Policy Manager: Admin Overview

Application administrators of Policy Manager need to set up the admin side of the application before it can be used.

In particular, the category and default policy permissions tabs need to be configured before content can start to be added.

Once the application has content in it, administrators can use the admin side controls to assist in the ongoing management of the policies over time.

This guide will cover all tabs available on the admin side and what they control.

The admin side

Head to Applications > Admin > Policy Manager to see all tabs.

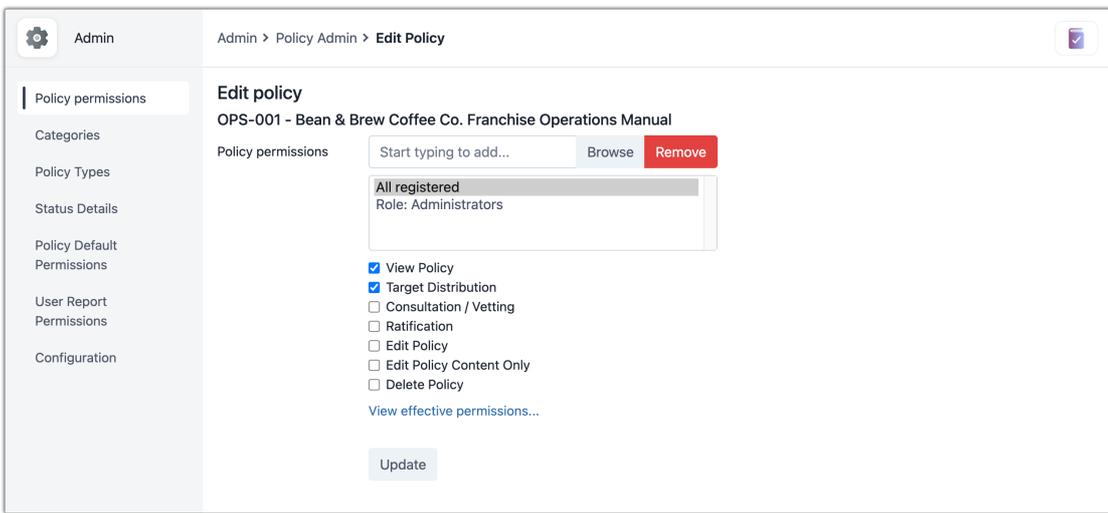## - Policy Permissions

This tab will be opened by default.

From here, administrators can see all policies and edit their permissions if needed.

A keyword and advanced search are available at the top of the screen.

Click the key symbol to edit the permissions for a policy.

Click the bin icon to delete a policy. (This is a permanent change and data cannot be retrieved) As there is no trash can in Policy Manager, consider archiving a policy rather than deleting it.
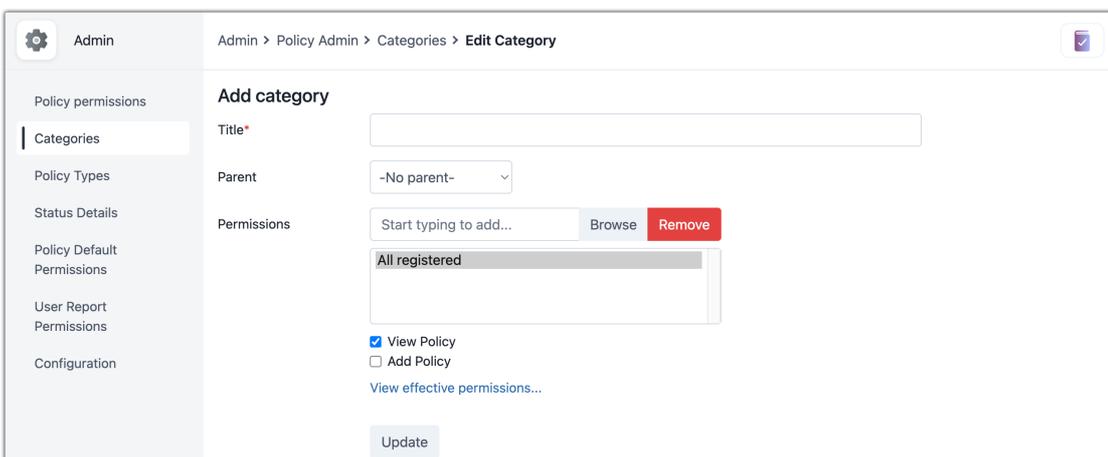
- Categories

Here, categories that policies will be saved under can be created.

