



# Policy Central (Tech Preview)

---

Version: 2024.1.0.0

# Copyright AppViewX, Inc.

**Copyright © 2025 AppViewX, Inc. All Rights Reserved.**

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general-purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

## **Trademarks**

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

## **External Reference Links**

This product includes software developed by Red Hat, Inc. ([www.redhat.com](http://www.redhat.com)).

This product includes software developed by VMware, Inc. ([www.vmware.com](http://www.vmware.com)).

All other trademarks mentioned in this document are the property of their respective owners.

## **Contact Information**

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: [info@appviewx.com](mailto:info@appviewx.com)

Web: [www.appviewx.com](http://www.appviewx.com)

# Contents

<b>Chapter 1. Policy Central.....</b>	<b>5</b>
<b>Chapter 2. Prerequisites.....</b>	<b>6</b>
Access to Policies.....	10
<b>Chapter 3. Getting Started.....</b>	<b>12</b>
<b>Chapter 4. Policy Inventory.....</b>	<b>13</b>
Tags.....	13
Create Policy.....	14
Policy Actions.....	36
<b>Chapter 5. Policy Requests.....</b>	<b>41</b>
<b>Chapter 6. FAQs.....</b>	<b>51</b>
What is the difference between the CA Policy and the Certificate Policy?.....	51
Should I configure a CA Policy even though I'm using a Certificate Policy in Policy Central?.....	51

# Preface

## Revision History

Revision	Description	Date
1.0	Initial draft of document for release 2024.1.0.0 Policy Central.	March 2025

## About the Documentation

This section includes the following guides that will give you an overview of Policy Central.

## Audience

This guide is intended for CERT, PKI Security, and Application Teams.

## Text Conventions

The following text conventions are used in this document:

Convention	Description
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in the text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>codeblock</code>	Indicates commands with a paragraph, URLs, codes in examples, text that appears on the screen, or text that you enter.

# Chapter 1: Policy Central

AppViewX's Policy Central is a comprehensive, centralized policy management platform designed to streamline compliance, enhance security, and enforce standardization across organizations. It provides a flexible framework for customizing policies to align with both organizational standards and specific operational needs. Its adaptability ensures seamless integration into existing workflows, driving improvements in security and compliance processes.

In version 2024.0.0 FP1, Policy Central enables policy creation for Certificate Enrollment compliance. Future releases will expand support to include additional Certificate Lifecycle Management (CLM) actions like renewal and regenerate.



**Important:** Policy Central is a unified policy management system introduced as a Tech Preview feature in AppViewX. Enabling access to Policy Central will also grant the required permissions for the CERT+, Platform, and Automation modules.

## Key Features:

- Enforce compliance in the certificate enrollment process through tailored forms and customizable approval levels.
- Provide an enhanced user experience with a custom self-service page designed for ease of use and accessibility.

## Chapter 2: Prerequisites

At present, Policy Central supports only the Certificate Enrollment Policy, so a CERT+ license is required to create a policy.

- [Access to Policies](#)

## Enabling Policy Central

By default, Policy Central is disabled for the admin role. Users can enable this permission as needed.

To enable Policy Central, follow these steps:

1. Go to  **(Menu)** > **Platform** > **IDENTITY** > **Role**.

You will be redirected to the **Role** page.

2. Click the role name to enable the ACF permission.

You will be redirected to the **Modify :: [RoleName]** page, with the **Information** tab open by default.

3. Switch to the **Authorized Functions** tab.
4. To enable **Policy Central**, select the checkbox for **Policy Central**.

Role > Modify :: admin

**Information** **Authorized functions**

Search...

**All functions**

**Policy Central** ⓘ
 

- Policy Inventory** ⓘ
  - View ⓘ
  - Add/Modify ⓘ
  - Clone ⓘ
  - Delete ⓘ
  - Enable/Disable ⓘ
- Policy Execution** ⓘ
  - View ⓘ
  - Execute ⓘ
  - Abort ⓘ
  - Resubmit ⓘ
  - Retry ⓘ



**Note:** Enabling access to Policy Central will also grant the necessary permissions for the Certificate, Platform, and Automation modules.

5. **Policy Inventory** Permission define the access control and user privileges required to manage and interact with policies. Users can be granted access to the Policy Inventory based on the permissions assigned to their role.

Permission	Description
<b>View</b>	Grants access to view the inventory.
<b>Add/Modify</b>	Allows users to create and modify policies.
<b>Clone</b>	Allows users to clone existing policies

Permission	Description
<b>Delete</b>	Allows users to delete policies.
<b>Enable/Disable</b>	Allows users to change the status of a policy (enable or disable).

6. **Policy Execution** Permission define the access control and user privileges required to manage and interact with policies. A user can be granted execution permissions based on the access assigned to their role.

Permission	Description
<b>View</b>	Grants access to view the Policy Requests History.
<b>Execute</b>	Allows users to execute policies.
<b>Abort</b>	Allows users to abort an ongoing policy request.
<b>Resubmit</b>	Allows users to resubmit a failed execution.
<b>Retry</b>	Allows users to retry an execution.

7. Click **Save**.

## Onboard a Certificate Authority

To create a policy, the required Certificate Authority must be onboarded. Currently, Policy Central supports the Certificate Enrollment Policy for the following Certificate Authorities:

- Digicert
- MSCA
- GlobalSign / GlobalSign MSSL
- Let's Encrypt
- Sectigo
- InCommon

## CA Policy Modifications

The existing CA policy in CERT+ is integrated with the certificate enrollment process. To ensure seamless experience with Policy Central, specific configuration changes must be made to the CA policy.

1. Go to  (Menu) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.

The **CA Policy** page is displayed.

2. For all CA policies in CERT+ change
  - **Policy Enforcement Type** from **Strict** to **Suggestive**.
  - **Certificate Requests Need Approval?** from **on** to **off**.
  - **Enable Access to Private Key?** from **off** to **on**. (If the certificate, along with its private key, needs to be mailed through Policy Central).

## Configure SMTP

Policy Central currently supports approvals and notifications via email only. To send and receive approval/notification emails, SMTP settings must be configured.

1. Go to  (Menu) > **Platform** > **SYSTEM ADMINISTRATION** > **SMTP**.

The **Settings :: SMTP** page is displayed.

2. [Configure the SMTP Settings](#).

## Enable the Default Email Template

By default, Policy Central uses the **AppViewXDefault** email template for sending approval and notification emails. This template must be enabled under the **Platform** module.

1. Go to  (Menu) > **Platform** > **SYSTEM ADMINISTRATION** > **Themes and Personalization**.

The **Settings :: Theme** page is displayed with the **Logo** tab open by default.

2. Click the **Email Attachment Customization** tab.
3. Under the **Email Template** section, select **AppViewXDefault**.
4. Click the **Edit** icon.
5. Turn on the toggle to use **AppViewXDefault** template.
6. Click **Update**.

The **AppViewXDefault** template will be set as the **Default** email template.

## Access to Policies

Policy access can be managed in the Policy Inventory using the User Access option. If access needs to be granted to multiple policies based on name patterns or if specific access is required for multiple policies, this can be handled in the **Platform** module.

1. Go to  (**Menu**) > **Platform** > **IDENTITY** > **Resource**.

The **Resource** page is displayed.

2. Click the resource name to which you want to grant policy access.

The **Information** tab is displayed.

3. Click the **Access control tab** to add/remove the items from the resource.

4. Click the respective resource in the left pane.

The list of items is displayed on the right with the checkboxes and the R or RW options enabled/disabled for the items.



**Note:** You can modify Read (R) and Read/Write (RW) permissions associated with a resource.

5. Select/Clear the checkbox(es) for the item(s) you want to associate with/dissociate from the resource.

The screenshot displays the 'Access control' interface for a resource named 'super access'. On the left, a vertical list of resources is shown, with 'Policy Central' selected. The main content area is divided into two panes. The left pane contains a search bar and a list of items with checkboxes and 'R' (Read) or 'RW' (Read/Write) permission indicators. The items listed are 'Select all', 'DigiCertTemplate', 'Internal Certificate Enrollment through MSCA', and 'TestPolicyforDoc'. The right pane, titled 'Regex', shows a search bar with the pattern '.\*' and a count of 3 items.

- A regex pattern can be created to assign R/RW access. All policies matching the regex will be granted the specified access.
- Multiple policies can also be selected and given R/RW access.

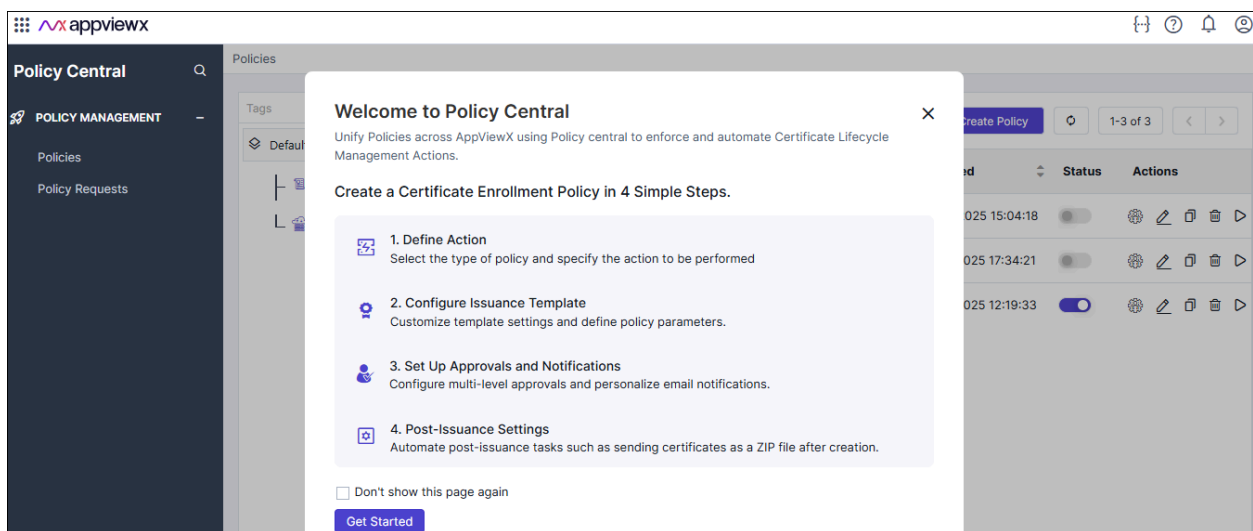
- a. Click **R (Read-only)** to assign read-only permissions.
  - b. Click **RW (Read and Write)** to assign read and write permissions.
6. Click **Save**.

