Link to article: https://discover.claromentis.com/knowledgebase/articles/845/policy-manager-permissions-explained

Policy Manager: Permissions Explained

In Policy Manager, we usually want to distinguish between end users who will simply read and/or accept policies and policy administrators who will manage them.

- **End users:** The primary actions are to read and, where required, accept policies. They should be granted **View** rights only for all relevant policy categories and the policies within them. If they also need to acknowledge or accept policies, you can additionally assign the **Target Distribution** permission.
- **Policy Administrators:** The main responsibility is to create and maintain policies. They should be granted permissions to **Add Policies** within each category, along with additional rights to manage those policies.

We'll detail how administrators can set this up and what each permission means.

Where are permissions set in Policy Manager?

User permissions in Policy Manager are set in two areas:

1. On the admin side by application administrators

2. On the front-end, per policy, by the users creating them

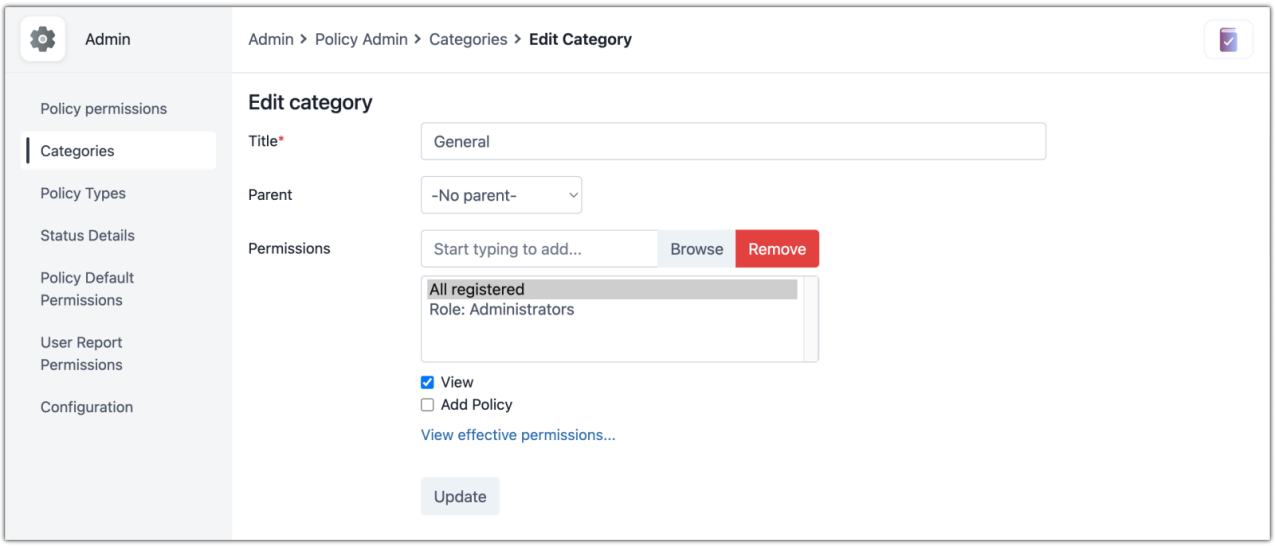
1. On the admin side by application administrators

In the Categories tab

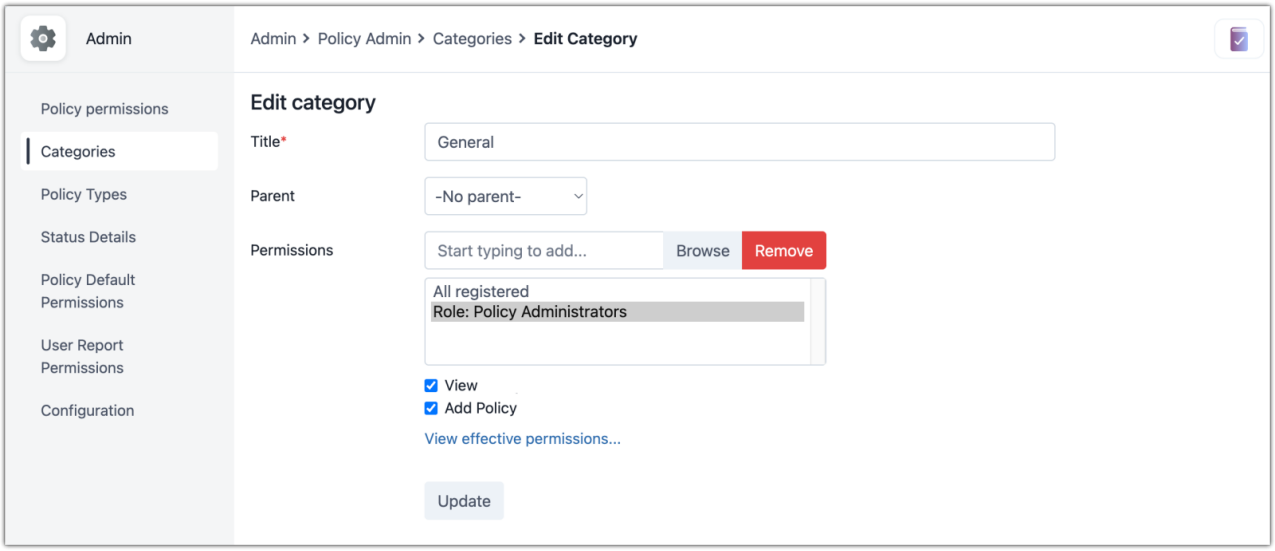
Your administrators must set up the admin side of the application before content can be added.

