appviewx

Policy Engine

Version: 2025.0.0.0

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.

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Preface

Revision History

Revision	Description	Date
1.0	Initial draft of Policy Engine document for release 2025.0.0.0	November 2025

About the Documentation

This section includes the following guides that gives you an overview of Policy Engine.

- Kubernetes Certificate Policy
- Managed Certificate Policy
- Device Management Policy

Audience

This guide is intended for all the users who are deploying AppViewX One products to manage their certificates.

Third-Party Software Acknowledgments

This section is placeholder to document the third-party components referenced in this guide, along with their associated trademark information.

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 1: Overview

The AppViewX Policy Engine is a centralized platform for managing policies. It streamlines compliance, enhances security, and enforces standardization across organizations. The flexible framework allows you to customize policies to align with organizational standards and operational needs. Its adaptability ensures seamless integration into existing workflows, improving security, and compliance processes.

Important: Enabling access to Policy Engine will also grant the required permissions for the CERT+, Platform, and Automation modules.

Key Features:

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

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 2: Prerequisites

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

- Access to Policies

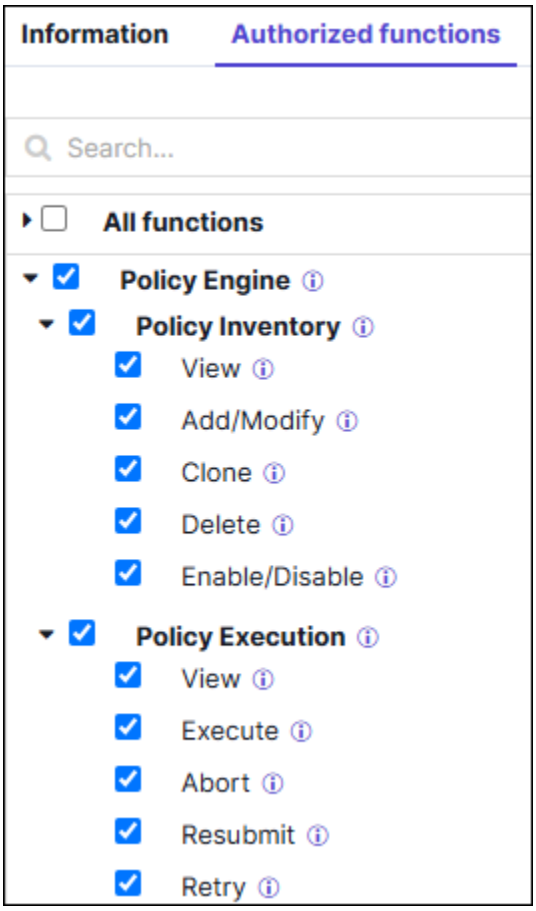
Enabling Policy Engine

Note: By default, Policy Engine is enabled for the admin role, along with **CERT+** and **KUBE+** licenses.

To enable Policy Engine:

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 Engine**, select the checkbox for **Policy Engine**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Note:

- Enabling access to Policy Engine will also grant the necessary permissions for the Certificate, Platform, and Automation modules.
- Users with Policy Engine ACF permissions can create or edit KUBE or CERT policies in Policy Engine without having the specific ACF permissions required for KUBE and CERT.

- **Policy Inventory**: This 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
View	Grants access to view the inventory.
Add/Modify	Allows users to create and modify policies.
Clone	Allows users to clone existing policies

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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

- **Policy Execution**: This permission define the access control and user privileges required to manage and interact with policies. A user may be granted execution permissions based on the access assigned to their role.

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

5. Click **Save**.

Onboard a Certificate Authority

To create a policy, onboard the required Certificate Authority. At present, Policy Engine supports the Certificate Enrollment Policy for all the Certificate Authorities.

Configure SMTP

Policy Engine currently supports approvals and notifications through email only. To send and receive approval/notification emails, configure the SMTP settings.

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 Engine uses the **AppViewXDefault** email template for sending approval and notification emails. This has to be enabled under the **Platform** module.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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

Access to Policies

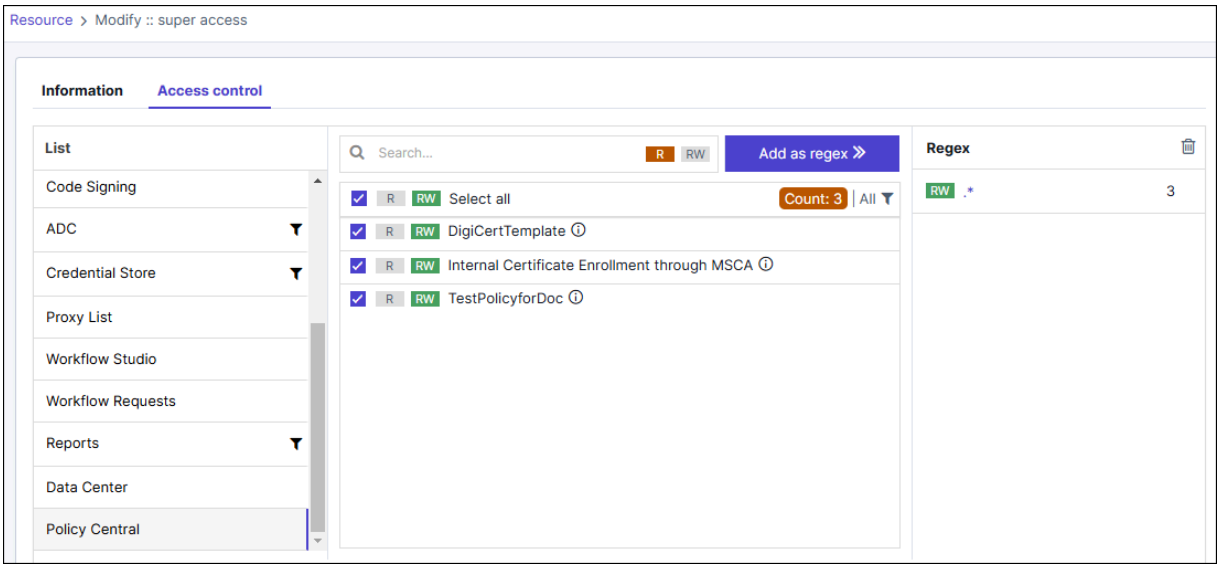
To manage policy access, use User Access option in the Policy Inventory. **Platform** module may be used to grant access to multiple policies based on name patterns or to provide specific access that is required for multiple policies.

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

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- You may create a regex pattern to assign R/RW access. Policies that match the pattern receive 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**.

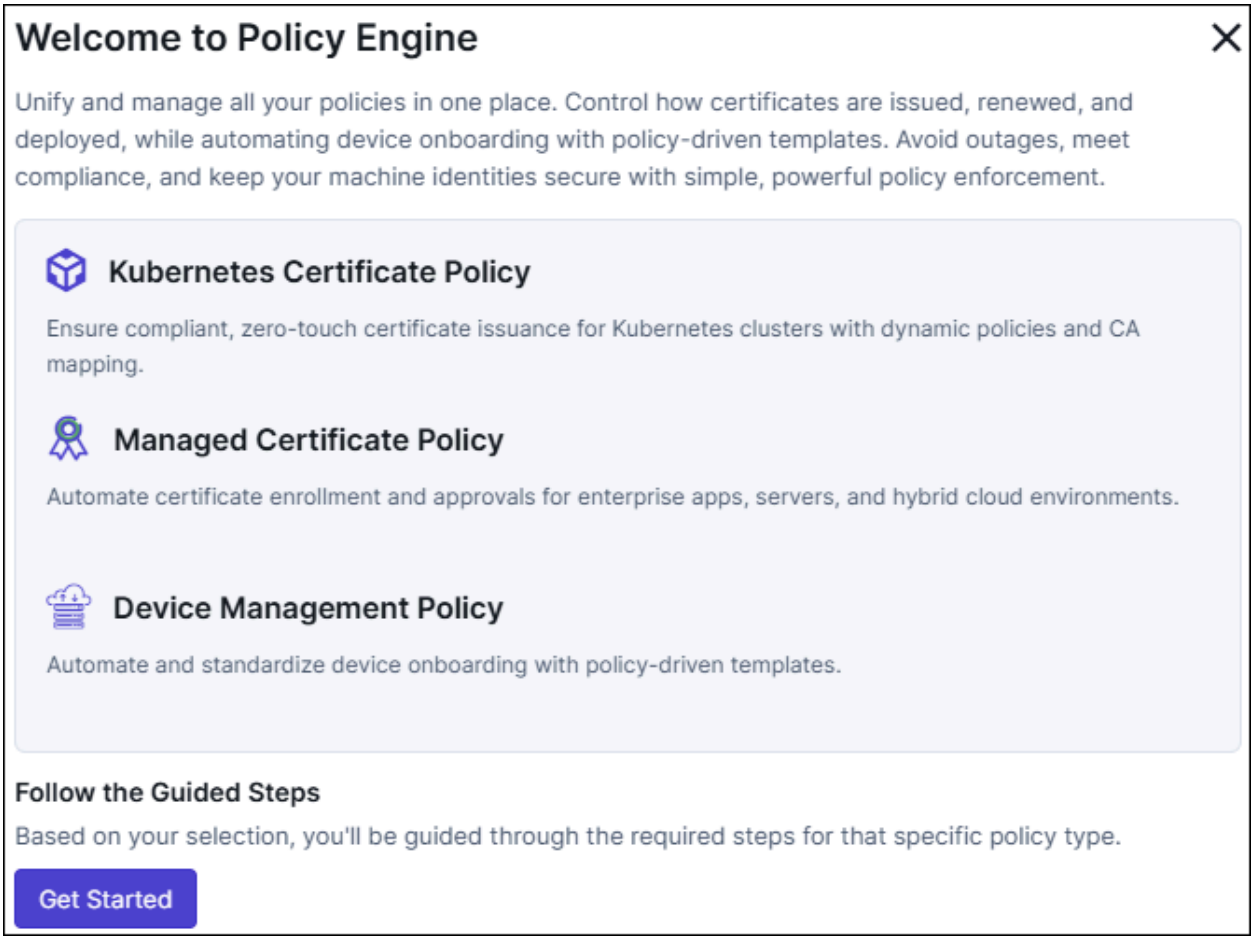
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 3: Getting Started

To enable Policy Engine, see Enabling Policy Engine.