# Chapter 3: Getting Started

To enable Policy Central, please refer [Enabling Policy Central](#).

A policy in Policy Central outlines the approved rules and steps for certain actions to ensure they meet established standards and regulations. For example, new certificates may be required to use a particular key type, or there may be specific naming conventions for common names. Additionally, the certificate enrollment process could require two distinct approval levels.

Once Policy Central is enabled, clicking the **Policy Central** option under  (**Menu**) dropdown will take you to the Policy Inventory page, where the **Welcome to Policy Central** popup will be displayed.

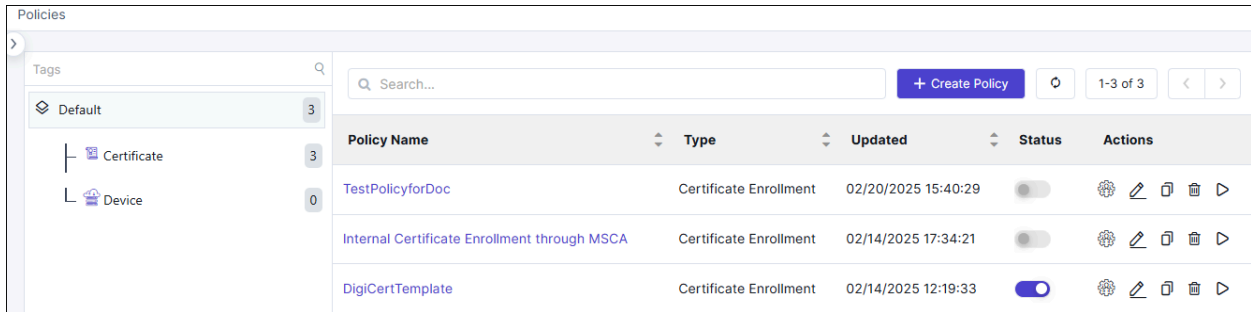


Click **Get Started** to create your first policy.

The Create Policy pop-up is displayed. To configure the policy refer the following steps [here](#).

# Chapter 4: Policy Inventory

The Policy Inventory serves as a centralized repository that lists all created policies. It provides key details such as policy names, types (e.g., certificate enrollment), status (enabled/disabled), and available actions, including granting user access, editing, deleting, cloning, and executing policies. This section enables administrators to efficiently track and manage policies, ensuring compliance with organizational standards.

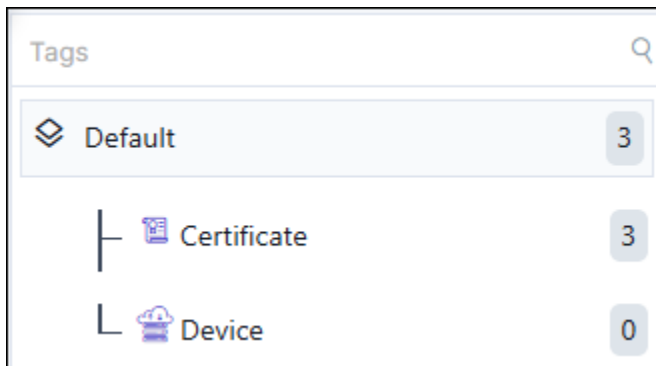


Here are some key elements displayed in the Policy Inventory:

- [Tags](#)
- [Create Policy](#)
- [Policy Actions](#)

## Tags



Tags are used to logically group the policies, simplifying their organization and management based on specific criteria. Users can map a policy to a particular tag for better classification and easier retrieval. Tagging enhances the ability to filter and search policies efficiently, particularly in environments with large number of policies. With well-organized tags, organizations can optimize policy management and enforcement.

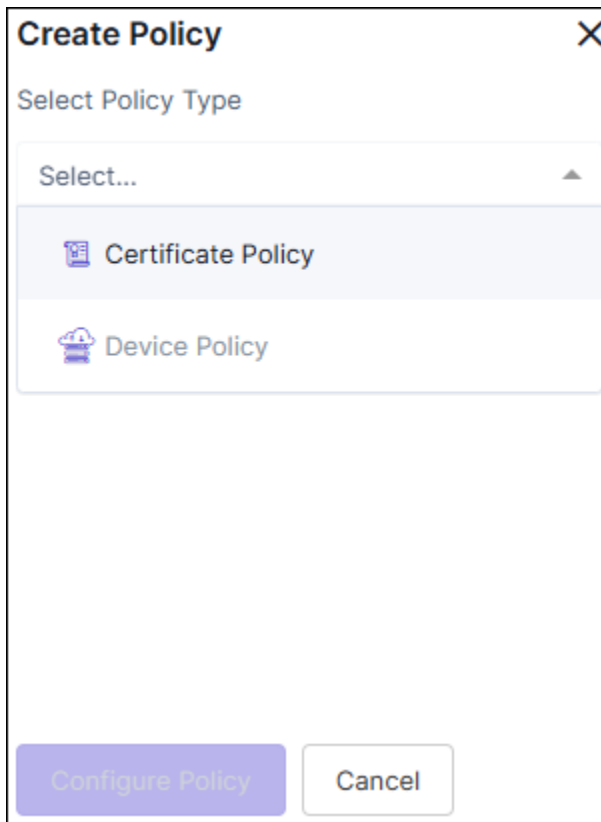


## Create Policy

Policies can be created for various Certificate Lifecycle Management actions to ensure compliance and align with organizational standards.

To create a new policy:


1. Go to  (**Menu**) > **Policy Central** > **POLICY MANAGEMENT** > **Policies**.  
The **Policy Inventory** page is displayed.
2. On the **Policy Inventory** page, click  (**+ Create Policy**).
3. Select **Policy Type** from the dropdown.



Choose the appropriate type of policy based on your specific requirements:

- a. **Certificate Policy**
  - b. **Device Policy**
4. Enter the following details to configure the policy.

**Field description for Create Policy**

Fields	Description
<b>*Policy Name</b>	Enter a policy name that can include alphabets, numbers, and the special characters - and _
<b>Description</b>	Enter the description for the policy.
<b>*Select a Tag</b>	<p>Select an existing tag from the dropdown or create a new one.</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;">  <b>Note:</b> Selecting the appropriate policy type allows you to group policies logically, simplifying organization and management based on specific criteria. </div>
*: <i>Mandatory fields</i>	

5. Click **Configure Policy**.

Once the policy is created successfully, a confirmation message will appear, and you will be redirected to the **Configure Policy** page.

## Configuring Policy

The policy creation process is made up of different functional blocks, with each block in the policy flow known as a component. The components that form a Certificate Enrollment Policy are as follows:

**Action > Issuance Template > Approval > Post Issuance Settings**

### Action to Trigger Policy

The Action Component enables to choose an action, such as **Enroll Certificate**, **Renew Certificate**, or **Regenerate Certificate**. A Display Name for the action must be provided, which will appear in Quick Actions to assist users in easily executing the policy.

To configure trigger policy:

1. Select an **Action**.

- **Enroll Certificate**

Currently, Policy Central supports the creation of certificate policies only for the Enroll Certificate action.

- Renew Certificate
- Regenerate Certificate.

2. Enter the name to be displayed to users in **Quick Actions** under **Policy Request**, instead of the policy name.

3. Click **Next**.

The **Issuance Template** screen is displayed.

## Issuance Template

An issuance template is a customizable form that defines how certificate request fields are created and processed. It enables administrators to control the information collected during the certificate request process and how it is validated.

To configure the issuance template:

1. Choose from the list of supported CA vendors (e.g., DigiCert, Entrust, etc.)
2. To customize the issuance template as per the requirement.
  - a. Select the template to be customized from the list.
  - b. Validate the available parameters and click **Confirm** to import the template.

**Note:**

- These templates include commonly used field configurations.
- Templates are designed to match vendor-specific certificate requirements.
- When you click **Confirm** to apply a template, any previous customizations will be replaced by the new template's configurations.



c. Enter the required details for each parameter.

d. To customize the existing fields:

i. Click  (**Settings**) icon.

The **Select/Text Box** popup is displayed

ii. **Field Customisation**

Fields	Description
Hide Field	Enable the toggle to completely remove field from view when not needed.
Read Only	Enable the toggle to display field values while preventing modifications.   <b>Note:</b> This field is disabled when the Hide Field toggle is turned on.
Set as mandatory	Enable the toggle to ensure critical information is always provided.   <b>Note:</b> This field is disabled when the Hide Field toggle is turned on.
*Label name	Customize field labels for clarity.
Help Tooltip	Provide additional guidance with hover tooltips.
*: <i>Mandatory fields</i>	



**Note:** For more details on custom regex validation, click [here](#).

iii. Click **Save**.

The field customisation is saved.

iv. Click  **(Hide/Unhide)** icon.

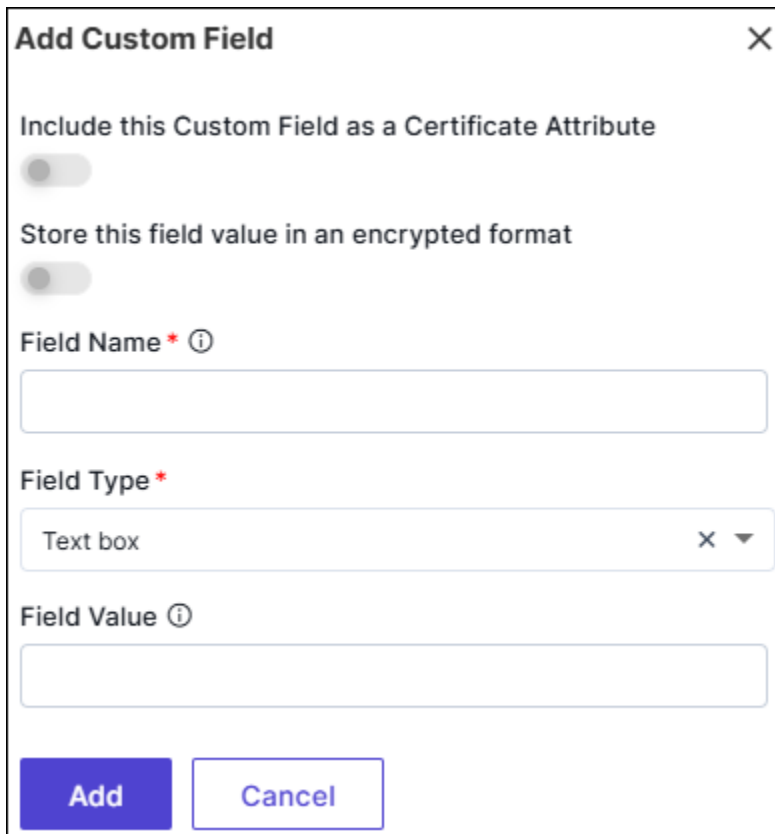
To hide/unhide the field directly without going to settings.

e. To add new custom fields:




You can add new custom fields to the Issuance Template for certificate attributes. When adding a custom field, the following options are available:

i. Click **+ Add Custom Field**.

