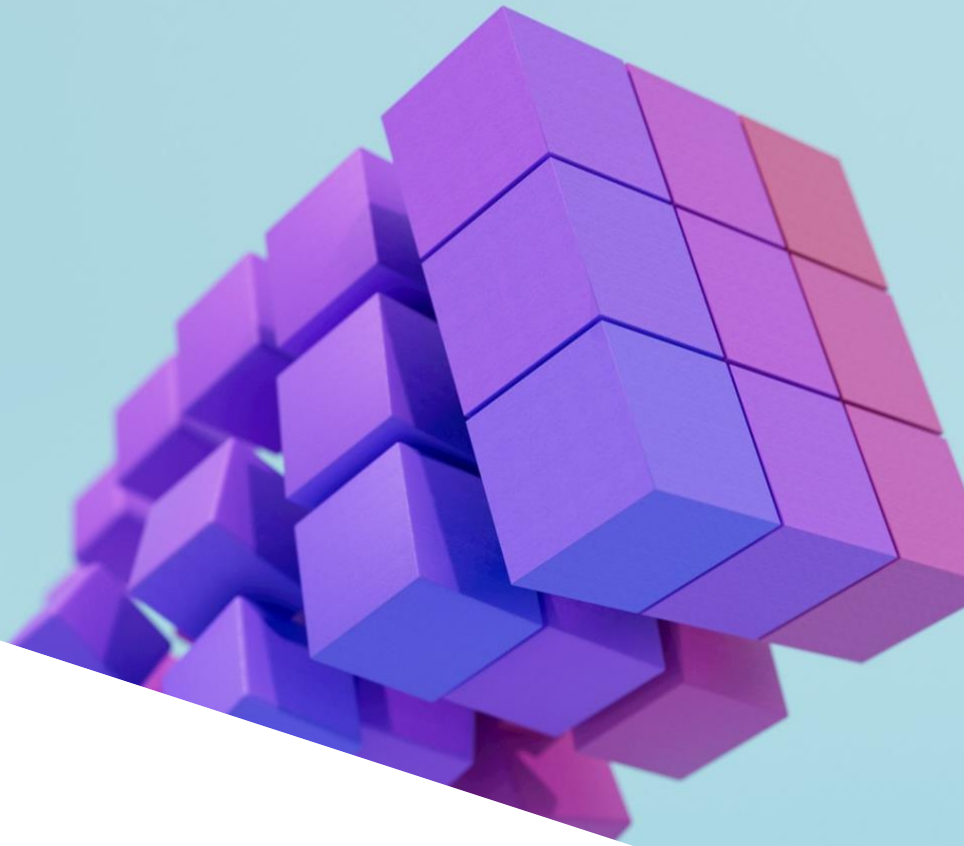


POLICIES – GETTING STARTED GUIDE

Learn More

Table of Contents

1. Policies – Work in Progress & Published Policies

Policies appear under two main tabs, based on their status:

1.1. Work In Progress

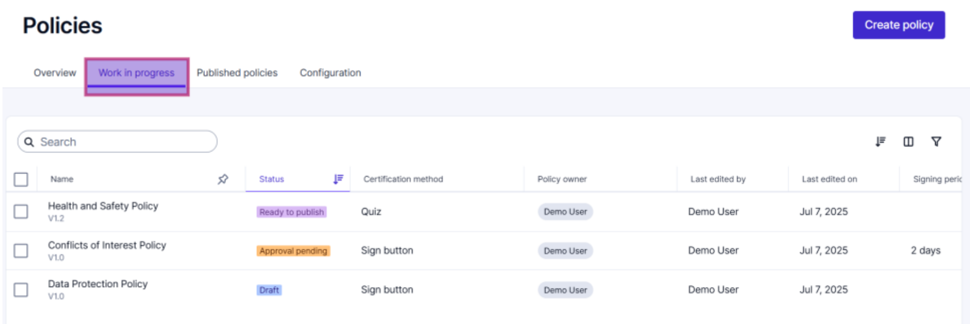
01. *Draft* – The policy is being created or edited and not yet submitted for approval.
02. *Approval Pending* – Submitted for review and awaiting approval.
03. *Ready to Publish* – Approved and ready to go live but not yet published.

