Link to article: https://discover.claromentis.com/knowledgebase/articles/492/policy-manager-admin-overview

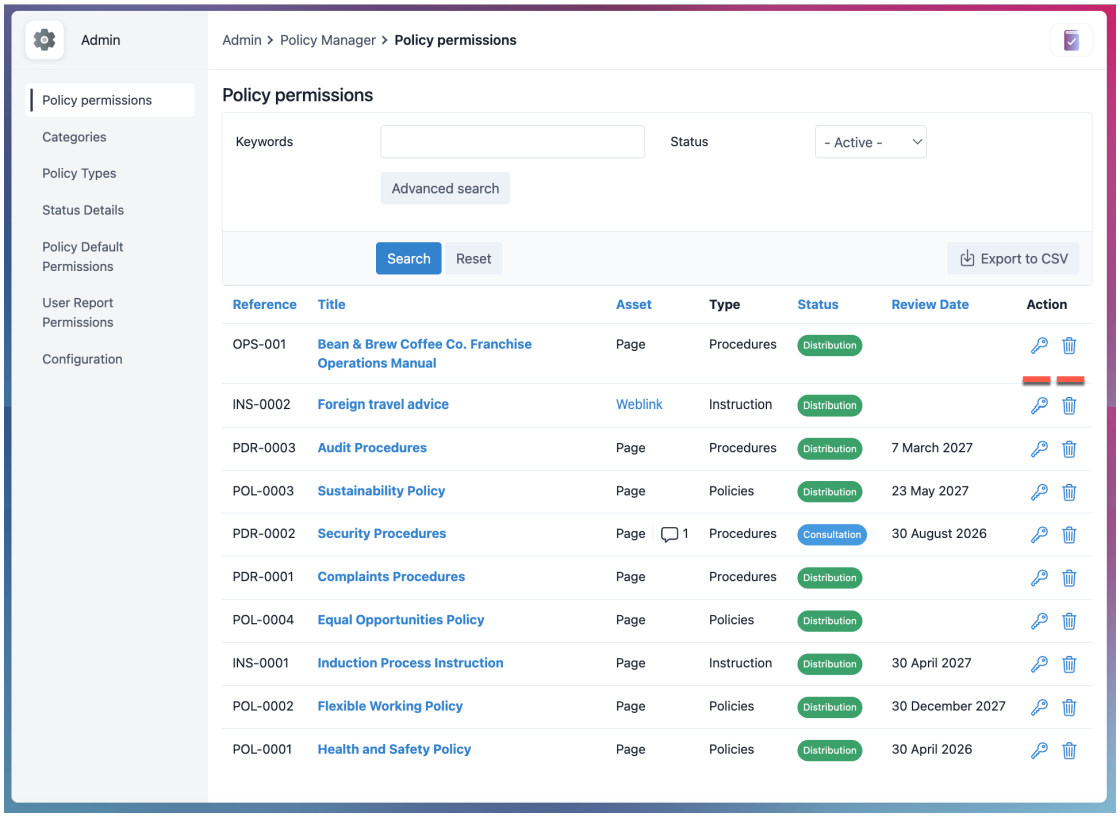
Policy Manager: Admin Overview

The Policy Manager Admin panel has a variety of configuration options.