Parent and subcategory structure can be set up to best organise your content.
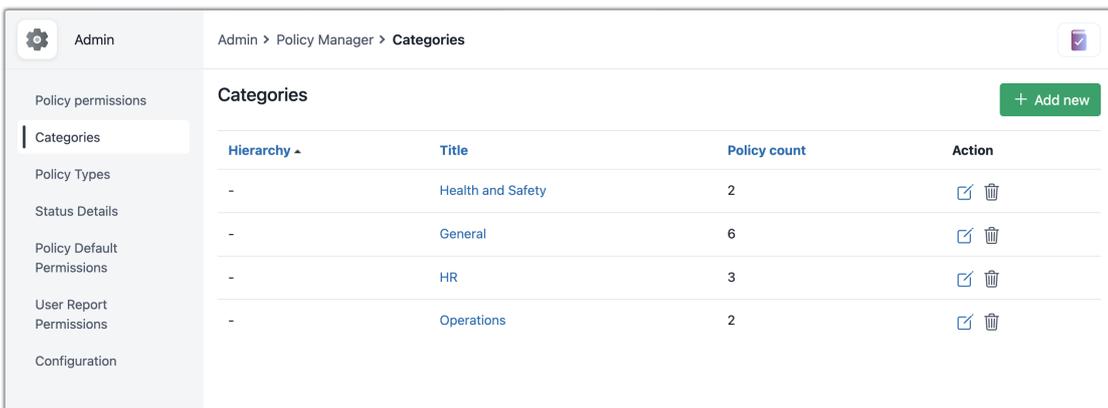
Consider the categories your company needs and create these; they will appear on the front end for users to create policies within.

The category is the first place a user needs permission to view content, so ensure you enter the appropriate users/roles/groups with permissions to view and or have the ability to create a policy within it.

Over time, new categories can be created, or administrators can change the permissions set on each category as needed.

On the front end, users with permissions to create policies in a category will see it listed when they are adding new ones.

Categories also act as a filter to show only policies saved under the one clicked on
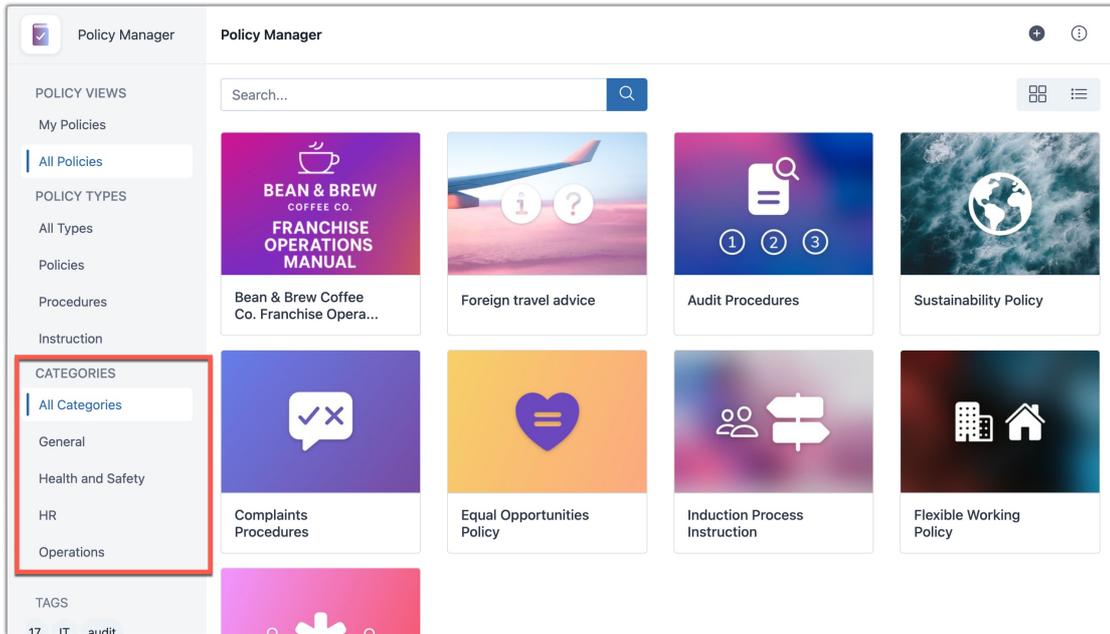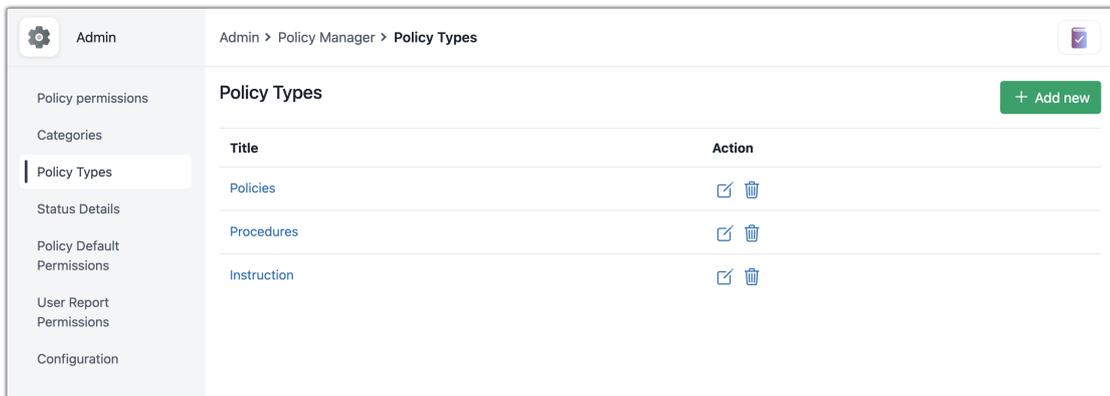