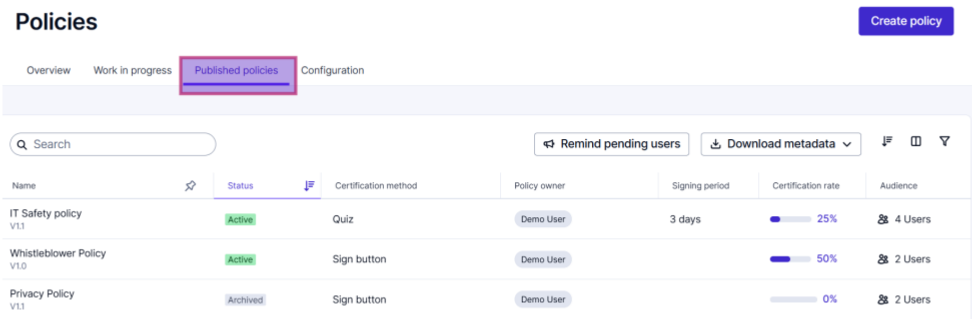
1.2. Published Policies

01. *Published* – The policy is live and visible to users.

Note: Publication usually includes a notification to employee users who have access to the policy.

02. *Archived* – The policy is no longer active but retained for reference.



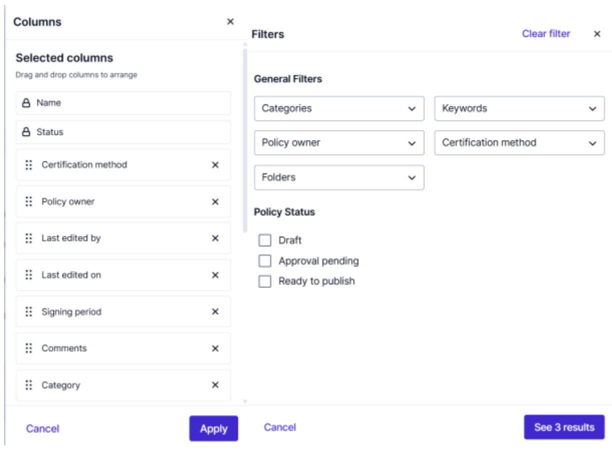


03. Within each tab, you can search for keywords to pull up specific policies.

04. By clicking on the **Filter funnel icon** (located on the right-hand side), you can edit the filters to your preference.

05. You can customize the columns, i.e. rearranging / removing, to further tailor your view. (Click the **Column icon**, next to the filter icon).

    a. Your Column preferences are auto-saved, so the next time you log in, your customized column layout will be preserved.



2. Policies – Configurations

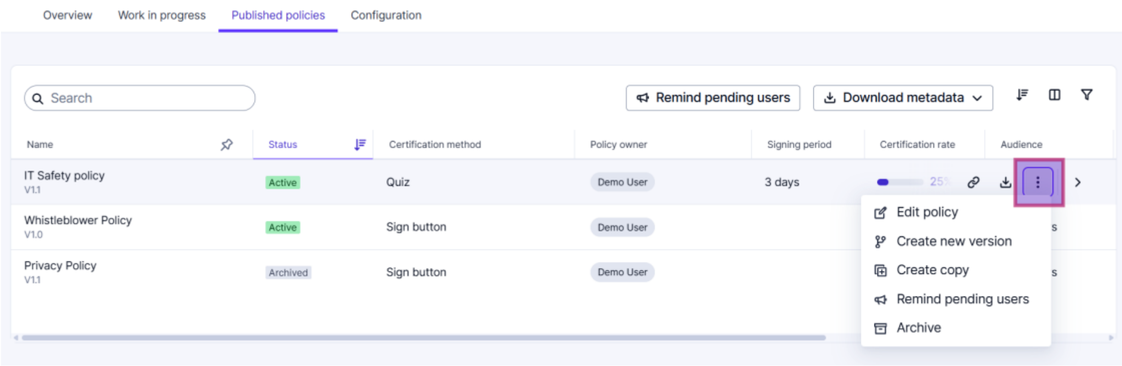
2.1. Creating a New Version of a Policy

01. To create a new version of an existing policy, navigate to the **'Published Policies'** tab;

02. Then locate the policy you want to update and click the three-dot menu (⁝) in the top-right corner of that policy.

03. From the dropdown menu, select **'Create New Version'**

a. Additional options available from the menu include Edit Policy, Create Copy, and more.