The **Add Custom Field** popup is displayed.



Fields	Description
<b>Include this Custom Field as a Certificate Attribute</b>	Enable the toggle to <b>Include this Custom Field as a Certificate Attribute</b> in the certificate attributes page and inventory.

Fields	Description
	 <b>Note:</b> <ul style="list-style-type: none"> <li>• When enabled, only Text Box and Select Box field types are supported under <b>Field Type</b>.</li> <li>• When disabled, all field types are available under <b>Field Type</b>.</li> </ul>
<b>Store this field value in an encrypted format</b>	Enable the toggle to <b>Store this field value in an encrypted format</b> .   <b>Note:</b> <ul style="list-style-type: none"> <li>• To encrypt sensitive field data for secure storage.</li> <li>• Encrypted fields are protected in the database.</li> </ul>
<b>Field Name</b>	Enter a unique identifier for the field in alphanumeric format, required for system identification and processing.
<b>*Field Type</b>	Select <b>Field Type</b> from the dropdown.  Standard field types include: <ul style="list-style-type: none"> <li>• Text Box</li> <li>• Text Area</li> <li>• Select Box</li> <li>• Multi-select Box</li> <li>• Check Box</li> <li>• Radio Button</li> </ul>  <b>Note:</b> When <b>Include this Custom Field as a Certificate Attribute</b> toggle is enabled, only <b>Text Box</b> and <b>Select Box</b> field types are supported.
<b>Field Value</b>	Default values can be provided for the field. For multiple values, use comma-separated values.
<i>*: Mandatory fields</i>	

ii. Click **Add**.

The Custom field is added under **Certificate Attributes**.

- To use the available saved templates without any changes.

The pre-configured master templates offer commonly used field configurations, can be customized to meet specific needs, save time on setup, and serve as a foundation for various certificate types.

- Choose the required vendor from the list to view the available templates for that specific vendor.

**Note:**

- You can also search for templates by typing two or more characters in the search bar.
- If this is your first time configuring the policy, only the master template will be available.

- Click **[Required Template]**.

The **Import Issuance Template** popup is displayed.

- Validate the template configurations and click **Confirm** to apply it.

The **Issuance Template** details will be displayed.



**Note:** When you click **Confirm** to apply a template, any previous customizations will be replaced by the new template's configurations.

- Enter the required details for each parameter.

- Click **Preview**, to preview the Issuance Template. (Optional)

For more details on preview option in issuance template, click [here](#).

- Click **Variables**, to view the available dynamic variables. (Optional)

For more details on dynamic variables, click [here](#).

- To Save the customized issuance template, click **Save as New**.



**Note:** The **Save Template** button appears only after making modifications to any template, while the **Update Existing** option is exclusively available for templates previously saved by users, not for out-of-box templates.

- To modify existing saved template with new customizations, click **Update Existing**.

- Click **Next**.

The **Approval** page is displayed.

## Form Building Capabilities

The **Issuance Template** component uses a form builder to dynamically add or modify fields, allowing a preview of how it will appear to a certificate requestor.

### Field Types

The template component supports various field types to capture different kinds of information:

- Text Input
  - Single-line text entry for basic information.
  - Password-protected fields for sensitive data.
  - Support for regex validation rules.
- Selection Fields
  - Dropdown menus for single selection.
  - Multi-select boxes for multiple choices.
  - Radio buttons for exclusive options.
  - Checkboxes for multiple toggles.
- Text Area
  - Multi-line text entry for longer content.

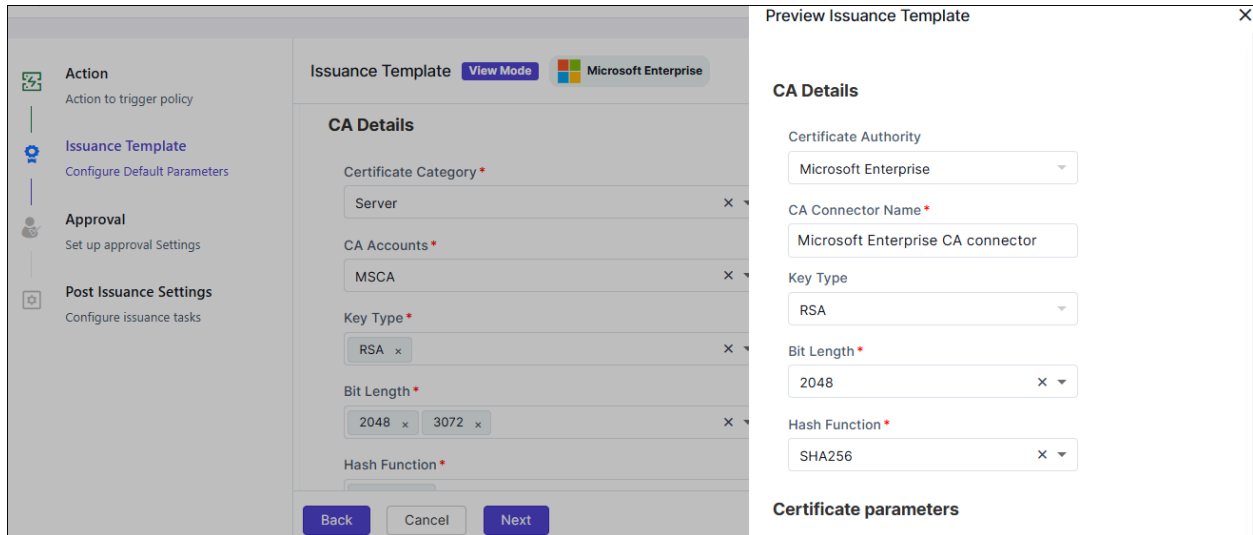
## Preview Option in Issuance Template

On the policy creation page, the Preview Option is available in the Issuance Template page, allowing the policy creator to see how the page will look to the end-user when they use the policy to create a request.

Preview Behavior:

- **Hidden fields** > Not displayed.
- **Read-only fields** > Disabled for editing.
- **Mandatory fields** > Marked with an asterisk (\*).
- **Dynamic Variables** > Replaced with real values based on the **current user's (policy creator's)** context.

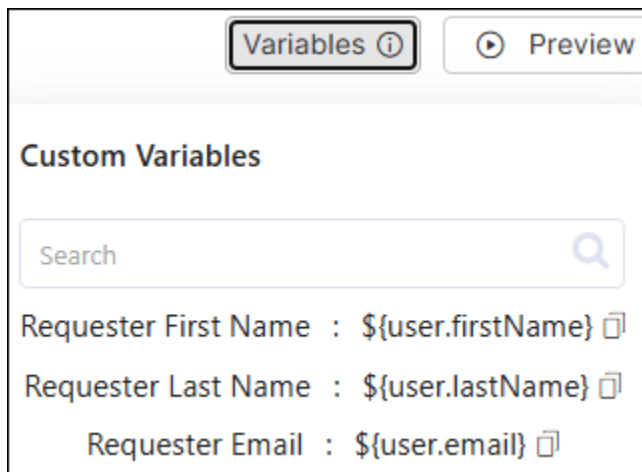
This feature helps policy creators check how the policy will apply configured rules (such as field visibility, editability, required fields, and dynamic variables) before finalizing it.



## Dynamic Variables Support

Text Input and Text Area fields support dynamic variables:

- Users can copy predefined variables (e.g., `${user.firstName}`, `${user.lastName}`).
- Variables can be inserted into text content.
- At runtime, variables are replaced with actual values.
- Supports copy-paste of variables from the provided list.



## Field Customization Options

### Validation Rules

Policy Central provides pre-configured out-of-box validations and support for custom regex patterns to ensure data accuracy and format consistency.

**Out-of-Box Validations:****1. Email**

- Regex: `^[a-z0-9_-]+@([da-z.-]+)([a-z.]{2,6})$`
- Validates:
  - Username: Allows lowercase letters, numbers, underscore, dots, hyphens, and single @ separator.
  - Domain: Allows letters, dots, and hyphens.
  - Top-level domain: 2-6 characters long.
- Valid examples: [user1@example.com](#), [user123@domain-name.co](#).

**2. FQDN with at least two dots**

- Regex: `^([a-zA-Z0-9])+[.]{1}([a-zA-Z0-9])+[.]{1}([a-zA-Z0-9])+([.]{1}([a-zA-Z0-9])+)*)*$`
- Validates:
  - Requires a minimum three parts separated by dots.
  - Allows letters (both cases) and numbers in each part.
  - Can have additional subdomains.
- Valid examples: [sub.domain.com](#), [example.org.uk](#).

**3. FQDN with two dots**

- Regex: `^([a-zA-Z0-9])+[.]{1}([a-zA-Z0-9])+[.]{1}([a-zA-Z0-9])+$`
- Validates:
  - Requires exactly three parts separated by two dots.
  - Allows letters (both cases) and numbers in each part.
- Valid examples: [www.testing.com](#).

**4. IP Address**

- Regex: `^(((0-9)|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5]).){3}((0-9)|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])$`
- Validates:
  - Four octets separated by dots.
  - Each octet must be between 0-255.
  - Properly handles all valid IP ranges.
- Valid examples: [192.168.1.1](#), [10.0.0.0](#), [255.255.255.255](#)

**5. IP Address with Port**

- Regex: `^(((0-9)|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5]).){3}((0-9)|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5]):(6553[0-5]|655[0-2]d|65[0-4]d{2}|6[0-4]d{3}|5d{4}|[0-9]d{0,3}))$`
- Validates:
  - Valid IP address (as above).
  - Followed by colon and port number.
  - Port number must be between 0-65535.
- Valid examples: [192.168.1.1:8080](#), [10.0.0.0:443](#)

## 6. Numbers

- Regex: `^[0-9]*$`
- Validates:
  - Allows only numeric digits.
  - Can be empty or any length.
- Valid examples: 123, 456789

## 7. Port

- Regex: `^([1-9][0-9]{0,3}|[1-5][0-9]{4}|6[0-4][0-9]{3}|65[0-4][0-9]{2}|655[0-3]|6553[0-5])$`
- Validates:
  - Numbers between 1-65535.
  - Properly validates all valid port ranges.
  - Prevents invalid port numbers.