In the **Categories** tab, they'll add the categories where users will create policies.

- **End Users:** Ensure relevant users (e.g., All Registered), or other roles/groups have the **View** permission to all relevant categories.



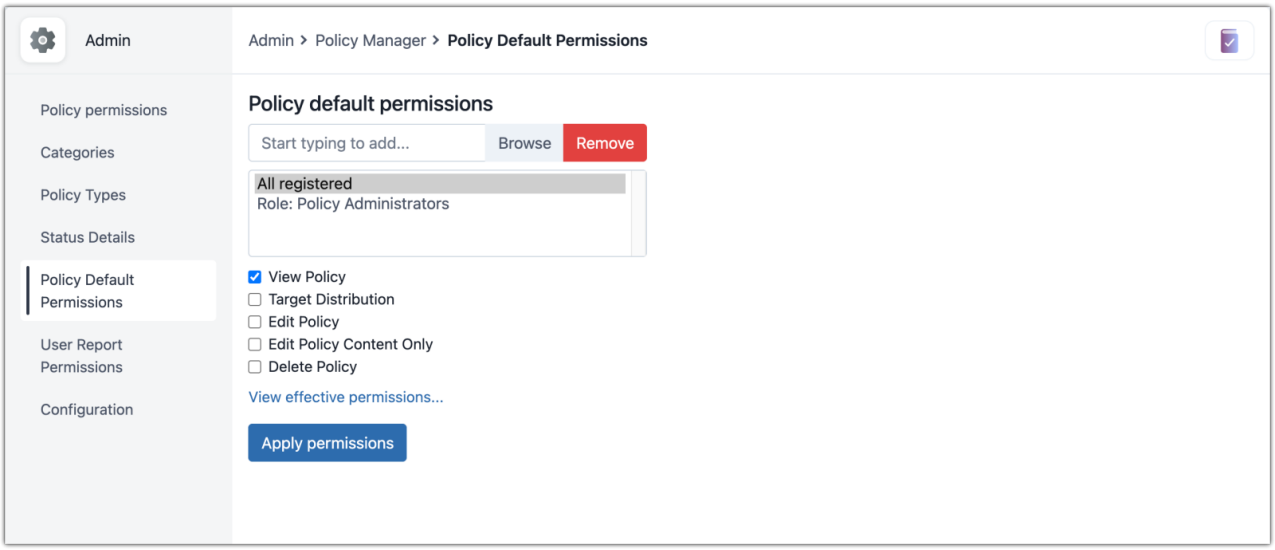
- **Policy Administrators:** Ensure your People Role created for Policy Administrators (or similar) is given both the **View** and **Add Policy** rights to all categories.