Policy Permissions

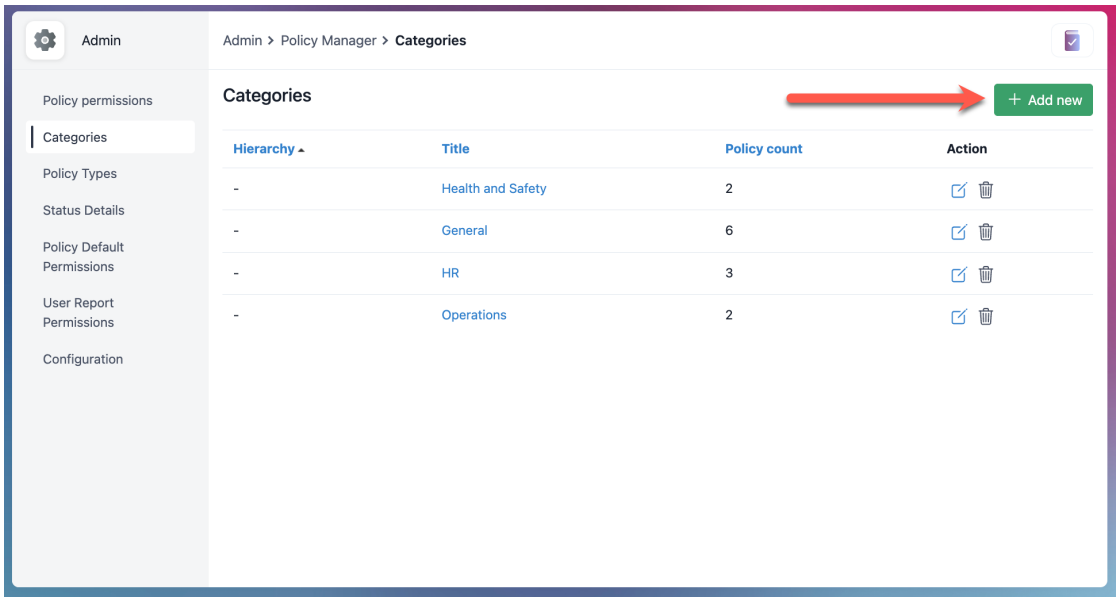
The **Policy Permission** section allows users to adjust the permissions for any pre-existing policy.

To change permissions for a certain policy, select the key (**Edit**) icon, or to remove it permanently, click the trash can (**Delete**) icon.



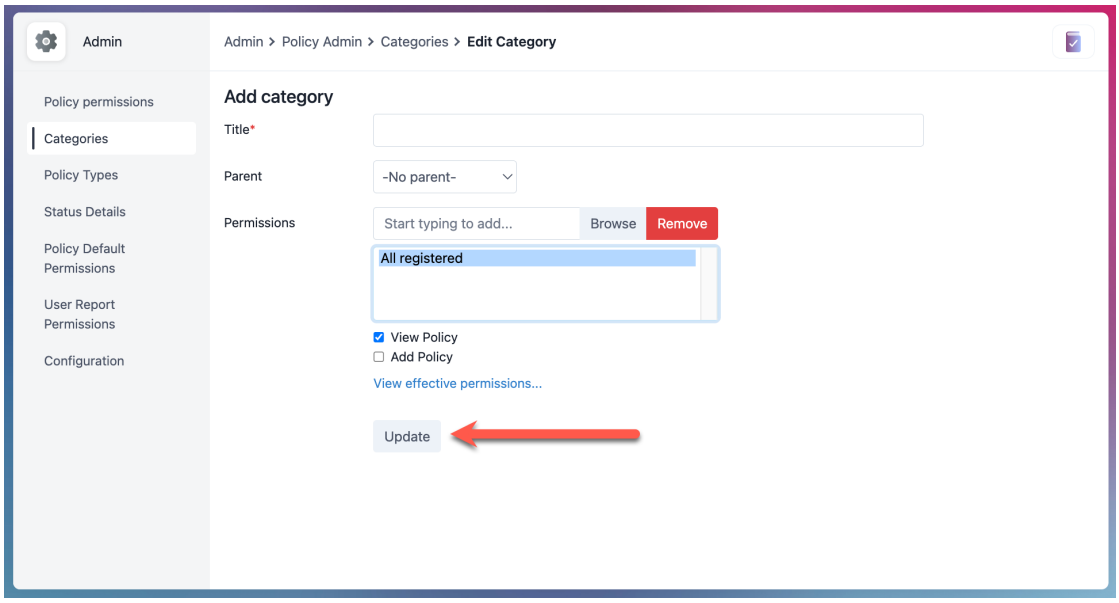
Categories

The **Categories** section allows users to create new categories for structuring the policies and to enhance search functionality.