- Valid examples: 80, 443, 8080, 65535

**Text Box** [X]

**Field Customisation**

Read Only

Set as mandatory

Label name \*  
Demo

Validation  
Select or Enter customRegex

Help Tooltip

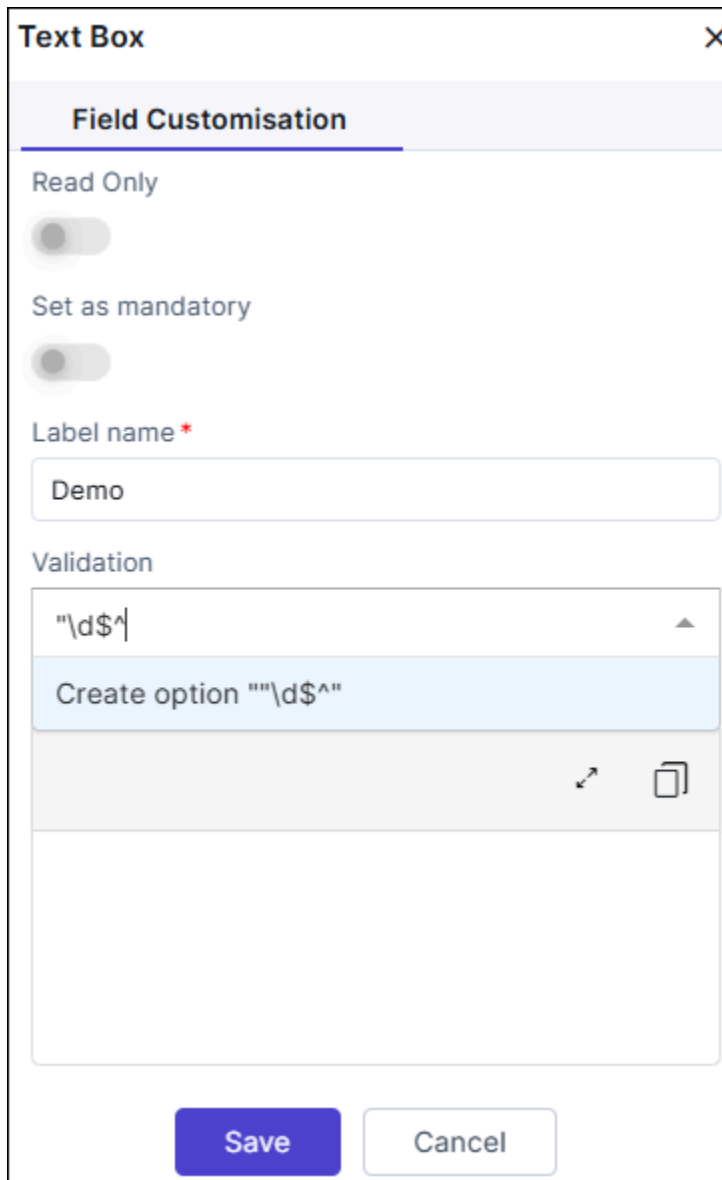
Save Cancel

## Custom Regex Validation

Administrators can create custom regex patterns for specific validation requirements by:

- Using the Creatable option.
- Entering a custom regex pattern.

- Testing the pattern against sample data before implementation.



**Text Box** [X]

**Field Customisation**

Read Only

Set as mandatory

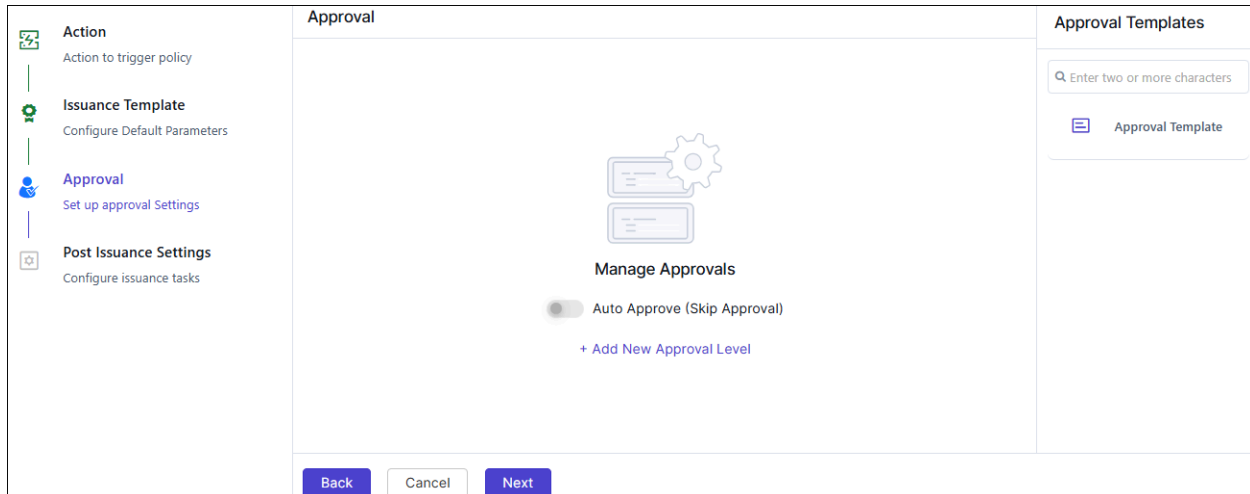
Label name \*  
Demo

Validation  
\\d\$  
Create option "\\d\$^"  
[undo] [copy]

**Save** **Cancel**

## Approval

The Approval Component allows multiple approval levels within Policy Central, so administrators can set up policies that require approvals. Each approval level can have different types of approvers, and the system makes sure requests are handled smoothly. You must set up at least one approval level, or enable auto-approval, which skips the approval process and executes the policy right away.



1. In the Manage Approvals, click one of the following:

- Auto Approve (Skip Approval), to auto approve.
- Add New Approval Level, to add new approval level.



**Note:** This is displayed when Auto approve is disabled.

a. Click Add New Approval Level, to add new approval level.

The Configure Approval screen is displayed with Approval Settings tab.

### Configure Approval

[Approval Settings](#) Email Template

---

**\*Approval Type**

User Group  User  Email  LDAP Manager

**\*User Group**

x ▼

**Notification Settings**

**\*Notify Via**

x ▼
✉ Email

**Advanced Options**






Allow Resubmission ?





Enable Comments ?

Add
Cancel

b. In the Approval Settings, enter the following details:

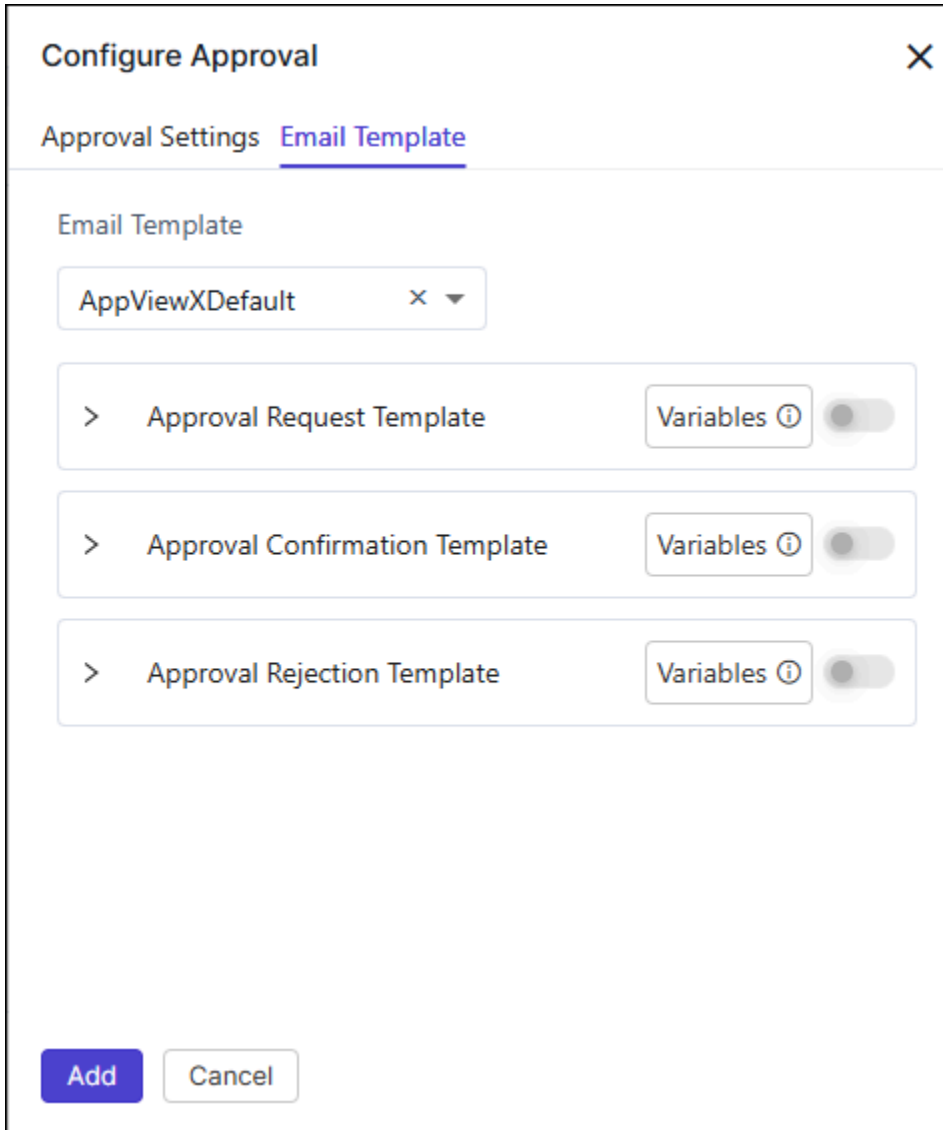
Field	Description
*Approval Type	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>User Group</b></li> <li>• <b>User</b></li> <li>• <b>Email</b></li> <li>• <b>LDAP Manager</b></li> </ul>