A policy in Policy Engine 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.

After enabling the **Policy Engine**, click the Policy Engine option under **(Menu)** dropdown to go to the Policy Inventory page, where the **Welcome to Policy Engine** popup will be displayed.



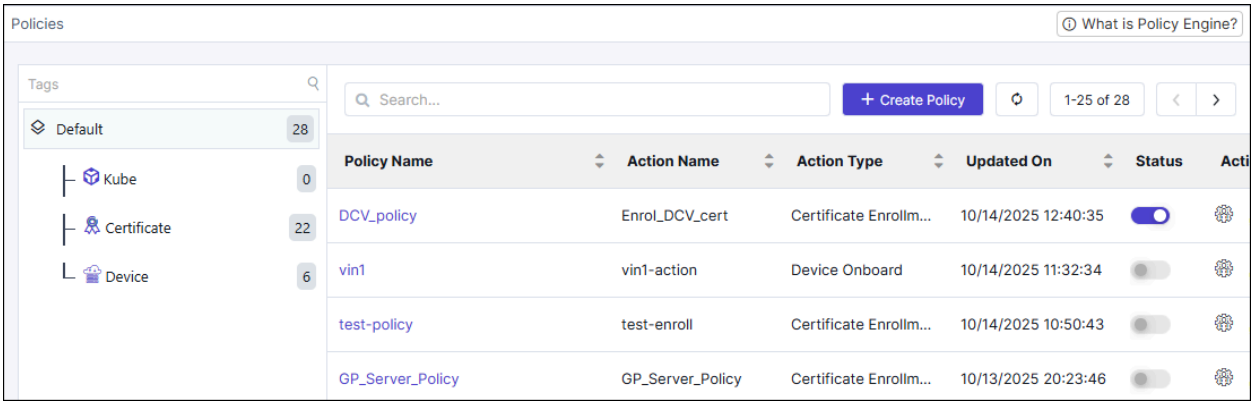
Click **Get Started** to create your first policy.

The Create Policy pop-up is displayed. To configure the policy, see Create Policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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 (For example: 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.



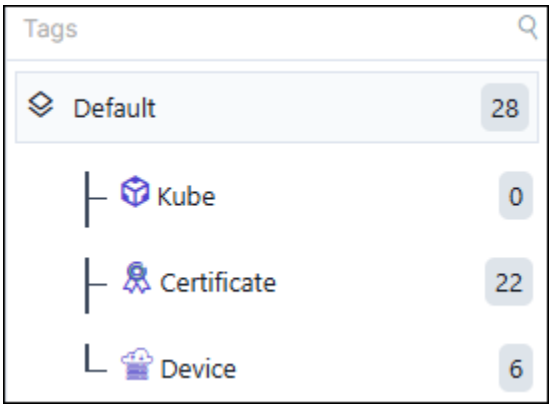
Here are some key elements displayed in the Policy Inventory:

- Tags
- Policy Actions
- Create Policy
- Creating a Cluster Policy Using Policy Engine

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.

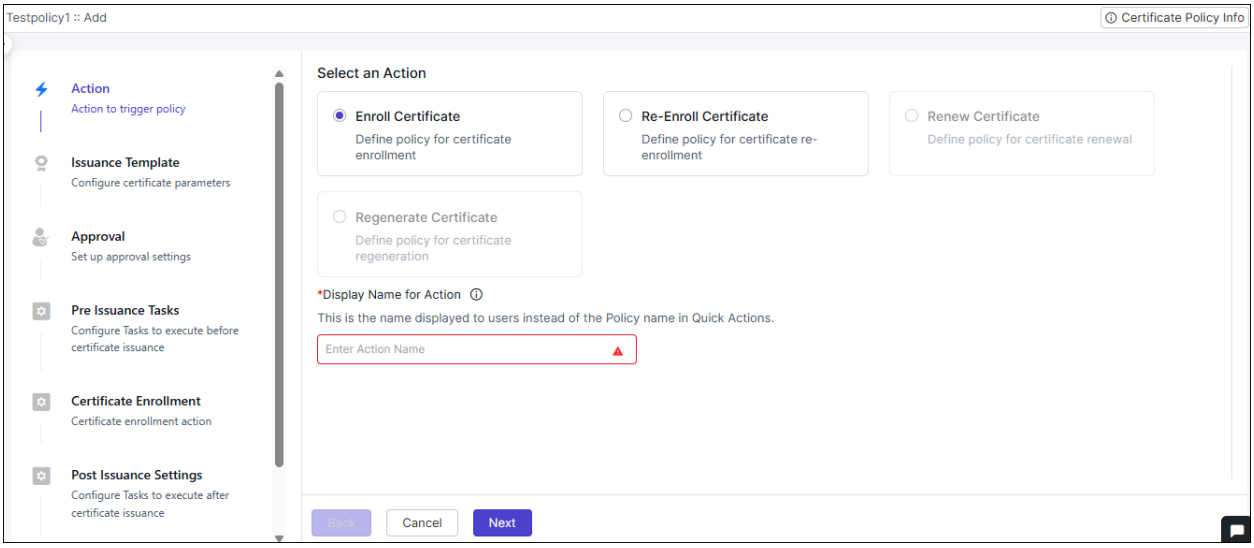
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



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.



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.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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:

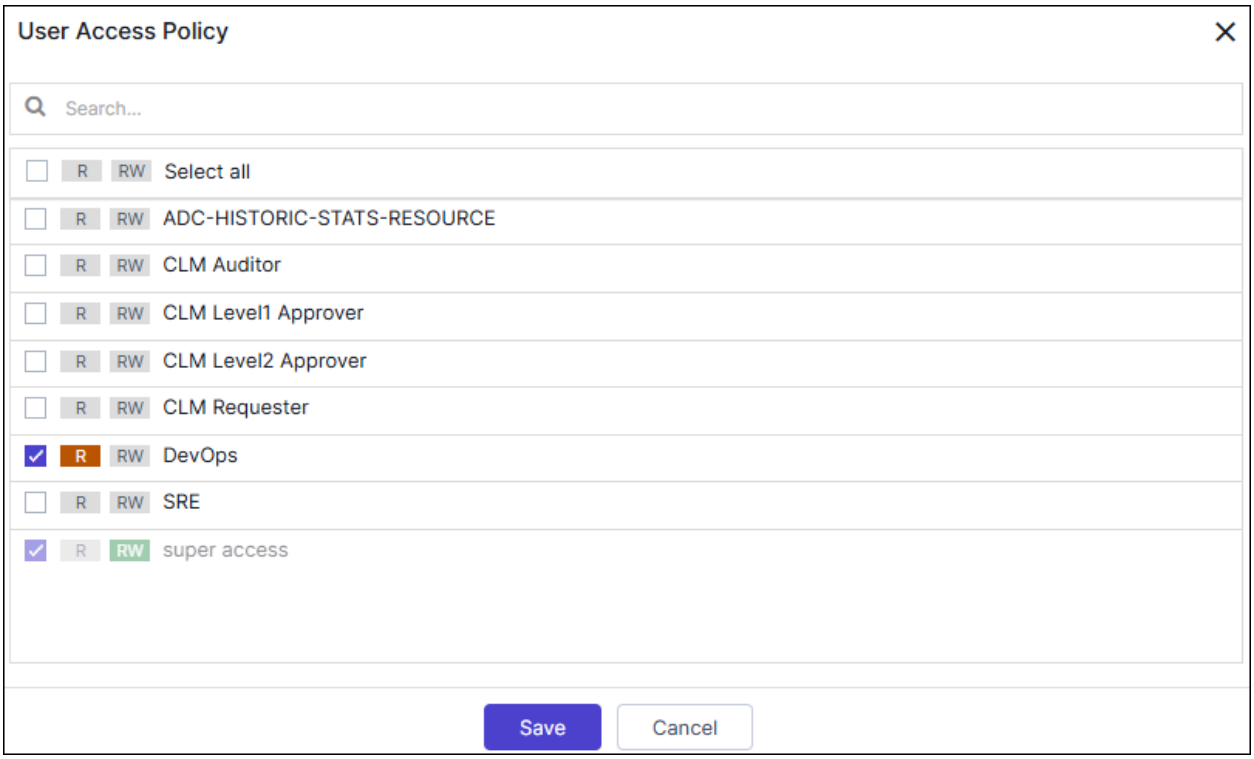
- View the policy
- Execute the policy
- Approve or reject a policy approval request.

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.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



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

1. On the **Policy Inventory** page, below the actions column.
2. Click **(User Access)** icon.

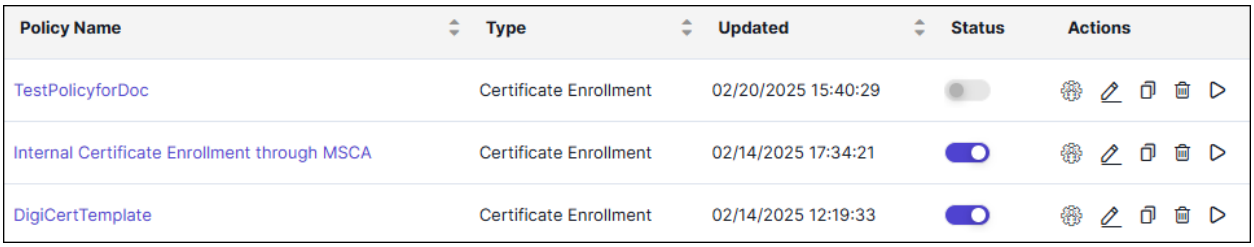
   The **User Access Policy** page is displayed.
3. Select the checkbox for the required user access.
4. Click **Save**.