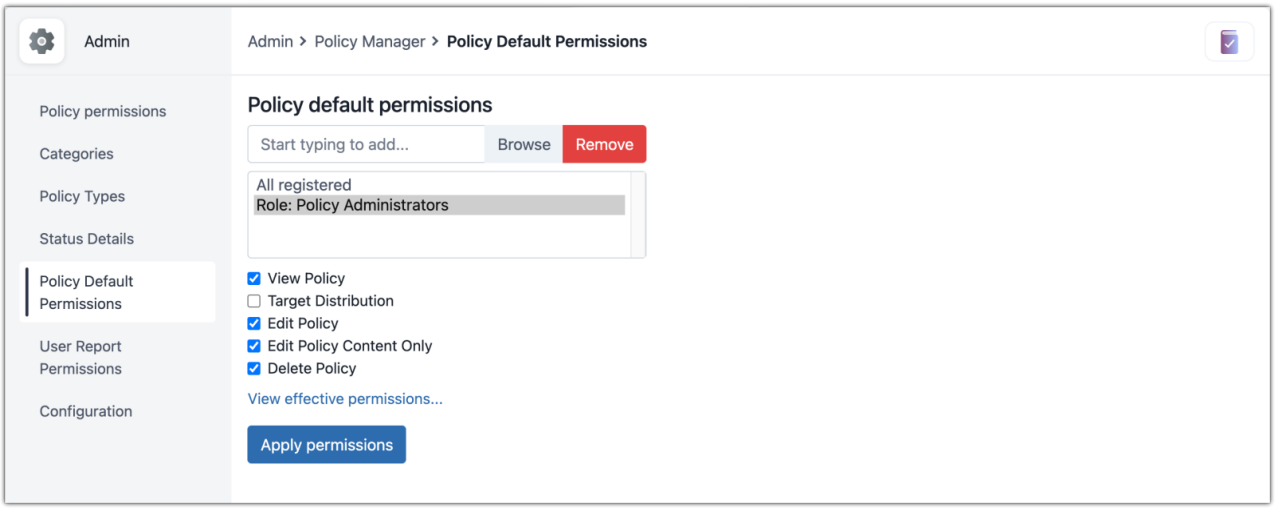
In the Default Policy permissions tab

The permissions will auto-populate when a new policy is created to help speed up the process and keep permissions static across policies.

- **End users:** Ensure relevant users (e.g., All Registered), or other roles/groups have the **View** permission to all relevant categories, and **Target Distribution** if they should accept policies.



- **Policy Administrators:** Ensure your People Role for Policy Administrators (or similar) is given all permissions (apart from **Target Distribution** unless you need them to accept the policies they manage).



2. On the front-end, per policy, by the users creating them

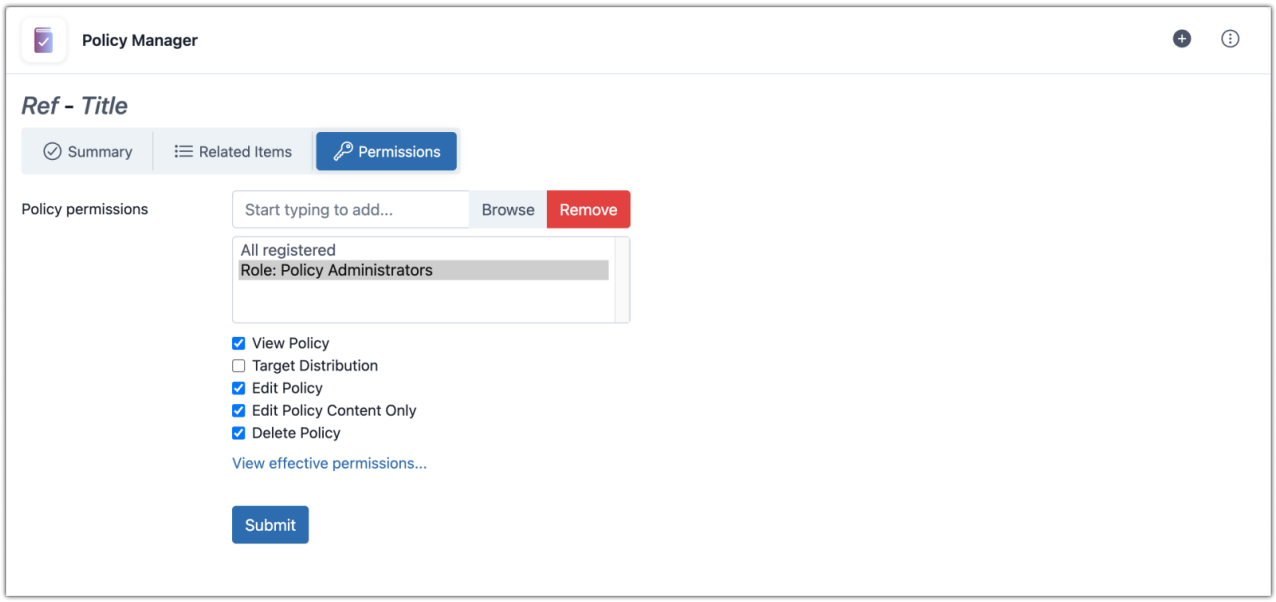
Now that the admin setup is complete, Policy Administrators can start creating policies on the front-end.