Field	Description
*User Group	<div data-bbox="857 302 1419 428" style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px;">  <b>Note:</b> This field is displayed if approval type is selected as User Group.         </div> <p>Any user within the selected user group can approve the request.</p>
*User	<div data-bbox="857 596 1419 722" style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px;">  <b>Note:</b> This field is displayed if approval type is selected as User.         </div> <p>Multiple users can be assigned as approvers for the level.</p>
*Email	<div data-bbox="857 890 1419 1016" style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px;">  <b>Note:</b> This field is displayed if approval type is selected as Email.         </div> <p>Static email addresses are provided for approvals. Multiple email addresses can be added, separated by commas.</p>
*LDAP Server	<div data-bbox="857 1226 1419 1352" style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px;">  <b>Note:</b> This field is displayed if approval type is selected as LDAP Manager.         </div> <p>A default query is used to fetch the LDAP manager from the LDAP server.</p> <p>The requester's LDAP manager is automatically assigned as the approver.</p>
Customize LDAP Query	<div data-bbox="857 1625 1419 1751" style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px;">  <b>Note:</b> This field is displayed if approval type is selected as LDAP Manager.         </div> <p>Custom queries can be defined by configuring:</p>

Field	Description
User Filter Attribute	<div data-bbox="854 296 1419 474" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-bottom: 10px;">  <b>Note:</b> This field is displayed when Customize LDAP Query toggle is enabled.         </div> <p data-bbox="854 506 1393 537">Identifies the requester's login name in LDAP.</p>
User Return Attribute	<div data-bbox="854 590 1419 768" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-bottom: 10px;">  <b>Note:</b> This field is displayed when Customize LDAP Query toggle is enabled.         </div> <p data-bbox="854 800 1357 873">Maps to the manager reference in the user context.</p>
Manager Filter Attribute	<div data-bbox="854 930 1419 1108" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-bottom: 10px;">  <b>Note:</b> This field is displayed when Customize LDAP Query toggle is enabled.         </div> <p data-bbox="854 1140 1247 1171">Identifies the manager document.</p>
Manager Return Attribute	<div data-bbox="854 1224 1419 1402" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-bottom: 10px;">  <b>Note:</b> This field is displayed when Customize LDAP Query toggle is enabled.         </div> <p data-bbox="854 1434 1318 1465">Identifies the manager's email in LDAP.</p>
*: <i>Mandatory fields</i>	

- c. In the Notification Settings section, select Email from the notify via dropdown
  - d. Advanced Options section, select the following toggle:
    - **Allow Re-submission:** On enabling, allows the resubmission of the policy request.
    - **Enable Comments:** On enabling, approver can add comments to the policy.
2. As part of the **Approval** step for creating a policy, you can select the required approval email template under the **Email Template** tab and customize it as required.

- a. To select/customize email templates, Click **Email Template**.  
The **Email Template** tab is displayed.



The screenshot shows a dialog box titled "Configure Approval" with a close button (X) in the top right corner. Below the title, there are two tabs: "Approval Settings" and "Email Template", with "Email Template" being the active tab. Under the "Email Template" section, there is a dropdown menu currently showing "AppViewXDefault" with a close (X) and a downward arrow icon. Below this, there are three rows of settings, each with a right-pointing chevron (>) on the left, a text label, a "Variables" button with an information icon (i), and a toggle switch. The rows are: "Approval Request Template", "Approval Confirmation Template", and "Approval Rejection Template". At the bottom left of the dialog, there are two buttons: "Add" (in a blue box) and "Cancel" (in a white box with a grey border).



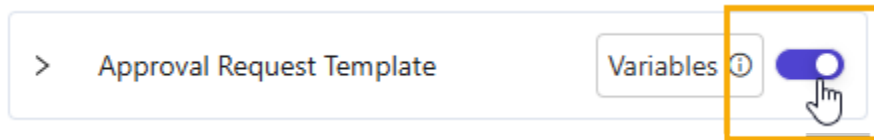
**Note:** Admins can create new user templates in the **Platform** module in AppViewX.  
For navigation and instructions to create a new email template, click [here](#).


- b. Select the required **Email Template** from the dropdown.
- c. Policy Central includes templates for three types of approval -related emails:

- **Approval Request Template** (Sent to the approver when a request needs approval)
- **Approval Confirmation Template** (Sent to the requester when the request is approved)
- **Approval Rejection Template** (Sent to the requester when the request is rejected)

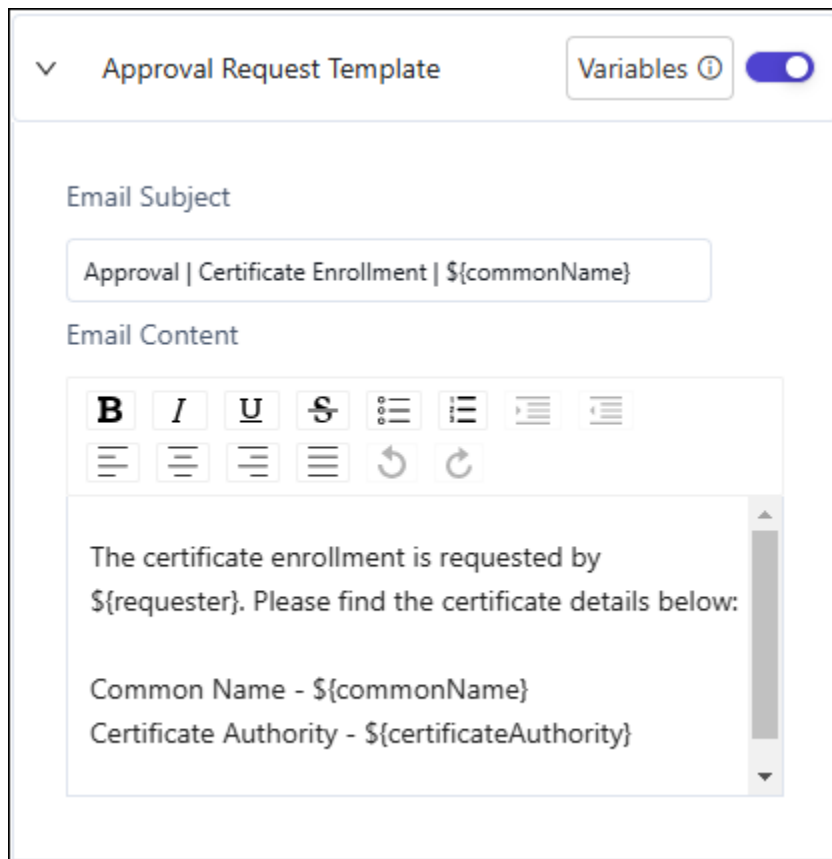
d. To customize the email templates in Policy Central:

e. To enable a template for editing, turn on the toggle button for the required template.



f. To view the email subject and body fields, click .

The contents of the email are displayed.



g. To view the full list of variables that can be added to the email body, click **Variables**.

h. Using the variables and plain text values, customize the email subject and content, as required.

- i. Click **Add**.

The contents of the email template are updated and saved.

## Approval Execution & Notifications

Approvals are processed in two ways:

1. **Email-Based Approvals:** Approvers receive an email and can approve the request directly from their email.
2. **Appviewx Policy Central Execution Timeline View:** Approvers can log into AppViewX, navigate to **Policy Central** → **Policy Requests**, select the corresponding request, and approve it.

### Approval Types and Execution Methods

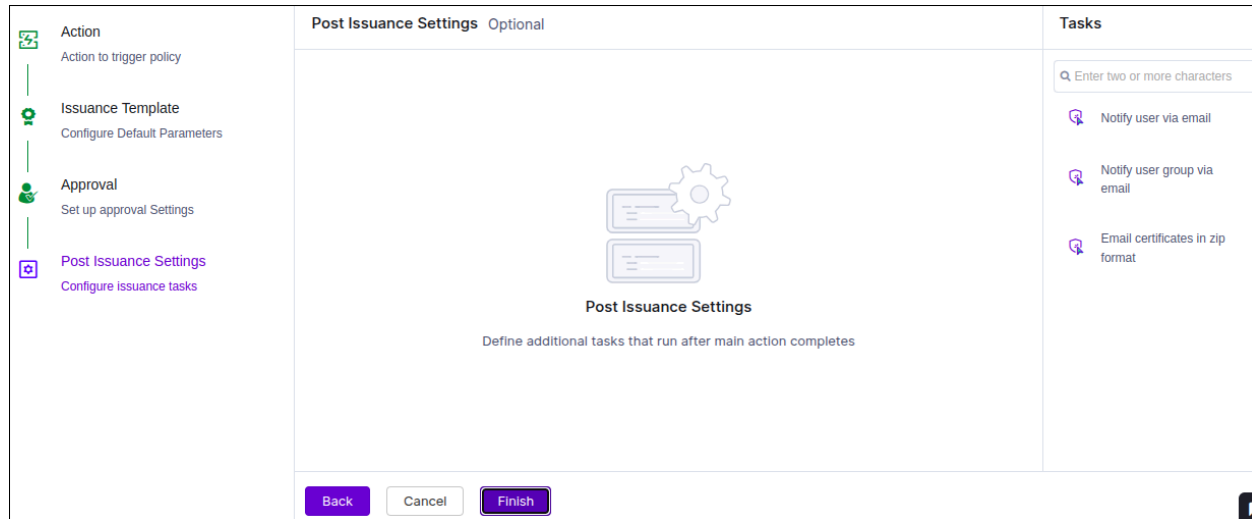
Approval Type	Approve via Email	Approve via Login
User	✓	✓
User Group	✓	✓
Email	✓	✗
LDAP Manager	✓	✓ (if part of AppViewX)

## Notifications

For each approval action, a notification is sent to the requester. Currently, notifications are sent via **email**, with future support planned for **Slack**.

## Post Issuance Settings (Optional)

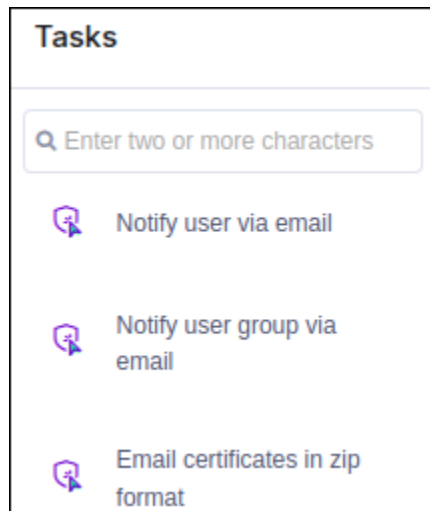
You can configure additional tasks to run after the main action is completed. Policy Central supports three post-action items, which are carried out once a policy is enforced.