   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.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



To Edit a policy:

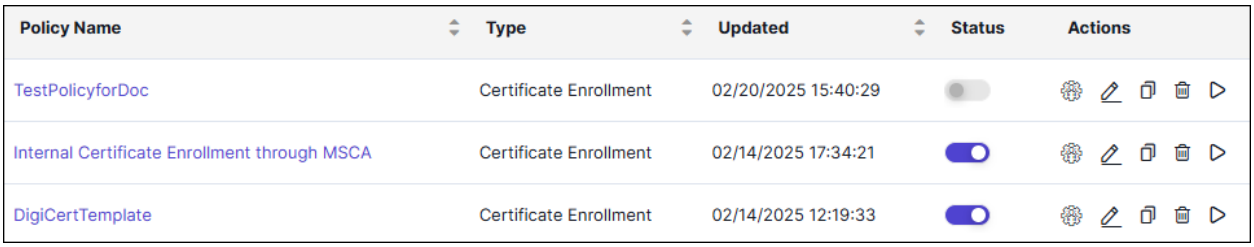
1. On the **Policy Inventory** page, below the actions column.
2. Click **(Edit Policy)** icon.

   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.



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**.

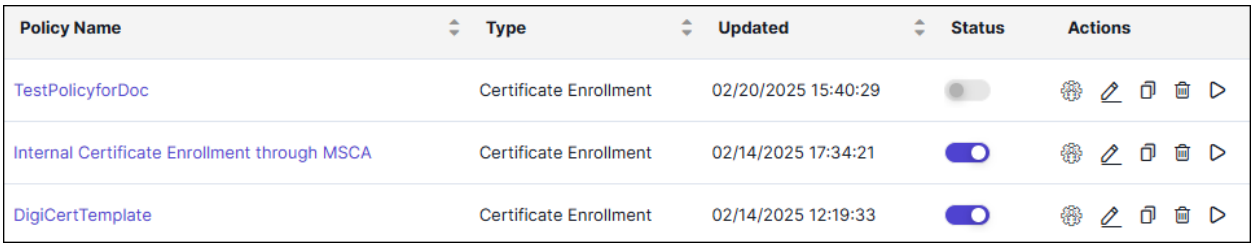
   The selected policy is cloned.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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.



To delete a policy:

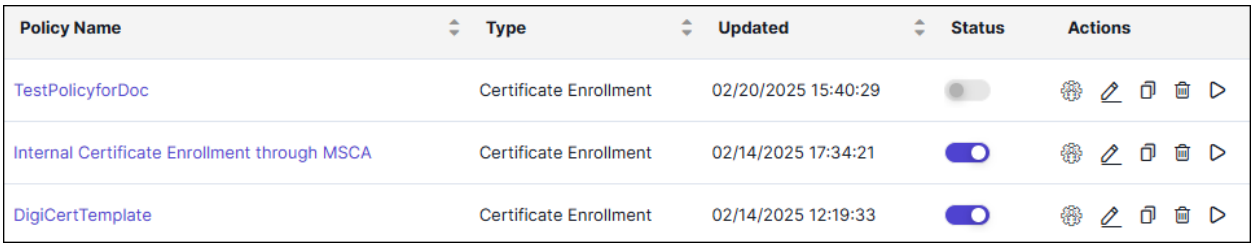
1. On the **Policy Inventory** page, below the actions column.
2. Click **(Delete Policy)** icon.

   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.



To execute a policy:

1. On the **Policy Inventory** page, below the actions column.
2. Click **(Execute Policy)** icon.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Policy Details** popup is displayed.

3. Update the **Certificate Parameters** details.
4. Click **Submit**.

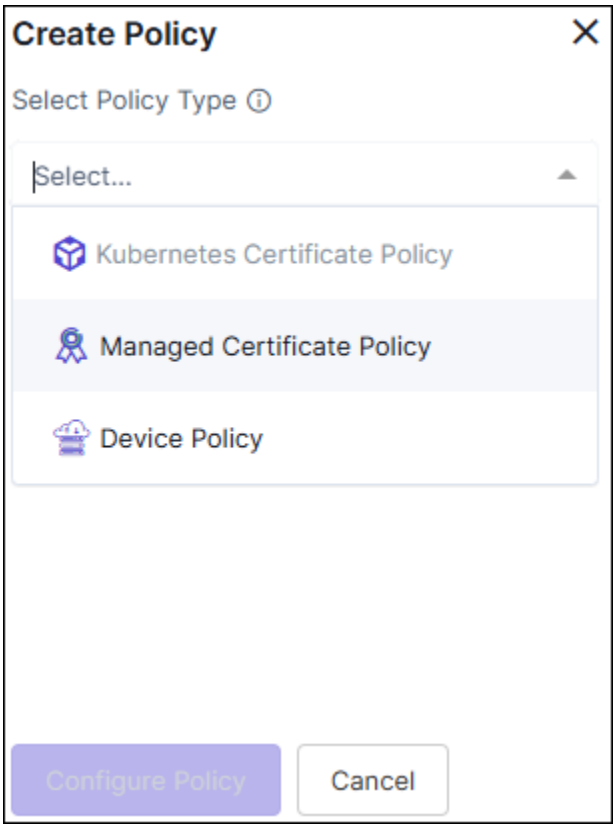
The selected policy is executed successfully.

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 Engine > POLICY MANAGEMENT > Policies**.
   The **Policy Inventory** page is displayed.
2. On the **Policy Inventory** page, click **(+ Create Policy)**.
   The **Create Policy** popup is displayed.
3. Select **Policy Type** from the dropdown.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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

a. **Kubernetes Certificate Policy**

Creating a Cluster Policy.

b. **Managed Certificate Policy**

Create a Certificate Enrollment Policy

Create a Certificate Re-enrollment Policy

c. **Device Policy**

Create a Device Onboarding Policy

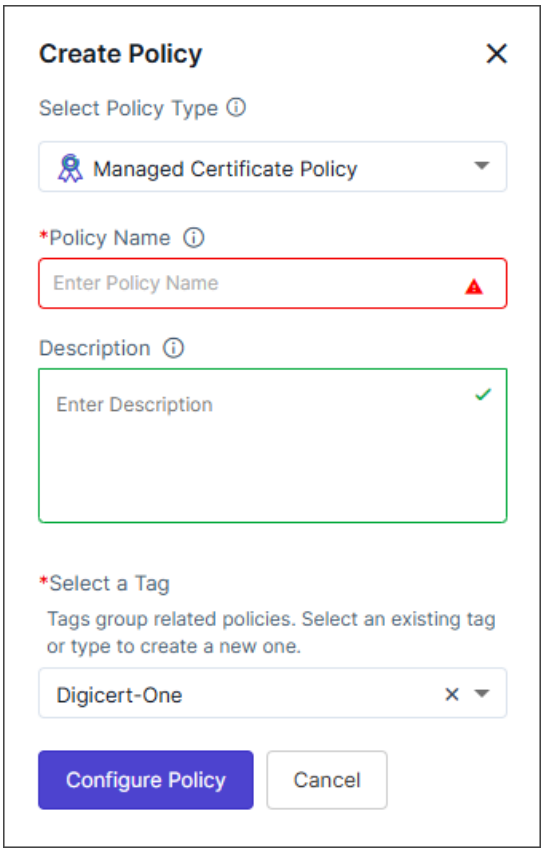
- Create Policy Enroll Certificate
- Create Policy Re-Enroll Certificate
- Create Policy for Device Onboarding

Create Policy Enroll Certificate

To create a new Enroll Certificate policy:

1. Go to **(Menu) > Policy Engine > POLICY MANAGEMENT > Policies**.
   The **Policy Inventory** page is displayed with all policies displayed for Kube, Certificate, and Device.
2. Click **(+ Create Policy)**.
   The **Create Policy** pop-up is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



3. In the **Create Policy** pop-up, from the **Select the Policy Type** dropdown, select **Managed Certificate Policy**.

   The fields for creating the device policy are displayed.
4. Enter/Select values for configuring the policy as described in the table below.

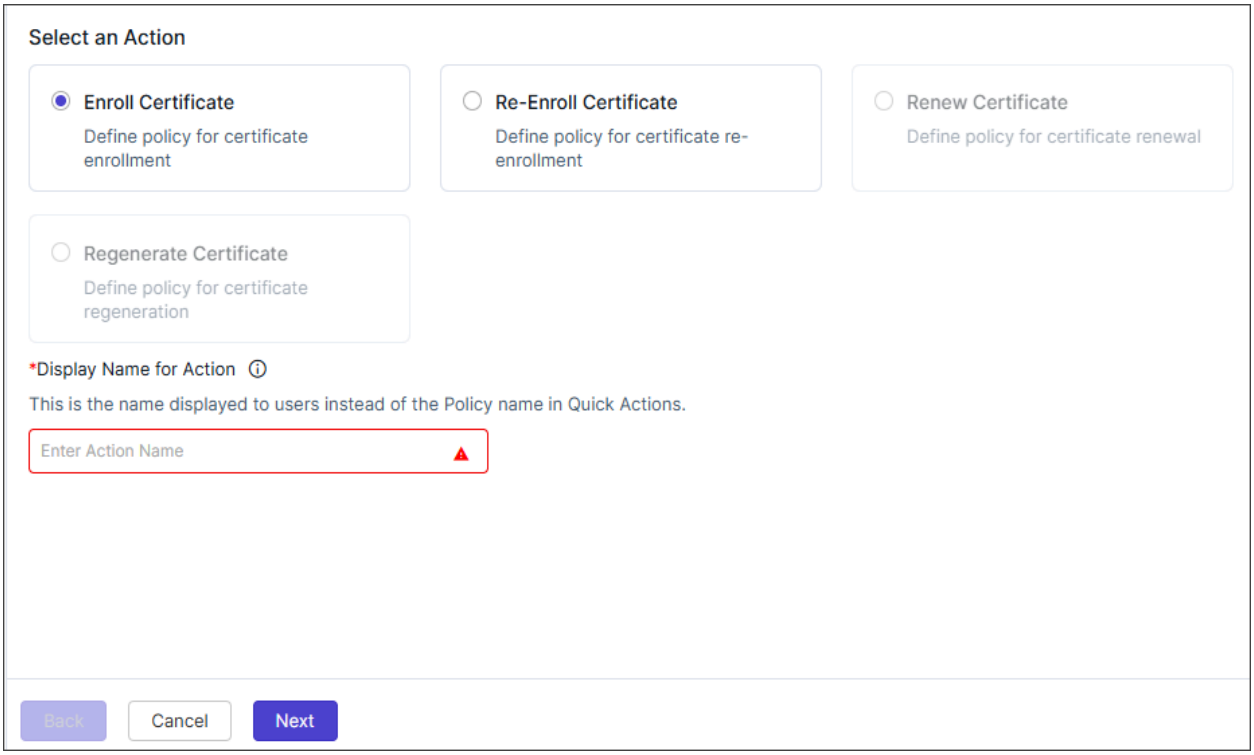
Field	Description
***Policy Name**	Enter a policy name that can include alphabets, numbers, and the special characters - (dash), _ (underscore).
Description	Enter a description for the policy.
***Select a Tag**	Select an existing tag or type to create a new one. Tags group the related policies. **Note:** Selecting the appropriate policy type allows you to group policies logically, simplifying organization and management based on specific criteria.
**: Mandatory field*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Click **Configure Policy**.
   The **Create a Certificate Enrollment Policy in 7 Simple Steps** pop-up is displayed with a short description of each step.
6. Click **Close** on the pop-up.
   The first of the seven steps, **Action** is enabled.