- Policy types

These are optional to create and attribute to policies.

They allow for further differentiation for filtering on the front end if the categories already in use are not enough.

There are no permissions tied to policy types.

Users with permissions to create policies will be able to see all types listed on the front end and be able to attribute them to their policies if applicable.

The types will appear on the front end for users to click on and see policies with that label.
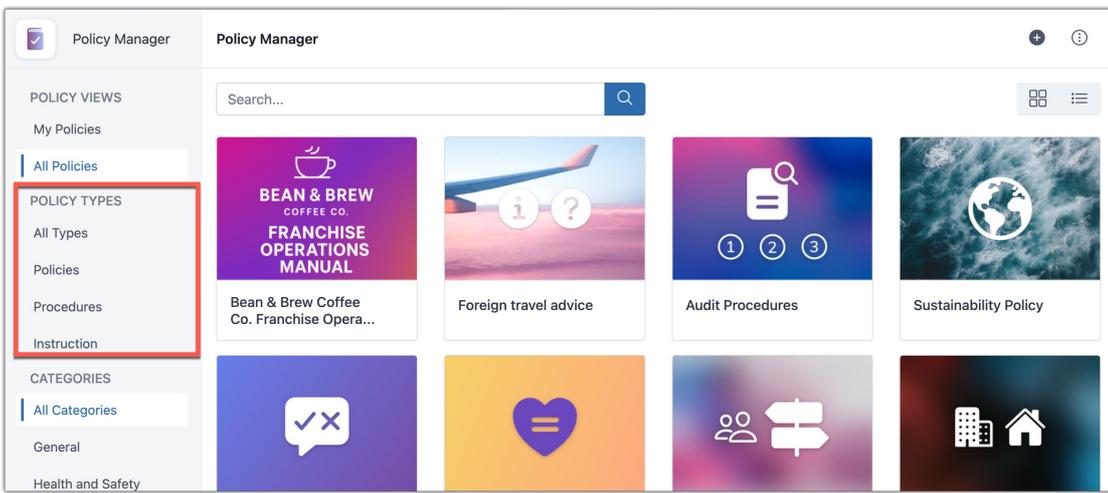
- Status details