Post action items are:

- Notifying users via email.
- Notifying user groups via email.
- Emailing certificates in the **.zip** format.

AppViewX Policy Central includes issuance templates for each of these actions.



Each action is customizable and is executed separately.

## Configuring and Customizing the Tasks

### Notifying Users via Email

1. On the **<policy name> :: Edit** page, under **Post Issuance Settings > Tasks**, select **Notify user via email**.

The **Notify user via email** dialog box is displayed.

2. In the **Notify user via email** dialog box, from the **Notify user via email** dropdown list, select email addresses/names of one or more users to be notified of action completion.
3. Click **Confirm**.

The Notify user via email task is displayed in the **Post Issuance Settings** page.

Upon policy enforcement, all selected users will receive the corresponding email notification.



**Note:** You can edit existing users or add new ones to the task by clicking the Edit icon, or delete the task by clicking the Delete icon.

### Notifying User Groups via Email

1. On the **<policy name> :: Edit** page, under **Post Issuance Settings > Tasks**, select **Notify user group via email**.

The **Notify user group via email** dialog box is displayed.

2. In the **Notify user group via email** dialog box, from the **Notify user group via email** dropdown list, select all user groups to be notified of action completion.
3. Click **Confirm**.

The Notify user group via email task is displayed in the **Post Issuance Settings** page.

Upon policy enforcement, all selected user groups will receive the corresponding email notification.



**Note:** You can edit existing user group or add new user group to the task by clicking the Edit icon, or delete the task by clicking the Delete icon.

### Emailed Certificates to the Requester

To receive certificates via email post action completion:

1. On the **<policy name> :: Edit** page, under **Post Issuance Settings > Tasks**, select **Email certificates in zip format**.

The **Email certificates in zip format** dialog box is displayed.

- In the **Email certificates in zip format** dialog box, from the **Certificate type** dropdown list, select the certificate type.



**Note:** Only one certificate type can be selected at a time.

- To also include the certificate chain when the certificates are emailed, select the **Include Root and Intermediate** checkbox.
- Click **Confirm**.

The Email certificates in zip format task is displayed in the **Post Issuance Settings** page.

Upon policy execution, an email with certificates attached in the **.zip** format will be sent to the requester.



**Note:** You can change the zip format in the task by clicking the Edit icon, or delete the task by clicking the Delete icon.

## Policy Actions

### View Policy

Clicking on a policy name opens it in view mode, where detailed information about its configuration is displayed. This view includes the configured template details, outlining the policy's structure and parameters. Additionally, the view shows the supported post-actions, such as notifications.

Internal Certificate Enrollment Through MSCA :: View

**Action**  
Action to trigger policy

**Issuance Template**  
Configure Default Parameters

**Approval**  
Set up approval Settings

**Post Issuance Settings**  
Configure issuance tasks

Select an Action View Mode

**Enroll Certificate**  
Define policy for certificate enrollment

**Renew Certificate**  
Define policy for certificate renewal

**Regenerate Certificate**  
Define policy for certificate regeneration

**\*Display Name for Action** ⓘ  
This is the name displayed to users instead of the Policy name in Quick Actions.

Back
Cancel
Next

## Enable/Disable Policy

Once a policy is fully configured, it must be enabled using a toggle button to allow execution.

1. After a policy is fully configured, enable it by toggle button to allow execution under Status column.
2. Enabling the policy makes it available for use within the system.
3. When the policy is enabled, update and delete actions are restricted to prevent unauthorized modifications or accidental removals.
4. To make changes to the policy, it must first be disabled.
5. Disabling the policy allows modifications or deletion to be made.
6. This process ensures the integrity of the policy and maintains operational consistency.

## User Access

Once a policy is created, it can be read (R) or modified (RW) by a user with the appropriate access. The User Access option allows granting access to the policy for various resources within an application.

By default, the resource associated with the policy creator is granted Read and Write (RW) permission, and this access cannot be modified later. Other resources can be granted Read (R) or Read and Write (RW) access, and these permissions can be modified at any time.

A user with Read (R) access to a policy can:

- View the policy
- Execute the policy
- Approve or reject a policy approval request.

A user with Read-Write (RW) access to a policy can:

- Edit the policy
- View the policy
- Execute the policy
- Approve or reject a policy approval request.




**Note:** Approvers must have Read (R) access to approve or reject requests.

### User Access Policy ✕

<input type="checkbox"/> <span style="background-color: #ccc; padding: 2px 5px;">R</span> <span style="background-color: #ccc; padding: 2px 5px;">RW</span> Select all
<input type="checkbox"/> <span style="background-color: #ccc; padding: 2px 5px;">R</span> <span style="background-color: #ccc; padding: 2px 5px;">RW</span> ADC-HISTORIC-STATS-RESOURCE
<input type="checkbox"/> <span style="background-color: #ccc; padding: 2px 5px;">R</span> <span style="background-color: #ccc; padding: 2px 5px;">RW</span> CLM Auditor
<input type="checkbox"/> <span style="background-color: #ccc; padding: 2px 5px;">R</span> <span style="background-color: #ccc; padding: 2px 5px;">RW</span> CLM Level1 Approver
<input type="checkbox"/> <span style="background-color: #ccc; padding: 2px 5px;">R</span> <span style="background-color: #ccc; padding: 2px 5px;">RW</span> CLM Level2 Approver
<input type="checkbox"/> <span style="background-color: #ccc; padding: 2px 5px;">R</span> <span style="background-color: #ccc; padding: 2px 5px;">RW</span> CLM Requester
<input checked="" type="checkbox"/> <span style="background-color: #f96; padding: 2px 5px;">R</span> <span style="background-color: #f96; padding: 2px 5px;">RW</span> DevOps
<input type="checkbox"/> <span style="background-color: #ccc; padding: 2px 5px;">R</span> <span style="background-color: #ccc; padding: 2px 5px;">RW</span> SRE
<input checked="" type="checkbox"/> <span style="background-color: #ccc; padding: 2px 5px;">R</span> <span style="background-color: #90ee90; padding: 2px 5px;">RW</span> super access
















Save
Cancel

To provide **User Access** to a policy:


1. On the **Policy Inventory** page, below the actions column.
2. Click  (**User Access**) icon.  
The **User Access Policy** page is displayed.
3. Select the checkbox for the required user access.
4. Click **Save**.  
The selected User Access is updated successfully.

## Edit Policy

Once a policy is created, users with Read and Write (RW) access can modify its details using the Edit option. Clicking on Edit allows the user to change any part of the policy, just as they did during the creation process. The Edit option is only visible to users with RW access.
















Policy Name	Type	Updated	Status	Actions
<a href="#">TestPolicyforDoc</a>	Certificate Enrollment	02/20/2025 15:40:29	<input type="checkbox"/>	    
<a href="#">Internal Certificate Enrollment through MSCA</a>	Certificate Enrollment	02/14/2025 17:34:21	<input checked="" type="checkbox"/>	    
<a href="#">DigiCertTemplate</a>	Certificate Enrollment	02/14/2025 12:19:33	<input checked="" type="checkbox"/>	    

To Edit a policy:


1. On the **Policy Inventory** page, below the actions column.
2. Click  (**Edit Policy**) icon.  
The **[Policy Name] :: Edit** page is displayed.
3. Modify the required details in the **Action, Issuance Template, Approval** and **Post Issuance Settings** sections.
4. Click **Save**.  
The selected Policy is modified.

## Clone Policy

A user can clone a policy, and all its properties and components will be duplicated in the cloned policy. The user can then make any necessary modifications to the cloned policy.

Policy Name	Type	Updated	Status	Actions
TestPolicyforDoc	Certificate Enrollment	02/20/2025 15:40:29	<input type="checkbox"/>	    
Internal Certificate Enrollment through MSCA	Certificate Enrollment	02/14/2025 17:34:21	<input checked="" type="checkbox"/>	    
DigiCertTemplate	Certificate Enrollment	02/14/2025 12:19:33	<input checked="" type="checkbox"/>	    
















To clone a policy:

1. On the **Policy Inventory** page, below the actions column.
2. Click  (**Clone Policy**) icon.  
The **Clone Policy** popup is displayed.
3. Enter the new **Policy Name, Description**, and **Select a Tag** for the policy.
4. Click **Clone Policy**.  
The selected policy is cloned.


## Delete Policy

A user can delete a policy, but it must be in a disabled state before deletion. Once deleted, all information related to the policy will be removed.

However, if the policy has been created and executed by a user, its ACL will be retained to ensure smoother execution. Additionally, the execution history will be preserved for users to view.
















Policy Name	Type	Updated	Status	Actions
<a href="#">TestPolicyforDoc</a>	Certificate Enrollment	02/20/2025 15:40:29	<input type="checkbox"/>	    
<a href="#">Internal Certificate Enrollment through MSCA</a>	Certificate Enrollment	02/14/2025 17:34:21	<input checked="" type="checkbox"/>	    
<a href="#">DigiCertTemplate</a>	Certificate Enrollment	02/14/2025 12:19:33	<input checked="" type="checkbox"/>	    

To delete a policy:


1. On the **Policy Inventory** page, below the actions column.
2. Click  (**Delete Policy**) icon.  
The **Delete Policy** popup is displayed.
3. In the **Confirmation** dialog box, click **Confirm**.  
The selected policy is deleted successfully.

## Execute Policy

After creating a policy, the Execute action enables the user to test the policy enforcement. A form based on the policy will be generated for the user to complete and submit. Execution details can be viewed on the Policy Requests page.