Selecting Action

The Action step lets you select a specific action to trigger the policy.



1. Enter/select the values as described in the table below.

Field	Description
Select an Action	Defines the policy for certificate enrollment. Select **Enroll Certificate**.
***Display Name for Action**	Enter the action name that is to be displayed to users instead of the Policy name in Quick Actions. This field accepts alphanumeric values and special characters - (dash), _ (underscore), and space.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

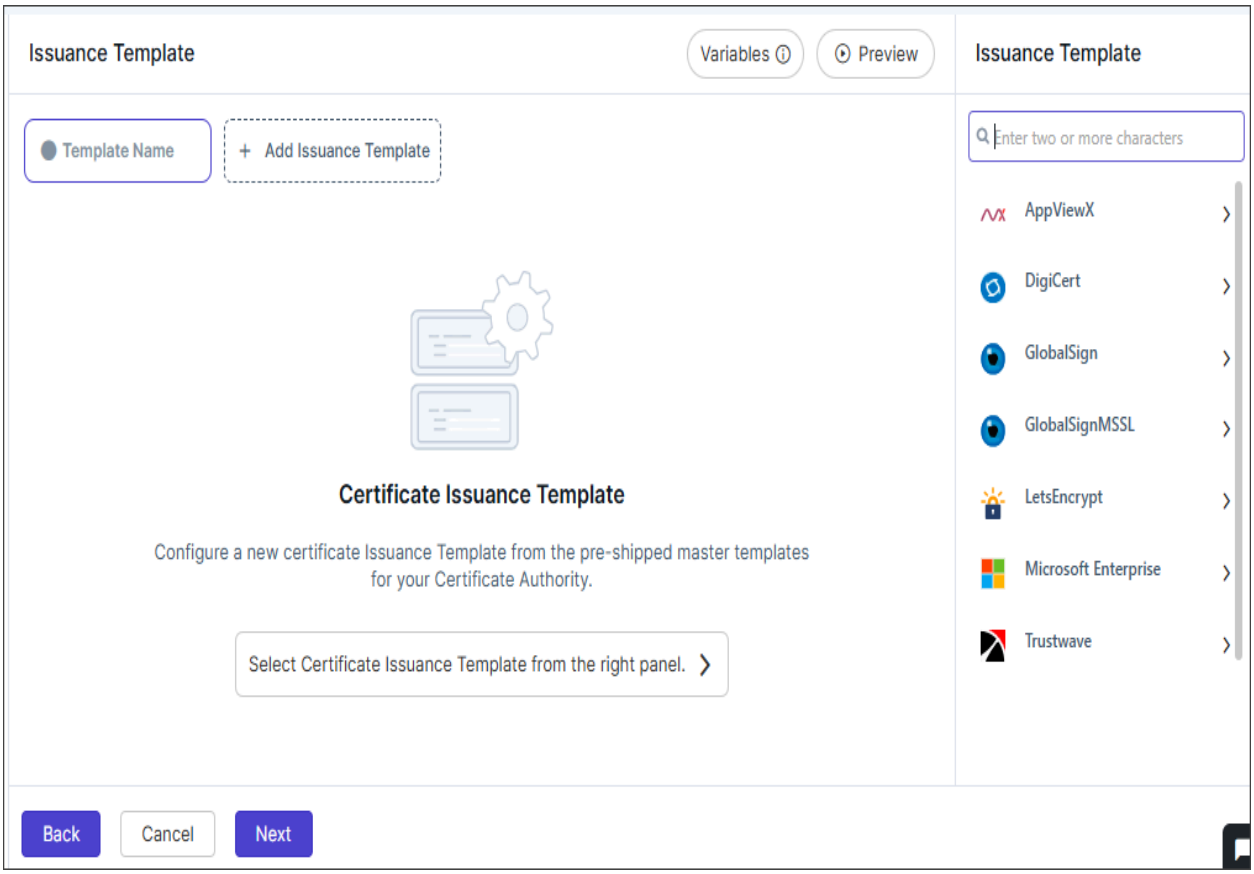
Field	Description
	Click the info icon to preview the Quick Actions.
**: Mandatory field*	

2. Click **Next**.

   The second step, the **Issuance Template** page is displayed.

Configuring 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. Multiple templates can be added.



1. Select a **Issuance Template** from the right panel.

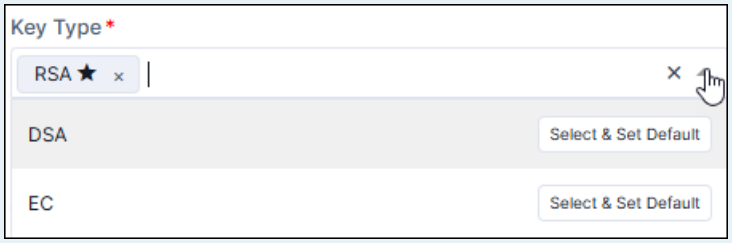
   A pre-shipped master template is displayed in the right panel.
2. Select the desired template.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The blank template form is displayed. This page displays the CA templates to configure certificate and vendor-specific parameters for the enrollment policy.

Note:

- While entering values for multi-select fields, it is mandatory to make any one of the values as default, by clicking the **Select & Set Default** button next to the value. See the image below.



- Each field type text-box, multi-select, dropdown, checkbox and others can be customized by selecting the (settings) icon next to the field. See to the section Field Customizations for more details

3. Enter field information for the vendors as described here.
4. [*Optional*] Click + Add Custom Field button to include additional custom fields.
   The **Add Custom Field** pop-up is displayed.
5. Enter/Select the values in the **Add Custom Field** pop-up as described in the table below.

Field	Description
Include this Custom Field as a Certificate Attribute	Enable or disable the toggle button to include or exclude the custom field as a certificate attribute.
Store this field value in an encrypted format	Enable or disable the toggle button to store the field value in an encrypted or non-encrypted format.
***Field Name**	Provide a field name for the custom field in alphanumeric format.
***Field Type**	Select a field type for the custom field. The available types are: • Label • Text Box • Text Area • Radio Button • Checkbox

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• Select Box • Multi-select Box
Field Value	Specify a default value for the field. The value can be modified according to the field type. For fields that accept multiple entries, use a comma-separated format.
**: Mandatory field*	

6. Click the **Add** button in the **Add Custom Field** pop-up to enable the value in the Vendor Template form.

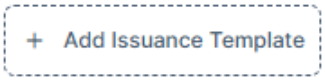
> **Note:** After adding custom fields, a (Settings) icon will appear to customize the field type, and a (Delete) icon will be available to remove the field from the form.

7. Click 

(**Preview**) to view the form information.

> **Note:** Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option, next to Preview. Variables can be inserted into text content and at runtime, they are replaced with actual values.

8. Click the **Save Template** dropdown next to the **Issuance Template** header, then select **Save as New** to create a new template and save this configuration as a reusable template for future use.
   The **Save as Template** pop-up is displayed.
9. Enter the **Template Name** and enter a template **Description.** (Template names can include alphanumeric and the - (dash), _ (underscore), and space special characters.)
10. Click **Save** on the pop-up.
    The Vendor template is saved successfully.
11. [*Optional*] Add another template, if required. Click 

and follow the steps above.
12. Click **Next**.
    The third step, the **Approval** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Customizations for Issuance Templates

1. **Label**

   There is no customization for labels.

2. **Text Box** - The customizations fields for Text Box are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Place holder	Enter the temporary text displayed inside the text box before the user enters any value. It provides a hint or example of what the user should type in that field.
Validation	Select or enter the customRegEx. Validation defines the rules that the input must meet before it can be submitted.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

Note: If any one of the toggle buttons are enabled Hide Field, Read Only, or Set as mandatory, then the other two toggle buttons remain disabled.