This tab is where an approval process can be set up; our guide that covers this in detail is here.
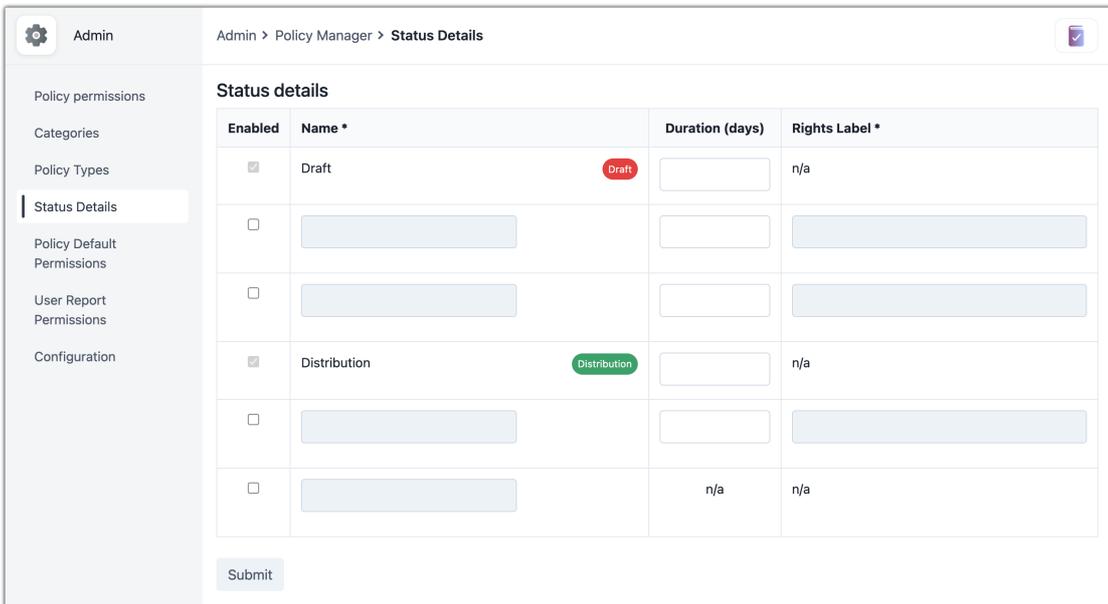
A 'draft' and 'distribution' status are hardcoded in this area and cannot be removed, as they are fundamental for Policy Manager to work.

Administrators can add more statuses to create an approval process if they wish.

- Default policy permissions

A very important tab to set up before Policy content starts to be added.

The permissions entered here will automatically pre-populate for any new policy that is created.

Which means what administrators enter here will speed up the policy creation process significantly, as usually the same users/roles/groups are needed across the majority of policies.
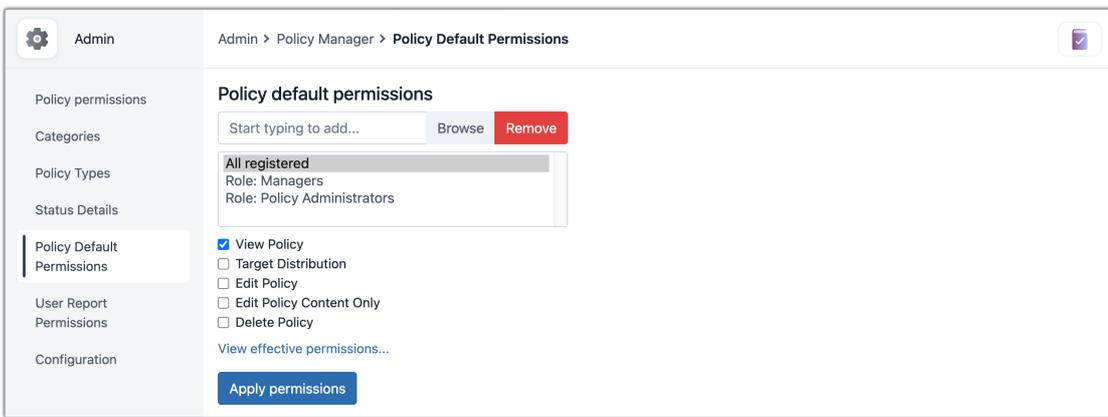
We recommend using 'All registered ' with the ability to 'view', then a 'Policy administrator' role or similar with all admin permissions.
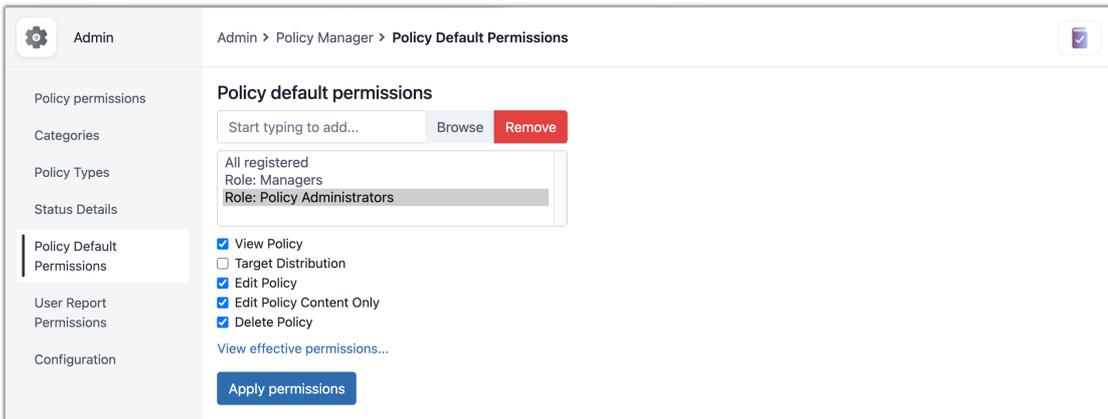
This means that when users with permissions create policies, these permissions will already be entered, and they can simply tweak what is already there to best fit their policy.

