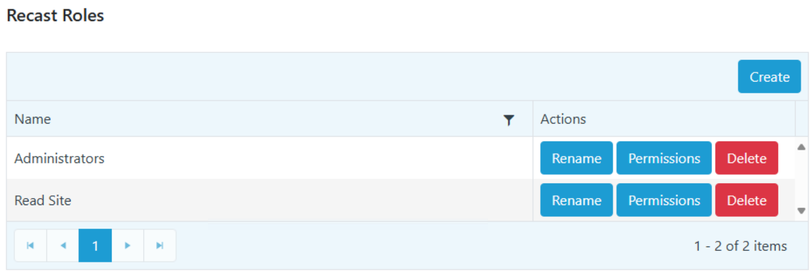
RECAST SOFTWARE

User Permissions

Last Modified on 02.27.25

To view or edit the permissions associated with a Recast role:

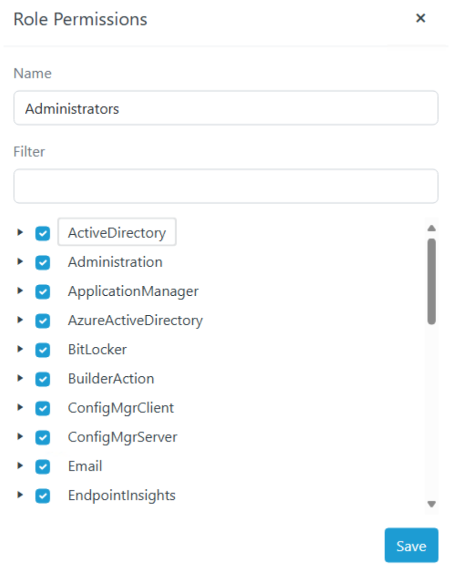
1. Under Recast Roles, click **Permissions** to the right of the role.



Recast Roles

Name	Actions
Administrators	Rename Permissions Delete
Read Site	Rename Permissions Delete

2. In the Role Permissions window that opens, expand categories to view or edit individual permissions.



Role Permissions

Name: Administrators

Filter:

- ☑ ActiveDirectory
- ☑ Administration
- ☑ ApplicationManager
- ☑ AzureActiveDirectory
- ☑ BitLocker
- ☑ BuilderAction
- ☑ ConfigMgrClient
- ☑ ConfigMgrServer
- ☑ Email
- ☑ EndpointInsights

Assign Roles to Users

You can grant users or user groups Recast permissions by assigning them a specific role, such as an Administrator role. Your Recast software must be connected to Recast Management Server to set up role-based permissions.

Add an Active Directory User or User Group

To add an AD user or user group:

1. In your Recast Management Server, navigate to **Administration** > **Permissions**.

2. Click **Add User** or **Add Group**.

3. In the window that opens, search for your AD name or AD user group and click the **Add** button.

> **NOTE**: You can include a **wildcard (*)** to facilitate your search.
>
> Wildcard examples:
>
> - **John Connor** returns strings that match exactly
> - **John C*** returns strings beginning with 'John C', such as '**John C**onnor', '**John C**onnors', and '**John C**ranston'
> - ***Connor** returns strings ending with 'Connor', such as 'John **Connor**' and 'Carol O'**Connor**'
> - ***Support*** returns strings that include 'Support' plus whatever is on the left and right, such as 'Customer **Support** Team' and 'Enterprise **Support** Group'

Assign a User a Role

Each user must be assigned at least one role. To assign Right Click Tools permissions using a role template, see Custom Role Templates for Right Click Tools.

To assign a user an Administrator's role:

1. On the **Permissions** page, click the Edit icon to the right of the user.

2. Under **Role Assignments**, select **Administrators**.

3. If desired, add a limiting rule that restricts user permissions to a set of devices by enabling **Limit this user to specific objects** and selecting a **Service Connection**.

4. Click **Save**.

NOTE: Beginning with Recast Software Version 5.9.2502.2105, you no longer have to set a **Refresh Interval** to repopulate your limiting rules (formerly known as scopes). The scheduled Discovery Sync will keep your service connection data up to date.

Custom Role Templates for Right Click Tools

Custom role templates offer a quick way to create permission sets for Right Click Tools users. You can find three custom role templates in your Recast Management Server and then adjust to suit by adding or removing individual permissions.

The following roles are available on the Recast Management Server **Permissions** page:

- **RCT Read Only Analyst** - This security role grants users read access to all of the Right Click Tools and web dashboards. This includes the Endpoint Insights Report Viewer role.

  For the complete list of permissions granted with this role, see Read-Only Analyst Role Permissions.

- **RCT Remote Software Center** - This security role grants users access to all the actions within the Right Click Tools Remote Software Center.

  For the complete list of permissions granted with this role, see Remote Software Center Role Permissions.

- **RCT Content Distribution Monitor Dashboard** - This security role grants users access to all the actions within the Right Click Tools Content Distribution Monitor (for Configuration Manager).

  For the complete list of permissions granted with this role, see Content Distribution Monitor Dashboard Role Permissions.

To assign a custom role to a user or user group:

1. On the **Permissions** page, click the Edit icon to the right of a user/user group.

2. Under **Role Assignments**, select RCT Read Only Analyst, RCT Remote Software Center, or RCT Content Distribution Monitor Dashboard.

3. If desired, add a limiting rule that restricts user permissions to a set of devices by enabling **Limit this user to specific objects** and selecting a **Service Connection**.

4. Click **Save**.