3. **Text Area** - The customizations fields for Text Area are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

4. **Radio Button** - The customizations fields for Radio Button are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

5. **Checkbox** - The customizations fields for Checkbox are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

6. **Select Box** - The customizations fields for Select Box are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

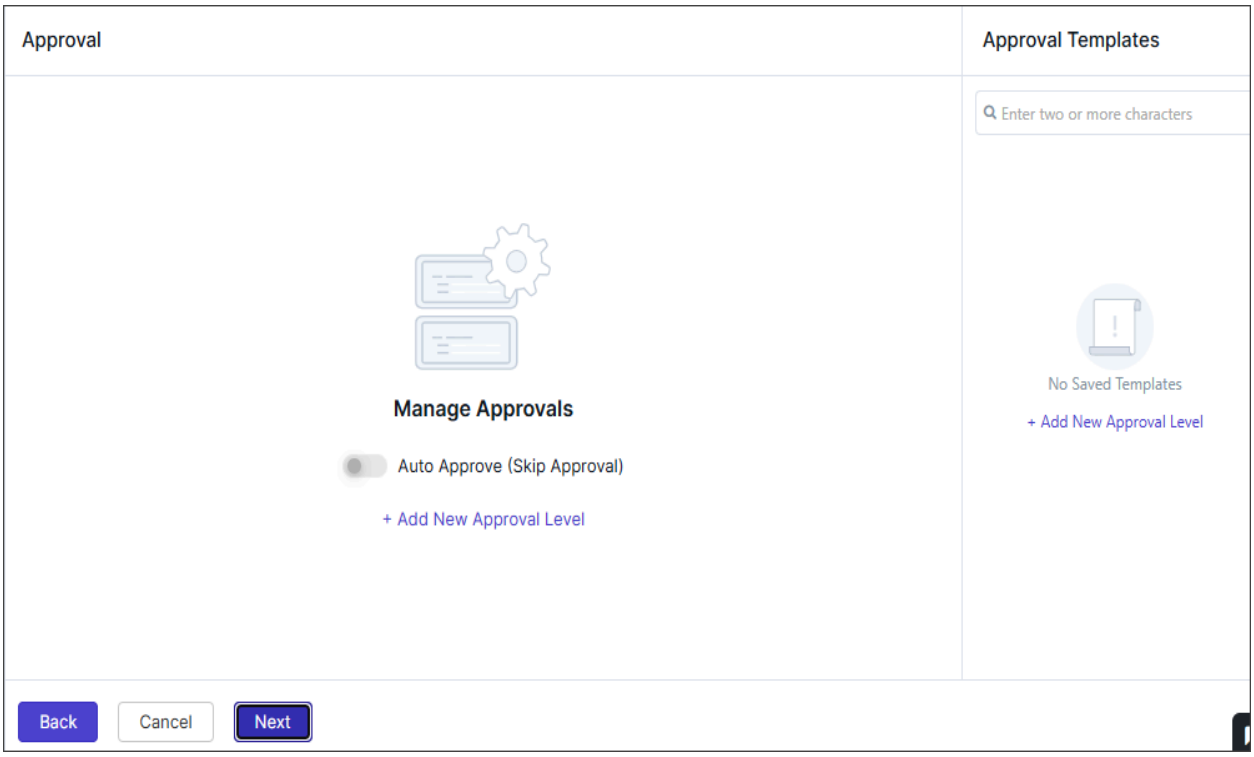
7. **Multi-select Box** - The customizations fields for Multi-select Box are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

Setting Approval

The Approval step allows you to manage the approval workflow before onboarding execution. You can choose to enable auto-approval or define approval levels, which can be configured as explained below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



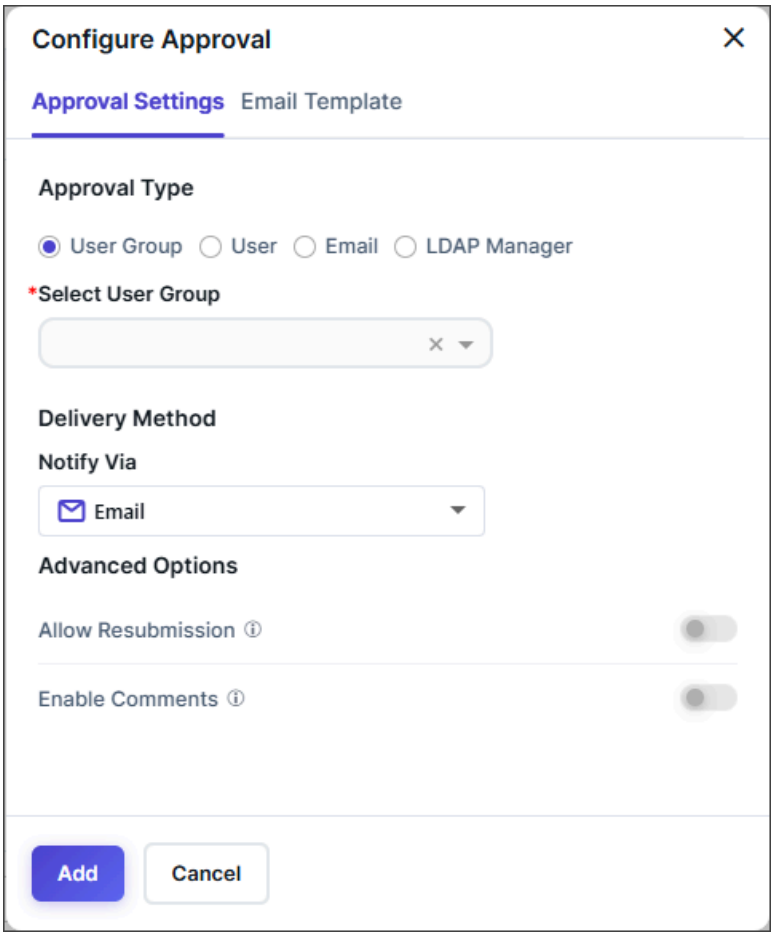
Auto-Approval

1. Enable the **Auto Approve (Skip Approval)** toggle button.
2. Click **Next**.
   The fourth step, **Pre Issuance Task** page is displayed.

Adding New Approval Level

1. Click **+ Add New Approval Level**.
   The **Configure Approval** pop-up is displayed with the **Approval Settings** tab (selected by default) and the **Email Template** tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



2. From the **Approval Settings** tab, configure the Approval Settings based on the **Approval Type** radio button selection as described below.

   a. If the **Approval Type** = **User Group**, enter/select the fields in the table below.

Field	Description
***Select User Group**	Select the User group(s) from the multi-select dropdown.
**: Mandatory field*	

   b. If the **Approval Type** = **User**, enter/select the fields in the table below.

Field	Description
***Select User**	Select the User(s) from the multi-select dropdown.
**: Mandatory field*	

   c. If the **Approval Type** = **Email**, enter/select the fields in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Select Email**	Enter a valid email address. Use either comma-separated email IDs, or a single variable like **${template_email}**.
**: Mandatory field*	

d. If the **Approval Type** = **LDAP Manager**, enter/select the fields in the table below. This option enables approval based on the manager information retrieved from the LDAP directory.

Field	Description
***Select LDAP Server**	Specifies which LDAP server to connect to for fetching user and manager details. Choose an existing LDAP server from the dropdown list or enter the connection URL manually.
***Customize LDAP Query** - Allows you to define or modify the LDAP query parameters used to identify the user and their manager. When enabled, additional fields appear to customize how LDAP attributes are queried.	
User Filter Attribute	Defines the LDAP attribute used to locate the requesting user
User Return Attribute	Specifies which LDAP attribute should be retrieved from the user's record to identify their manager.
Manager Filter Attribute	Defines the LDAP attribute used to locate the manager's record in LDAP.
Manager Return Attribute	Specifies which attribute value from the manager's record should be returned and used as the approver's identifier (For example: email address).
**: Mandatory field*	

e. In the **Delivery Method** section, select the values as follows:

Field	Description
Notify Via	The dropdown has the value **Email** selected by default.

f. In the **Advanced Options** section, select the values as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Allow Resubmission	Enable the toggle button to allow resubmission of the policy request. The button is disabled by default.
Enable Comments	Enable the toggle button to allow approvers to add comments to the policy request. The button is disabled by default.
**: Mandatory field*	

3. From the **Email Template** tab, enter/select the information as follows:

Field	Description
Template Name	Choose an email template to customize approval notifications
Email Templates	Enable the toggle buttons to use any of the templates below: • Approval Request Template • Approval Confirmation Template • Approval Rejection Template To customize the email templates, a. Enable the toggle button of the respective email template b. Click the arrow icon next to the toggle button to expand/display the email contents. c. Edit the **Email Subject**, **CC** (Carbon Copy), and **Email Content**. **Note:** Users can copy predefined variables (For example: ${user.firstName}, ${user.lastName}) from the  option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.
**: Mandatory field*	

4. Click **Add**.
   The Approval template is displayed with the Edit and Delete icons and the option to further Add New Approval levels.
5. Click the **Save Template** dropdown next to the **Approval** header, then select **Save as New** to create a new template and save this configuration as a reusable template for future use.

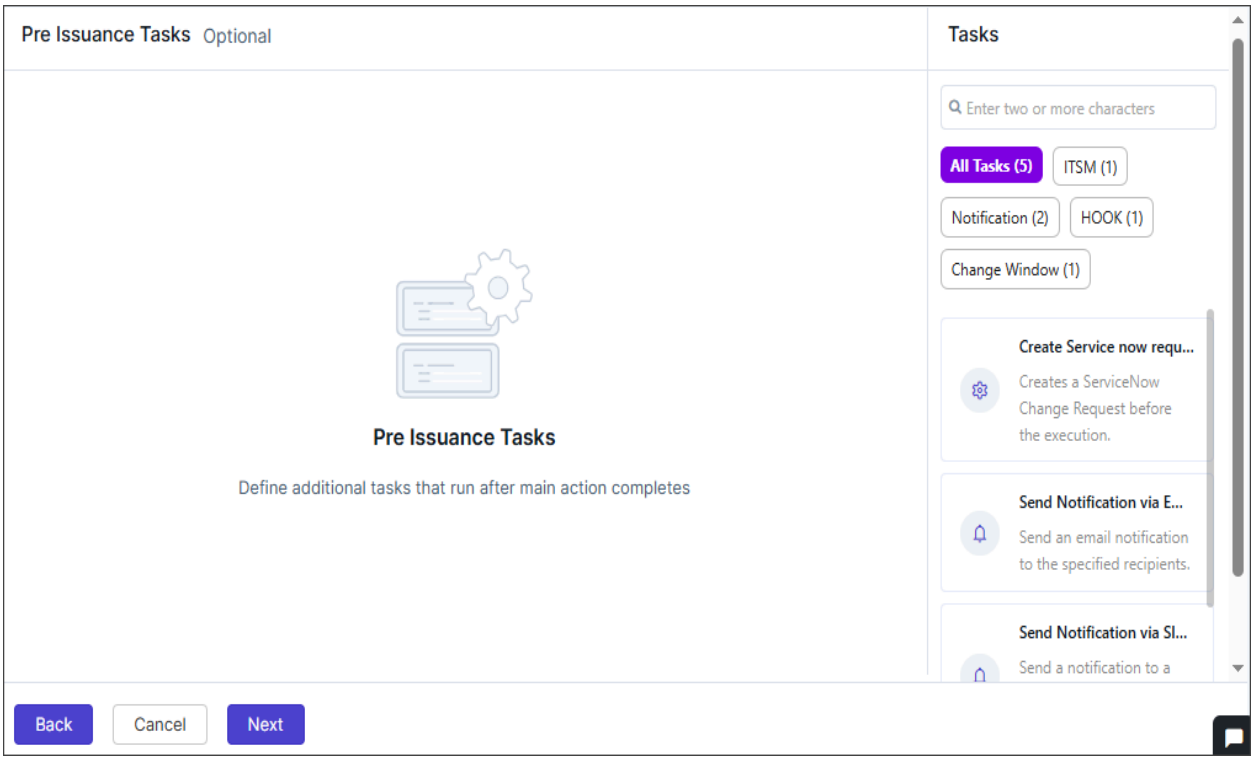
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The Save as Template pop-up is displayed.