This ensures consistency across policies as the same users/roles/groups have been used, which means there should be no access issues.

One important thing to note is that the Policy Creator will need to set the 'target disruption' if needed, or administrators can include that permission in the default.

☐**Tip:** We recommend establishing an Intranet role specifically for granting administrators policy permissions. Make sure to include this**Policy Administrator** role in the permissions list for every policy, granting it full rights. This approach simplifies ongoing management as new policies are added, eliminating the need to assign permissions to individual users each time.

- User report permissions

Here, administrators can enter users/roles/groups who should have access to policy reports on the front end.
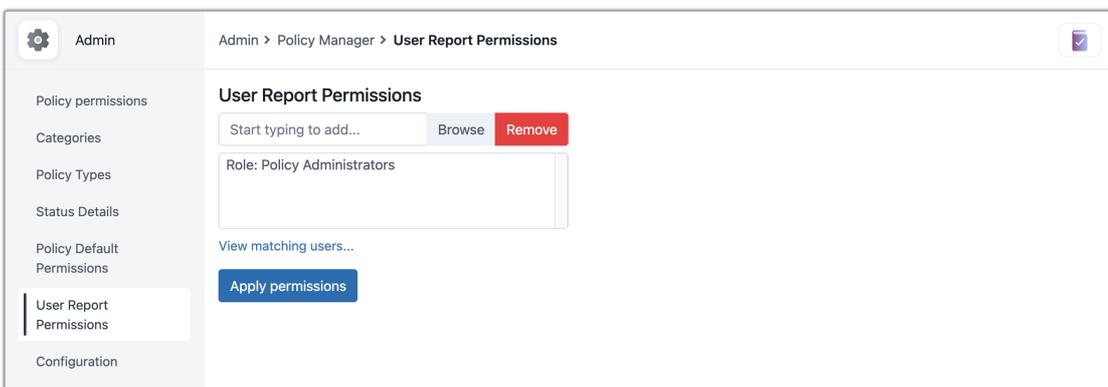
- Configuration

Administrators can adjust features related to the visibility and accessibility of the Policy Manager.

- Policy reference pattern: Enter a code to appear against all policies when created
- Policy items per page: How many policies to show per page
- Allow minor edits: Select 'yes' if edits can be made to live policies to fix spelling or other errors
- Filters display: Show or hide filters on the left of the screen when in a policy
- Landing page: Set which tab is opened by defauly (If 'no' the default tab will be 'My policies')
- Show download as PDF: Set whether a button should download polciies to PDF appears

Created on 19 March 2026 by Hannah Door

Tags: admin, administrator, policy