They'll select a category the policy will appear in, and the **Permissions** tab will automatically populate with the permissions set in the default tab on the admin side.

If the Policy creator does not change any of the permissions, the default ones as set in 1. will ensure end users can see (and possibly accept) the policy whilst administrators can edit and manage it.

If the creator decides to change the permissions from the default, then they're in control of the impact this has on who can see it and the level of interaction they have.

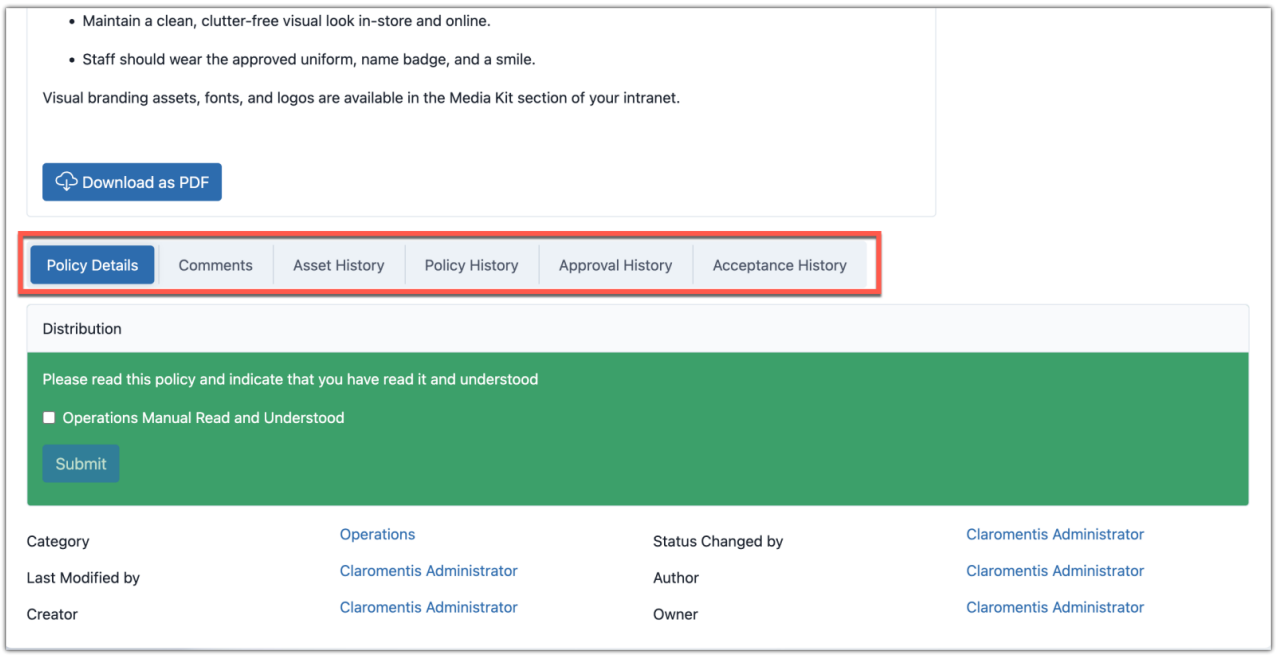
What does each permission mean?



- **View Policy:** The policy will be visible to the user
- **Target Distribution:** The user will be prompted to read and accept the policy
- **Edit Policy:** The user can make changes to the policy's properties, content, permissions and see acceptance status.
- **Edit policy content only:** The user can edit the body content of the policy
- **Delete Policy:** The user will be able to remove the policy

Q: How does this change what a user can see in a Policy?
Extra information about a policy can be viewed by users with appropriate permissions, as detailed in the table.

Generally, end users will only see policy details through their **View** rights, whilst administrators can see all other tabs as they have all other permissions.



Tab	Policy Details	Comments	Asset History	Policy History	Approval History	Acceptance History
View Policy	✓	✗	✗	✗	✗	✗
Target Distribution	✓	✗	✗	✗	✗	✗

Edit Policy	✔	✔	✔	✔	✔	✔
Edit Policy Content only	✔	✔	✔	✖	✖	✔

Q: What if a user reports that they cannot see a Policy?
First, check they have permissions to view the category the policy is saved under on the admin side via **Admin > Policy Manager > Categories**.

If they have this, edit the policy itself and open its permissions tab to check they have the**View** rights.

Q: What if a user reports that they cannot edit a Policy?
Edit the policy in question and check that they have the **Edit Policy** rights.

Last modified on 22 April 2026 by Veronica Kim

Created on 20 March 2026 by Hannah Door
Tags: permissions, policy, policy manager