6. Enter the **Template Name** and enter a template **Description.** (Template names can include alphanumeric and the - (dash), _ (underscore), and space special characters.)
7. Click **Save** on the pop-up.
   The Approval level template is saved successfully.
8. Click **Next**.
   The fourth step, the **Pre Issuance Task**page is displayed.

Configuring Pre Issuance Tasks

This is an optional fifth step that lets you configure tasks to execute before certificate issuance. A Task panel is available on the right with five tasks as follows:



1. **ITSM** - Create a ServiceNow Change Request before the execution.
2. **Notifications**
   a. **Send Notification via Email** - Send an email notification to the specified recipients.
   b. **Send Notification via Slack** - Send a notification to a Slack channel using the configured webhook URL.
3. **Hook Execution** - Initiates the execution of the selected hook.
4. **Configure Change Window** - Allows users to configure a change window during which the policy tasks should be executed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

ITSM - Create a ServiceNow Change Request

Enter the following fields to configure the ServiceNow Change Request.

Field	Description
Configuration tab	
***Configuration tab* - ServiceNow Instance**	
Configure ServiceNow Instance	Select or configure the type of ServiceNow instance.
***Configuration tab* - Change Request Fields**	
Type	Defines the type of ServiceNow request to be created (For example: Normal, Emergency, Standard). Select the value from the dropdown.
Priority	Specifies the urgency level or importance of the change request. Select the value from the dropdown (1-Critical, 2-High, 3-Moderate, 4-Low).
Short Description	A brief summary or title describing the purpose of the change request.
Description	A detailed explanation of the change request, including context or justification.
Category	Classifies the change under a specific functional or operational category.
Risk	Select the potential risk level associated with implementing the change. Select the value from the dropdown (VeryHigh, High, Moderate, Low, None).
Impact	Specifies the extent to which the change might affect users, services, or infrastructure. Select the value from the dropdown (1-High, 2-Medium, 3-Low).
Urgency	Reflects how quickly the change needs to be addressed or implemented. Select the value from the dropdown (1-High, 2-Medium, 3-Low).
Assignment Group	The ServiceNow group responsible for reviewing and implementing the change.
CAB Required	Specifies whether the change requires approval from the Change Advisory Board (CAB). Select value **True** or **False**.
Wait for State Change	Determines whether AppViewX should pause workflow execution until the ServiceNow change request reaches a specific state. Select value **True** or **False**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Notifications - Send Notification via Email

Enter the following fields to set up notifications for Email or Slack.

Field	Description
Configuration tab	
***Recipient Type**	Select either or all of the following: • User Group • User • Email
***User Group**	This field is enabled when **Recipient Type = User Group**. Select single or multiple user groups.
***User**	This field is enabled when **Recipient Type = User** Select single or multiple users.
***Email**	This field is enabled when **Recipient Type = Email.** Enter a valid email address. Use either comma-separated email IDs, or a single variable like **${template_email}**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	Select the email template name.
***Email Subject**	This field is enabled when **Notify Via = Email**. Enter the subject for the email. Use the **Variables** option to add database values as variables.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Notifications - Send Notification via Slack

Enter the following fields to set up notifications for Email or Slack.

Field	Description
Configuration tab	
***Slack Channel**	This field is enabled when **Notify Via = Slack**. Select the slack channel.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory field	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Hook Execution

Enter the following fields to configure the hooks.

Field	Description
Configuration tab	
***Configuration tab* - Hook** (Select a hook from the available inventory that you want to execute.)	
Task Name	Displays the default name of the task (*Hook Execution*). You can rename it if needed for clarity in the workflow.
Select Hook	Choose the specific hook (script or API integration) to be executed within the workflow.
***Configuration tab* - Expose Variables**	
Do you want to expose hook response as variables for following tasks?	Toggle this option to expose the hook's response as variables for use in subsequent workflow tasks. Enables or disables the ability to pass hook output values as input variables to later tasks in the workflow.
Output Variable Mapping	Map output variables from the hook response to custom keys for easier reference in subsequent tasks. Paste the expected JSON response from the hook to view and select available variables. **Fields:** • **Variable Key:** Enter a custom key name for the variable. • **Output Variable:** Select the output variable path from the JSON response (options include `$.output`, `$.path`, `$.type`).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To add variables, click  button.
Expected Response Format	Paste a sample JSON response from the hook in the `output {}` section. This helps AppViewX identify available response parameters for variable mapping and validation.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Configuring Change Window

This page allows users to define a specific **change window** a scheduled timeframe during which policy-related tasks can be executed.

Field	Description
Configuration tab	
Change Window Configuration	Configure when policy changes are allowed to run. Use the **Preview Windows** option to visualize the scheduled change windows based on the selected configuration.
***Mode Selection**	Choose the frequency or recurrence pattern for the change window. The options available are as follows: • **Daily:** Executes policy tasks during the defined window each day. • **Weekly:** Executes tasks on specific days of the week. • **Monthly:** Executes tasks on specified dates or weeks within a month. • **User Defined:** Allows users to define a custom schedule or window duration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Daily Schedule Settings	This section is enabled when **Mode Selection = Daily**. Enter the values in the following fields: • ***Start Time** (HH:MM) • ***End Time** (HH:MM)
Weekly Schedule Settings	This section is enabled when **Mode Selection = Weekly**. Enter the values in the following fields: • ***Day of the Week** - (select Monday, Tuesday etc.) • **End Day of Week** (Optional) (select Monday, Tuesday etc.) • ***Start Time** (HH:MM) • ***End Time** (HH:MM)
Monthly Schedule Settings	This section is enabled when **Mode Selection = Monthly**. Enter the values in the following fields: • ***Day of the Month** - (select date between 1-31) • **End Day of Month** (Optional) (select date between 1-31) • ***Start Time** (HH:MM) • ***End Time** (HH:MM)
Custom Date & Time	This section is enabled when **Mode Selection = User Defined**. Enter the values in the following fields: • ***Explicit Start Time** (YYYY-MM-DDTHH:MM:SSZ) • ***Explicit End Time** (YYYY-MM-DDTHH:MM:SSZ)
***Missed Window Policy**	Determines the system behavior if a task misses its scheduled change window. Options include: • **Run Next Window:** The task will automatically run during the next available window. • **Skip:** The missed task will be skipped without execution. • **Fail Immediately:** The task will fail immediately if it cannot execute within the defined window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Allow Override	Enables authorized users or groups to allow execution outside the defined change window.
Override Type	This field is enabled when **Allow Override** toggle is enabled. Select from **User Group** or **User**.
User Group	This field is enabled when **Allow Override** toggle is enabled and **Override Type = User Group** Select **User Group** from the dropdown.
User	This field is enabled when **Allow Override** toggle is enabled and **Override Type = User** Select **User** from the dropdown.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

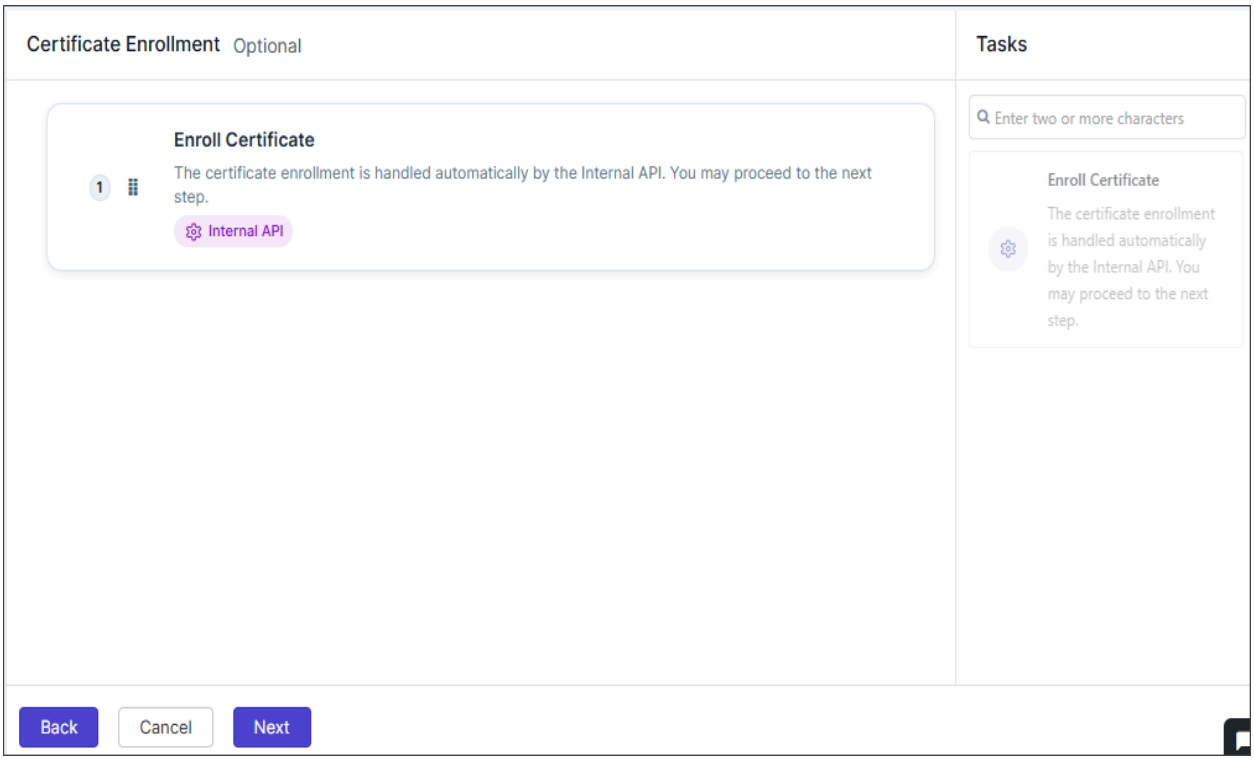
Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Certificate Enrollment