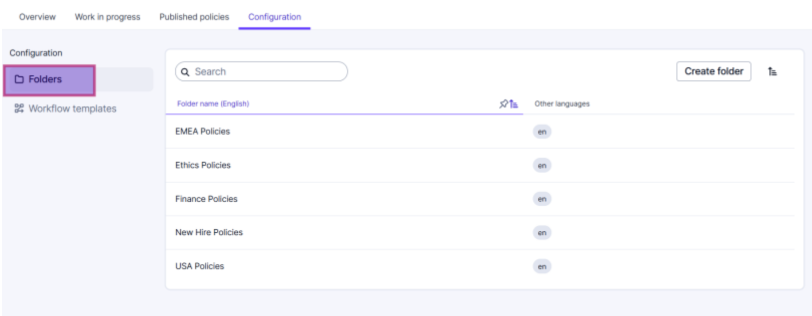
2.2. Folders

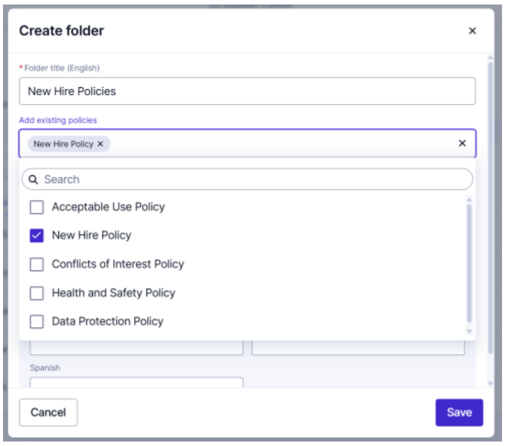
Grouping Policies by Folders

01. You can organize policies by assigning them to folders in the **'Folders'** section under the **'Configuration'** tab.

02. Folders can be created based on various criteria such as Department, Region or Country, Category, Employee Status, and more.

Note - Access to folders and their associated policies can be managed through Compliance Cockpit admin roles. These roles support specific access permissions, enabling control over which users can view or manage specific folders and policies, among other capabilities. For Employee users who have access to the Integrity Hub, this type of access control is managed via the Audience for each policy, rather than folders. For more details, refer to the 'Data Center – User Management' section.



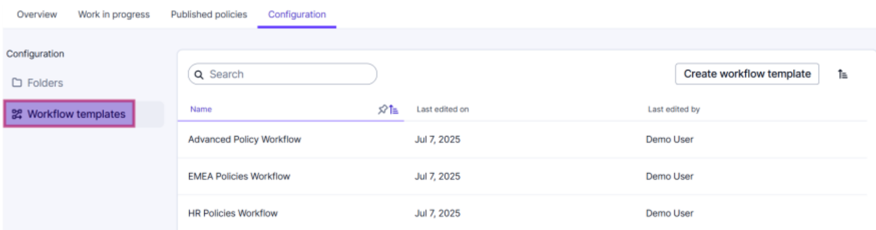


2.3. Workflows

01. Policy Workflows can be configured in the **'Workflow Template'** section under the **'Configuration'** tab.

02. In Convercent, this corresponds **to 'Policy Status and Tasks'**.

03. In OneTrust, this corresponds to **'Workflow Stages'**.

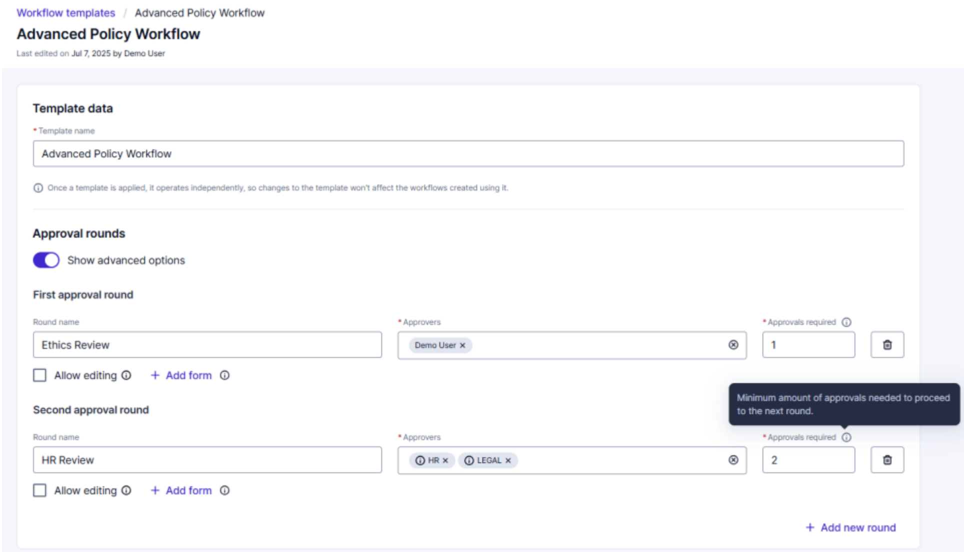


04. Approval Rounds – Policies can go through multiple approval rounds, allowing for a structured, step-by-step review process.