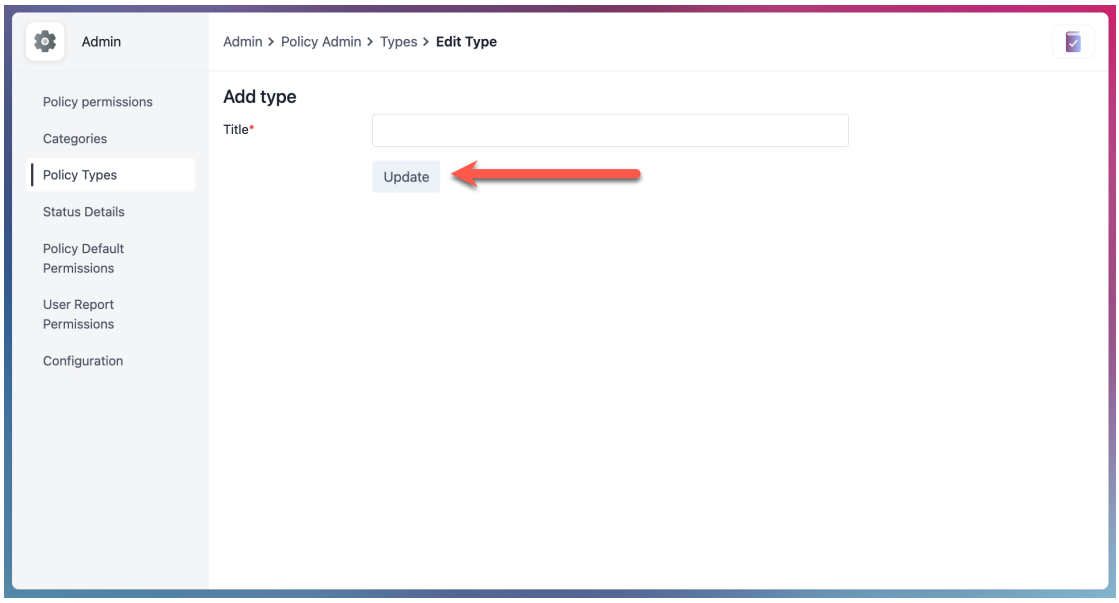
When adding a new category, you can define who has permission to view it and add policies to the category.

If other categories already exist, you may also assign a Parent category, making the new category a sub-category, allowing for more granular organisation.



Types

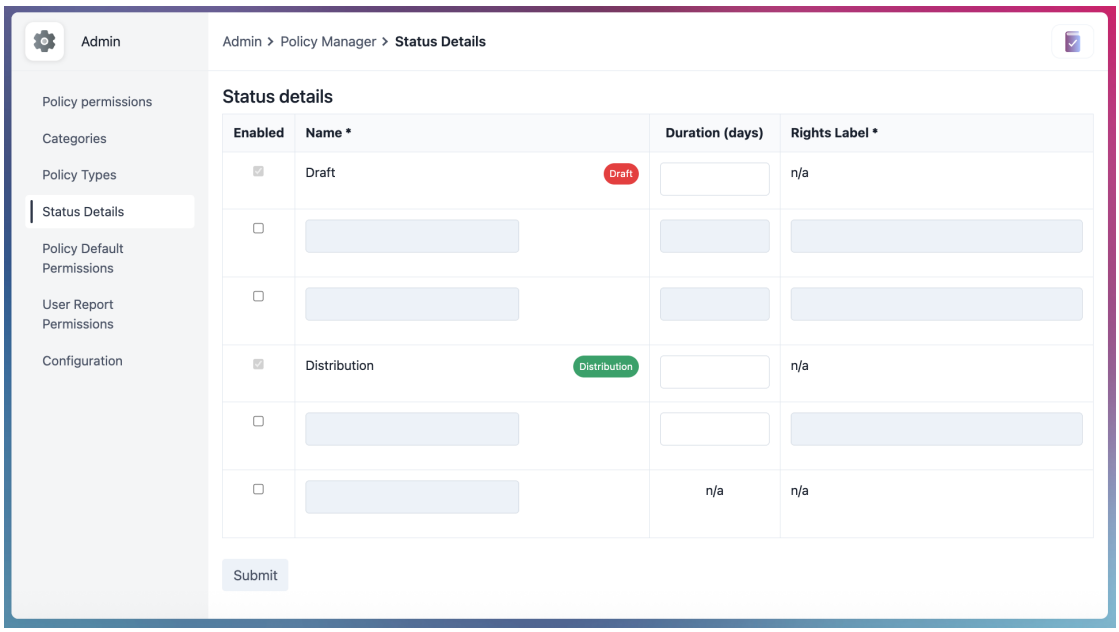
The **Type** section allows you to further filter and sort the policies. However, unlike Categories, you cannot assign permissions based on newly created types.