This is an optional fifth step where the certificate enrollment is handled automatically by the Internal API. You may proceed to the next step. There are no actions required on this page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

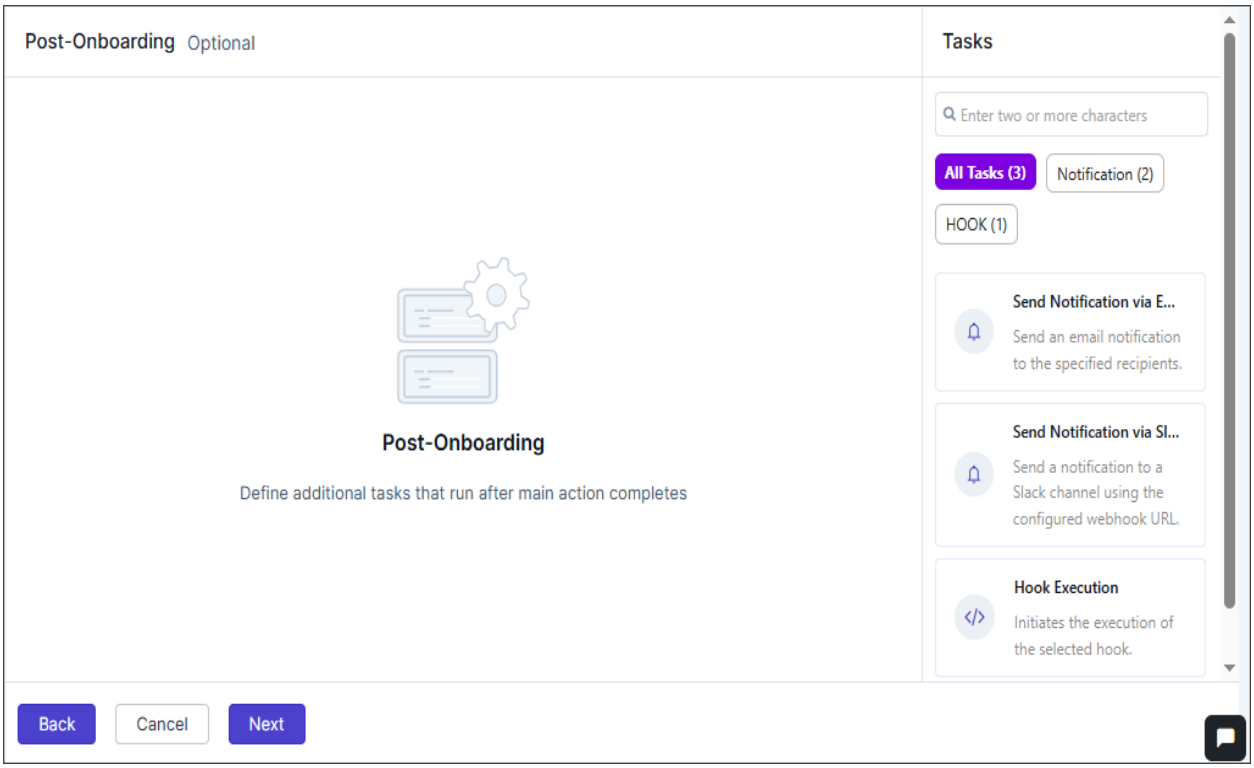


• Click the **Next** button to move to the next step, **Post-Onboarding**.

Configuring Post Issuance Settings

The sixth step in the enroll certificate process is to configure tasks to execute after certificate issuance. These are additional tasks that run after the main action completes. The Task panel on the right has the following tasks to be configured:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



1. Send Notifications via Email (For details, click here)
2. Send Notifications via Slack (For details, click here)
3. Email certificates in zip format (see section below)
4. Hook Execution (For details, click here)

Email Certificates in Zip Format

This task is used to configure an email containing the certificates packaged in a ZIP file to be sent to the requester.

Field	Description
Configuration tab	
***Certificate Type**	Select any of the following certificate types: • PEM (*.crt) • PEM (*.cer) • DER (*.crt) • DER (*.cer) • PKCS#7 Binary (*.p7b) • PKCS#7 PEM (*.p7b)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• PKCS#12 (*.p12) • PKCS#12 (*.pfx) • JKS (*.jks)
Include Root and Intermediate	This checkbox is enabled only for the following certificate types. • PEM (*.crt) • PEM (*.cer) • DER (*.der) If the checkbox is selected, the certificate chain will be included and sent via email.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

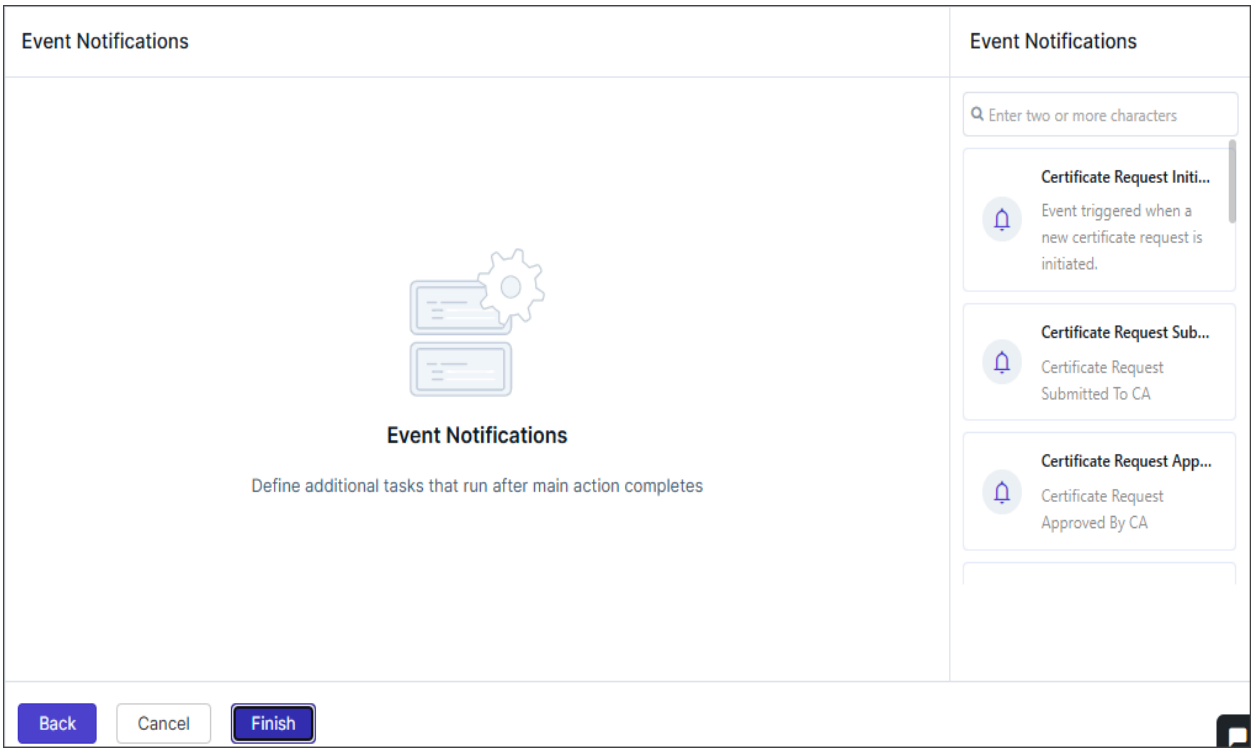
Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Configuring Event Notifications

The final step in the enroll certificate process is to send email notifications to users, groups, or external recipients on certificate enrollment lifecycle events.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



1. Certificate Request Initiated (Event triggered when a new certificate request is initiated.)
2. Certificate Request Submitted To CA (
3. Certificate Request Approved By CA

To configure any of the above emails,

1. From the notification panel on the right, click any of the specific emails to be configured. The <email_name> pop-up is displayed.
   The <email_name> pop-up is displayed.

   Note: All the email templates have the same fields, see to the table below to configure any of the emails.