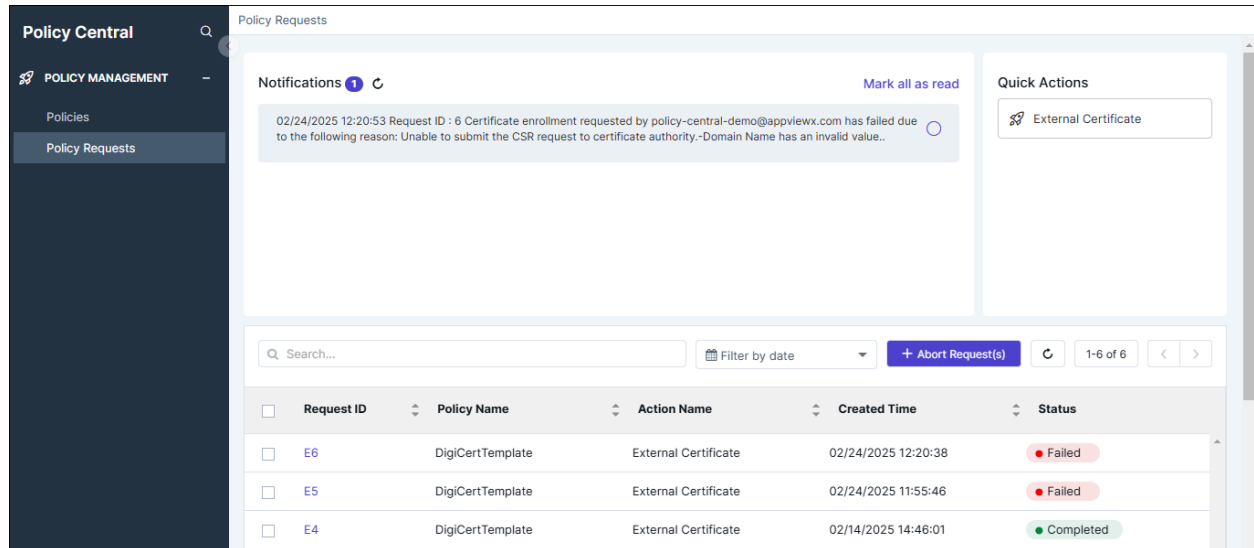
Policy Name	Type	Updated	Status	Actions
<a href="#">TestPolicyforDoc</a>	Certificate Enrollment	02/20/2025 15:40:29	<input type="checkbox"/>	    
<a href="#">Internal Certificate Enrollment through MSCA</a>	Certificate Enrollment	02/14/2025 17:34:21	<input checked="" type="checkbox"/>	    
<a href="#">DigiCertTemplate</a>	Certificate Enrollment	02/14/2025 12:19:33	<input checked="" type="checkbox"/>	    

To execute a policy:

1. On the **Policy Inventory** page, below the actions column.
2. Click  (**Execute Policy**) icon.  
The **Policy Details** popup is displayed.
3. Update the **Certificate Parameters** details.
4. Click **Submit**.  
The selected policy is executed successfully.

# Chapter 5: Policy Requests

To access the policy request inventory, go to  (Menu) > **Policy Central** > **POLICY MANAGEMENT** > **Policy Requests**.

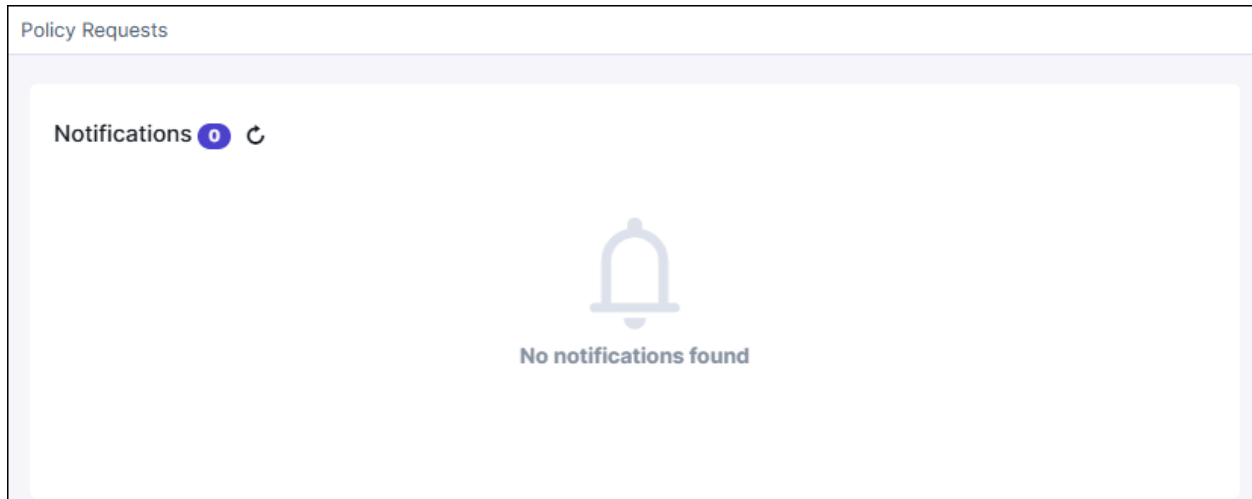


## Notifications

The **Notifications** system provides real-time updates on policy requests, approvals, failures, and completions. The notification system ensures that **policy creators, requesters and approvers** receive timely updates and can take necessary actions.

To view these notifications, go to (Menu) > **Policy Central** > **POLICY MANAGEMENT** > **Policy Requests**.

The **Policy Requests** page, with the **Notifications** section is displayed.



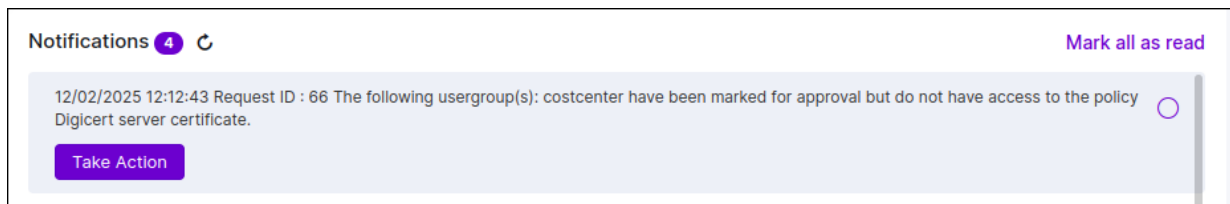
## Understanding Notifications for User Roles

### Policy Creator

The policy creator will receive notifications for the following events:

- **Approval Access Issue**

If the approver does not have access to the policy requested by the user, the policy creator is notified.



To grant the requisite permissions for the approver, click **Take Action** and update the policy access using the dialog box displayed.

### Requester

The requester will receive notifications for the following events:

- **Approval/Rejection Notification**


Sent when the approver accepts/rejects the request.

- **Failure Notification**

Sent to the requester if there has been a failure during policy execution.

- **Successful notification**

Sent to the requester when the request has been executed successfully.

Notifications **4**  Mark all as read

- 12/02/2025 12:16:38 Request ID : 66 Certificate enrollment requested by admin has been completed.
- 12/02/2025 12:16:24 Request ID : 66 Certificate enrollment request is approved by costcenter.
- 12/02/2025 12:12:42 Request ID : 66 Certificate enrollment request is approved by sre\_lead.
- 12/02/2025 10:35:26 Request ID : 64 Certificate enrollment requested by admin has failed due to the following reason: Unable to submit the CSR request to certificate authority.-The CSR uses an unsupported key size, please generate a new CSR..

## Approver


The approver will receive notifications for the following events:

- **Pending Approval Notification**

The approver will receive a notification if a request is pending for approval.

To review the approval request, click **Take Action** for the corresponding notification.

You will be redirected to the request ID's timeline, where you can approve/reject the request.

Notifications **1**  Mark all as read

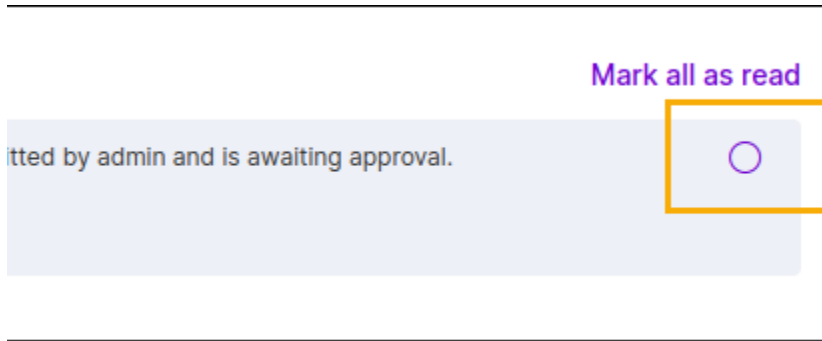
- 02/12/2025 12:09:16 Request ID : 66 Certificate Enrollment request has been submitted by admin and is awaiting approval.

**Take Action**

## Managing Notifications

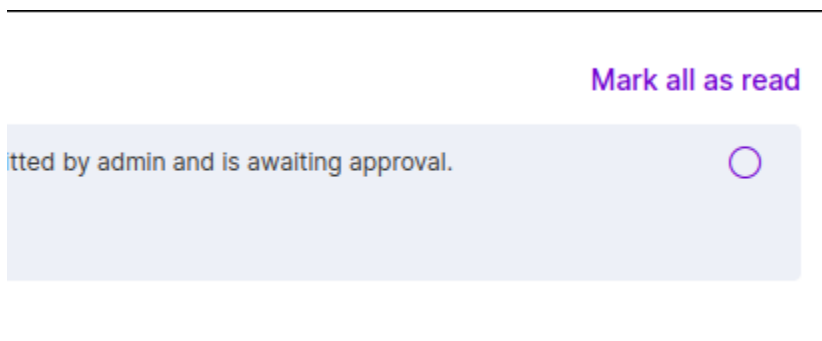
### Marking individual notifications as read

To mark an individual notification as read, click  corresponding to the notification.



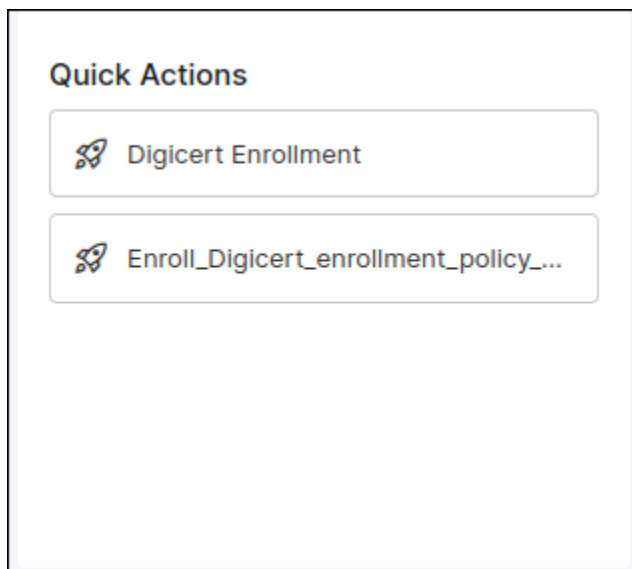
### **Marking all notifications as read**

To mark all notifications as read, click **Mark all as read**.