Status Details

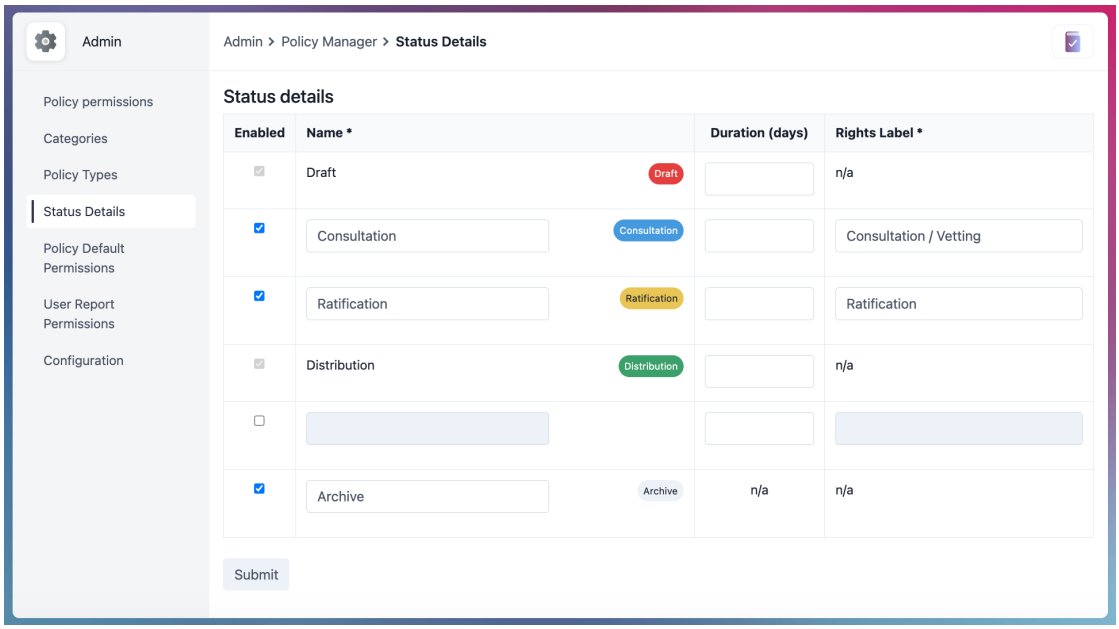
The **Status Details** section allows for the creation of new statuses to be added to your newly created policies, allowing for an approval workflow.

By default, only the **Draft** and **Distribution** statuses are available. However, you can add up to two additional statuses between these, as well as two more after Distribution.



The purpose of these statuses is to establish an approval process and an archiving process.