05. Approvers – For each round, you can assign specific individuals or groups as approvers, as many as needed.

06. Approvals Required – You can define how many approvals are needed to move the policy forward. I.e.: even if three approvers are assigned, only one may be required to approve for the policy to proceed to the next round.

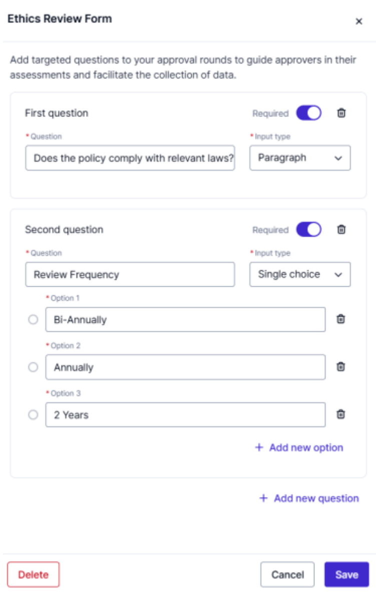
07. Allow editing – Approvers in this round will have the ability to edit the policy.



2.4. Add Form

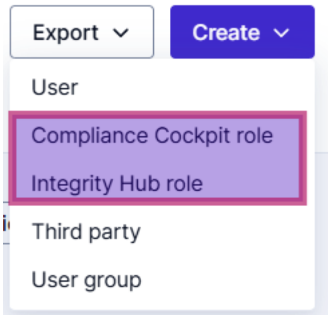
01. The 'Add Form' feature allows you to include targeted questions for reviewers during the approval process.

02. Forms are useful for capturing specific data points—such as stakeholder input, compliance confirmations, or details that would otherwise be stored as custom attributes. As custom attributes are not yet available in EQS, the 'Add Form' feature can be used to store this information, similar to how it was stored in OneTrust.



3. Data Center – User Management

In Data Center, you can manage your users, user roles and user groups, and create custom roles for the Policy module.

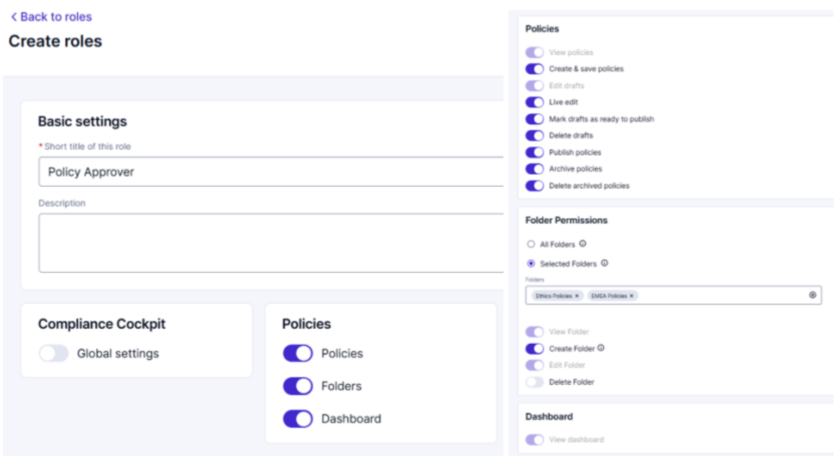


3.1. Compliance Cockpit role

For Administrators

01. Compliance Cockpit roles give access to the Compliance Cockpit

Note – 'Compliance Cockpit' roles, such as the 'Policy Approver' role, support configurable access permissions. These roles allow you to define specific access levels, e.g., whether users can view all folders or only selected ones, whether they have permissions to publish/ delete policies etc.



3.2. Integrity Hub role

For Employees

01. Integrity Hub roles give access to the Integrity Hub

Note: 'Integrity Hub' roles, such as the 'Employee' role, do not support configurable access permissions. As a result, access management similar to the 'OneTrust Organization Hierarchy' is not supported. E.g., it is not possible to create a regional Employee role (i.e., "EMEA Employee") that can only view EMEA Folder Policies.

Note - Employee access to policies is instead managed via the 'Audience' setting configured for each policy. For example, you can create an 'EMEA User Group' and assign it as the Audience for policies specific to the EMEA region.