## Quick Links

The **Quick Actions** panel provides a convenient way to initiate policy executions. It displays a list of **Action Names** associated with policies, allowing users to quickly trigger executions.





**Note:** Only Active policies are displayed in Quick Actions.

## Policy Execution Inventory

### Understanding the Policy Execution Inventory

The **Policy Execution Inventory** is a list of all policy executions that includes key policy details as well as the search and abort functionalities, as explained below:

- **Request ID:** A unique identifier assigned to each policy execution for tracking purposes. Click the request ID to view the request timeline. To understand the request timeline details, click [here](#).
- **Policy Name:** Name of the policy associated with the execution
- **Action Name:** Name of the action associated with the policy, which is used to initiate the execution
- **Created Time:** Timestamp of policy execution initiation
- **Status:** Current status of the policy execution

The policy execution **Status** is indicated using the following values:

Status	Description
<b>In Progress</b>	Policy execution is in progress.
<b>Waiting</b>	Policy execution is pending approval or is waiting for certificate issuance.
<b>Rejected</b>	Policy execution request has been rejected by the approver.
<b>Failed</b>	Policy execution has encountered a system error or a failure scenario.
<b>Aborted</b>	Policy execution request has been aborted.
<b>Completed</b>	Policy execution has been successfully completed.

### Searching for Execution Requests in the Inventory

To search for execution requests, you can:

- Use the **Search** field to search for execution requests by policy name, action name, and request ID.
- Use the **Filter by date** field to filter requests for a required timeline.

### Aborting Policy Execution Requests

To abort policy execution request(s):

1. Select the checkbox corresponding to the execution request(s) you want to abort.
2. From the execution inventory, click **Abort Request(s)**.

## Understanding the Request Timeline

When the **Request ID** is clicked, a timeline view of the execution request is displayed, showing the sequence of execution stages. The execution stages define the step-by-step process of handling a request. Each stage represents a distinct step, ensuring a clear progression from submission to final delivery.

## Execution Stages

- **Certificate Enrollment Request**

This stage displays all certificate parameters submitted by the user. It provides a summary of the request, including details such as certificate type, validity period, and associated metadata. This serves as the initial checkpoint before moving to the approval process.

- **Approval Levels**

Each approval level is treated as a separate stage, displaying the approver responsible for reviewing and approving the request. Approver comments, if provided before approving or rejecting the request, are also displayed here.

If multiple approval levels are configured (for example, Level 1 and Level 2), only the first level will be visible initially. Once the first level approval is obtained, the request will move to the next level, thus progressing until all required approvals are obtained.

- **CSR Creation**

Once all approval levels are completed, the request proceeds to the Certificate Signing Request (CSR) creation stage. This stage displays details such as the Common Name (CN) for which the certificate is being requested.

- **Certificate Issuance**

After CSR creation, the process moves to the certificate issuance stage. In this step, the certificate is generated and issued based on the provided details. Once issued, the certificate is ready for further actions.

## Post Action Stages

Each post-action is treated as a separate stage and occurs only if it is configured. These stages define additional actions taken after certificate issuance. By default, the system automatically notifies the requester via email upon certificate issuance, but this notification is not considered part of the execution stages.

The three post-action stages supported in Policy Central are:

- **Email with certificate**

This stage is triggered if the **Email certificates in zip format** post-action is configured. The system sends an email containing the issued certificate to the requester.

- **Notify users**

If the **Notify users via email** post-action is configured, this stage sends an email notification to the selected user(s), informing that the certificate has been successfully issued.

- **Notify user groups**

If the **Notify user groups via email** post-action is configured, this stage sends an email notification to the selected user group(s), ensuring that relevant users are informed about the certificate issuance.

Execution ID : 31

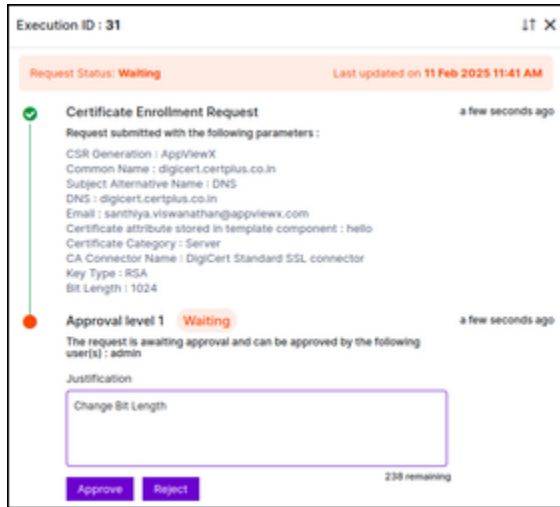
Request Status: **Completed** Last updated on 07 Feb 2025 01:05 PM

- Certificate Enrollment Request** 2 minutes ago  
 Request submitted with the following parameters :  
 Common Name : demo.certplus.co.in  
 DNS : demo.certplus.co.in  
 Key Type : RSA  
 Bit Length : 2048  
 Certificate Category : Server  
 CA Connector Name : DigiCert Standard SSL connector
- Approval level 1** a few seconds ago  
 Reviewed certificate parameters and approved by : admin  
 Comments:  
 Verified
- CSR Creation** a few seconds ago  
 Certificate Signing Request(CSR) created and added to inventory  
 Common Name : demo.certplus.co.in
- Certificate Issuance** a few seconds ago  
 Certificate issued successfully  
 Common Name : demo.certplus.co.in
- Email with Certificate** a few seconds ago  
 Email with the certificate sent to requester [systemuserjy@ppviewx.com]  
 Requester : admin  
 RequestorEmail : vishnvm.szr@ppviewx.com
- Notify User** a few seconds ago  
 Notification sent to user [admin]  
 Users : admin

## Actions

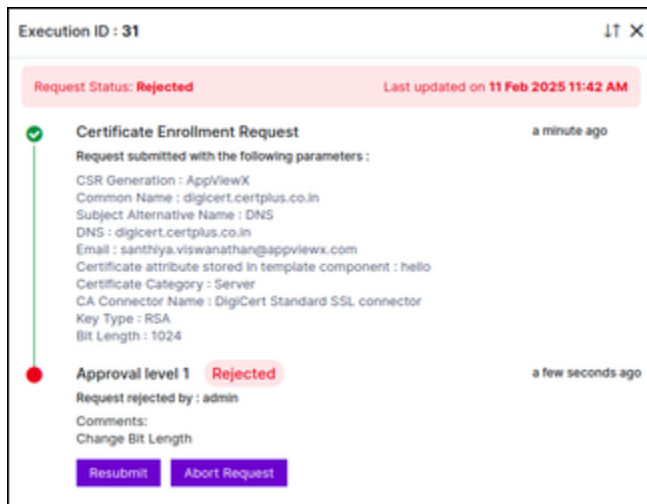
### • Approve and reject

Approvers with policy access can either approve or reject a request. If the **Allow Comments** option is enabled in the policy, approvers can provide comments explaining their decision. If the request contains incorrect details or does not meet the required criteria, the approver can reject it. However, if all parameters are valid, the request can be approved for further processing.



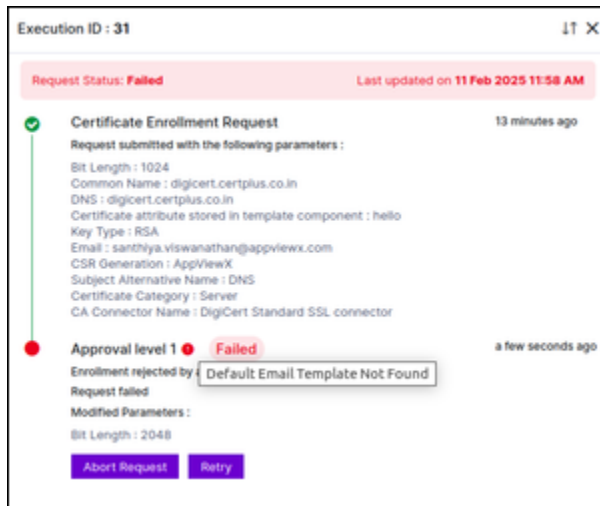
### • Resubmit

If a request is rejected, the requester can resubmit it after making necessary modifications, provided that **Allow Resubmission** is enabled in the policy. This ensures that rejected requests can be corrected and reconsidered without requiring a completely new submission.



## • Retry

If a policy request fails due to system errors or other issues, the Retry action allows the request to be executed again. This ensures that temporary failures do not require a full resubmission and can be resolved efficiently. When a **stage fails**, an exclamation mark (!) indicator appears beside the failed stage. The **error message becomes visible only when hovering over the exclamation mark**.



## • Abort

If a policy request is no longer required, it can be aborted to prevent further processing. However, once the request reaches the implementation stage (e.g., certificate issuance), the abort action is no longer allowed. This restriction ensures that partially executed processes are not left in an inconsistent state.

## Transitions in Execution Stages

execution progresses through the following stages:

### 1. In Progress

Represents an active process that is being executed.

Can transition to:

- **Waiting** (if the request is awaiting approval or further execution steps)
- **Failed** (if an error occurs)
- **Completed** (if successfully processed)

### 2. Waiting

Represents a paused process, either waiting for approval or for certificate issuance.

Can transition to:

- **In Progress** (if the request has been approved or the certificate has been issued)
- **Rejected** (if approval is denied)
- **Aborted** (only if awaiting approval, not during certificate issuance)

### 3. **Rejected**

Represents a rejected request.

Can transition to:

- **In Progress** (if resubmitted)
- **Aborted**

### 4. **Failed**

Represents a process that encountered an error.

Can transition to:

- **In Progress** (if retried)
- **Aborted**

This can also be a final state if retry is not possible.

### 5. **Aborted**

Represents a process that is manually stopped.

This is a terminal state.

### 6. **Completed**

Represents a process that has successfully completed execution.

This is a terminal state.

## Chapter 6: FAQs

### **What is the difference between the CA Policy and the Certificate Policy?**

The **Certificate Policy** feature in Policy Central allows for the configuration of certificate parameters, designation of approvers, and specification of actions to be taken after certificate issuance.

### **Should I configure a CA Policy even though I'm using a Certificate Policy in Policy Central?**

A CA policy must be configured to control aspects such as generating compliance reports and controlling private key downloads, as well as to identify non-compliant certificates. While the certificate policy in Policy Central can set guidelines and enforce them during certificate enrollment, it does not cover all the features supported by CA policy.