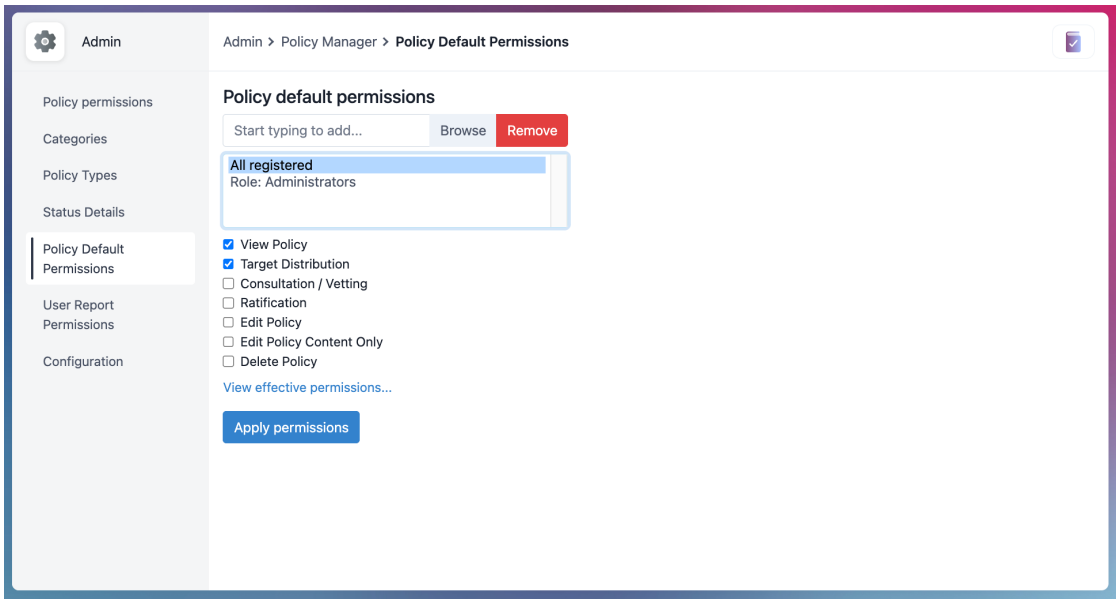
Each status needs to be checked, named, and assigned a **Rights Label**, specifying how it appears in permissions. You can also set a default duration for each status. This triggers a reminder to review or update the status when the duration expires.



Default Policy Permissions

The **Default Policy Permissions** section enables you to set the standard permissions for all future policies you create. Any custom statuses will automatically be included for you to assign permissions.

Once set, these permissions are automatically applied to all new policies. While you can still adjust the permissions for each policy individually, setting these defaults ensures a consistent starting point that you can adjust as needed for specific policies.

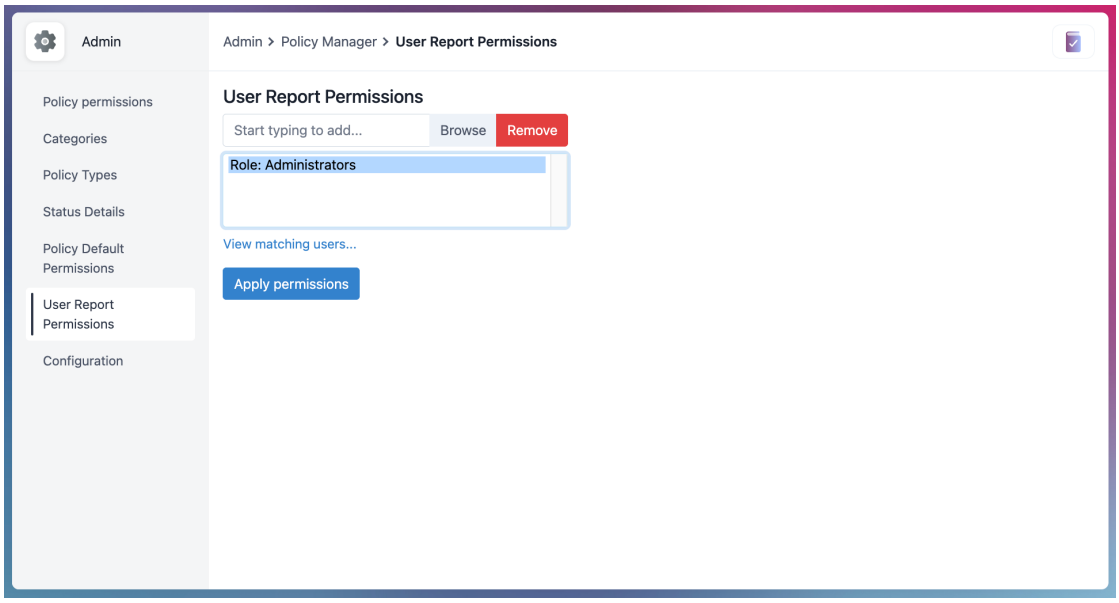


Tip: We recommend establishing an Intranet role specifically for granting administrators policy permissions. Make sure to include this **Policy Administrator** role in the permissions list for every policy, granting it full rights. This approach simplifies ongoing management as new policies are added,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

User Report Permissions

The **User Report Permissions** allows you to grant access to the reporting tools from the front-end.

With Policy Manager Reports, you can track whether users have accepted relevant policies by running customised reports with optional filters.

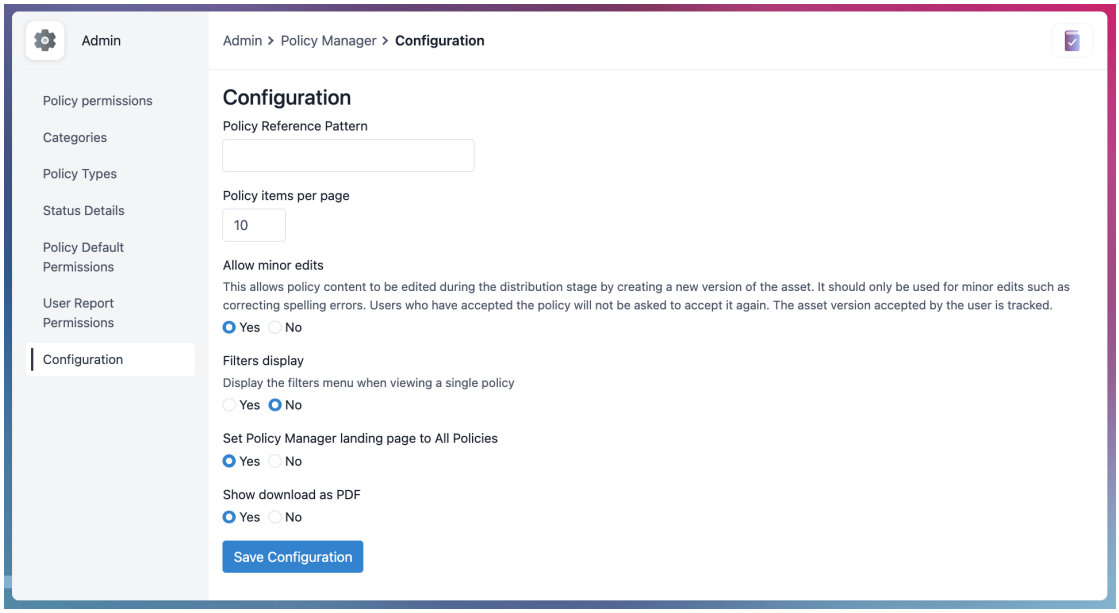


Configuration

The **Configuration** section allows users to adjust features related to the visibility and accessibility of the Policy Manager.

Users can set a default **Policy Reference Pattern** so all policies are consistent without re-typing the format each time. You can also specify how many policies appear per page on the front-end.

Another setting involves enabling **Minor Edits** to policies. When enabled, it allows small changes, such as fixing typos, without creating a new version. Since accepting a policy can be a legal requirement, any significant changes must result in a new version.



Created on 25 November 2025 by Veronica Kim
Tags: admin, administrator, policy