2. Enter the following details in the email configuration pop-up.

Field	Description
***Notify Via**	Select from the following: • Email • Slack

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Recipient Type**	This field is enabled when **Notify Via = Email**. Select either or all of the following: • User Group • User • Email
***Slack Channel**	This field is enabled when **Notify Via = Slack**. Select the slack channel.
***User Group**	This field is enabled when **Notify Via = Email** and **Recipient Type = User Group**. Select single or multiple user groups.
***User**	This field is enabled when **Notify Via = Email** and **Recipient Type = User** Select single or multiple users.
***Email**	This field is enabled when **Notify Via = Email** and **Recipient Type = User Email.** Enter a valid email address. Use either comma-separated email IDs, or a single variable like **${template_email}**.
***Template Name**	This field is enabled when **Notify Via = Email**. Select the email template name.
***Email Subject**	This field is enabled when **Notify Via = Email**. Enter the subject for the email. Use the **Variables** option to add database values as variables.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.
**: Mandatory field*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

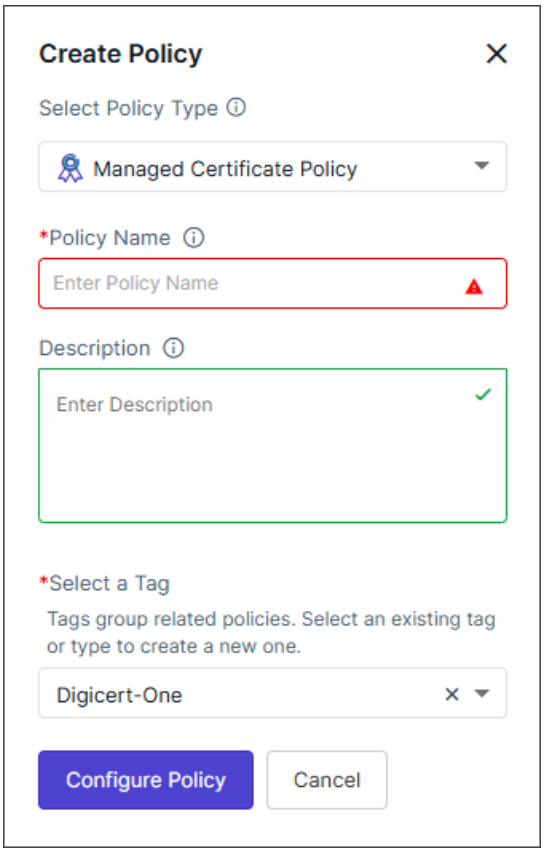
Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the Variables option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

3. Click **Add**.
   The email templates are created successfully.
4. Click **Finish** at the bottom of the screen to complete the enroll certificate policy creation.

Create Policy Re-Enroll Certificate

To create a Re-Enroll Certificate policy:

1. Go to **(Menu) > Policy Engine > POLICY MANAGEMENT > Policies**.
   The **Policy Inventory** page is displayed with all policies displayed for Kube, Certificate, and Device.
2. Click **(+ Create Policy)**.
   The **Create Policy** pop-up is displayed.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. In the **Create Policy** pop-up, from the **Select the Policy Type** dropdown, select **Managed Certificate Policy**.
   The fields for creating the device policy are displayed.
4. Enter/Select values for configuring the policy as described in the table below.

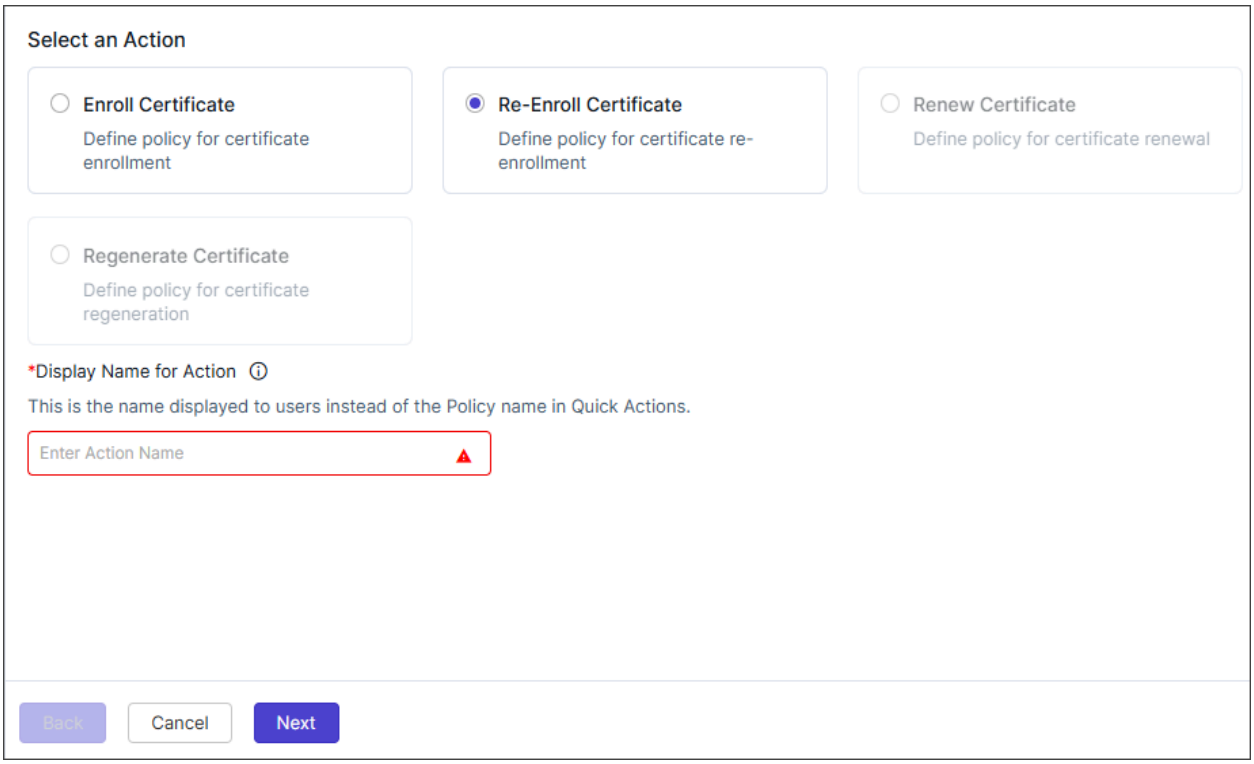
Field	Description
***Policy Name**	Enter a policy name that can include alphabets, numbers, and the special characters - (dash), _ (underscore).
Description	Enter a description for the policy.
***Select a Tag**	Select an existing tag or type to create a new one. Tags group the related policies.  **Note:** Selecting the appropriate policy type allows you to group policies logically, simplifying organization and management based on specific criteria.
**: Mandatory field*	

5. Click **Configure Policy**.
   The **Create a Certificate Re-enrollment Policy in 7 Simple Steps** pop-up is displayed with a short description of each step.
6. Click **Close** on the pop-up.
   The first of the seven steps, **Action** is enabled.

Selecting Action

The Action step lets you select a specific action to trigger the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



1. Enter/select the values as described in the table below.

Field	Description
Select an Action	Defines the policy for certificate enrollment. Select **Enroll Certificate**.
***Display Name for Action**	Enter the action name that is to be displayed to users instead of the Policy name in Quick Actions. This field accepts alphanumeric values and special characters - (dash), _ (underscore), and space. Click the info icon to preview the Quick Actions.
**: Mandatory field*	

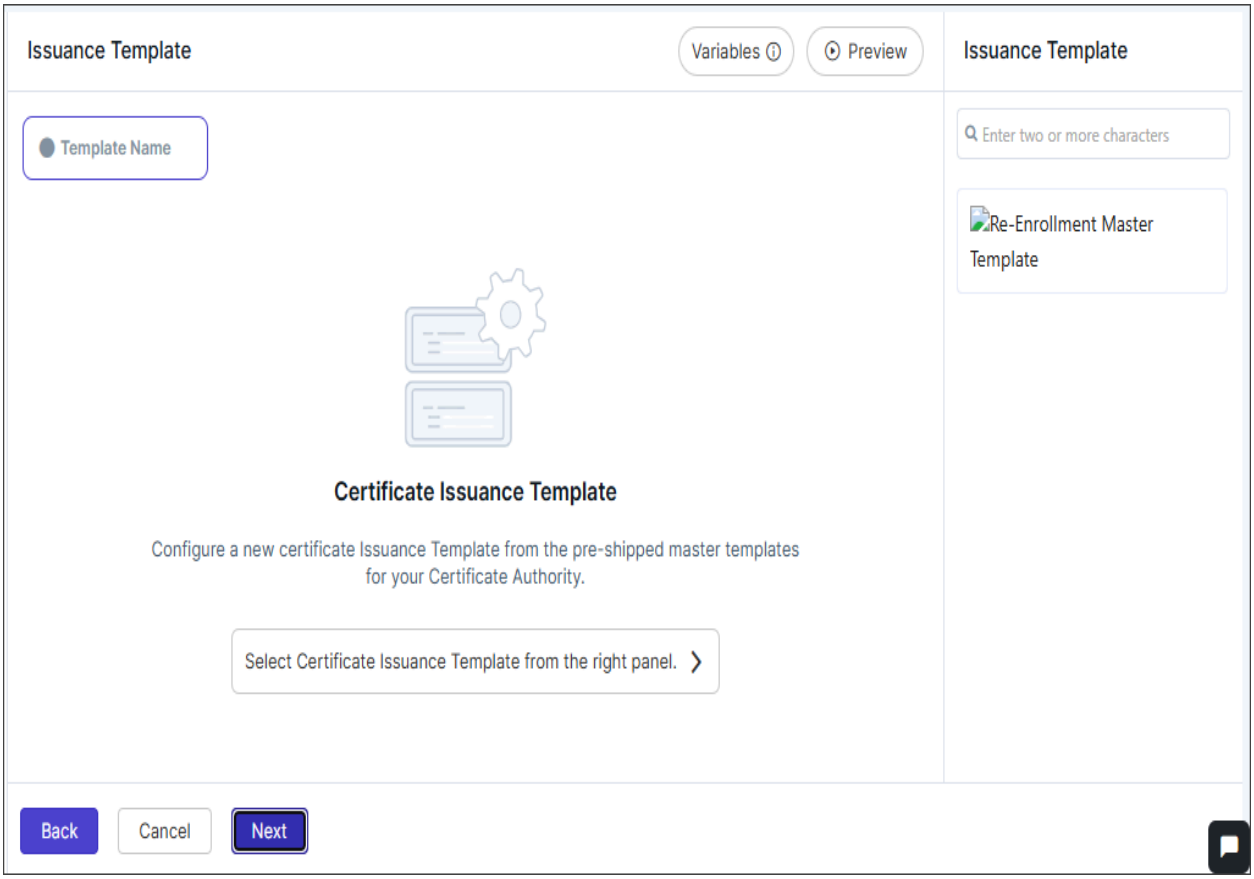
2. Click **Next**.

   The second step, the **Issuance Template** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring 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. Multiple templates can be added.



1. Select the **Re-Enrollment Master Template** from the **Inssuance Template** panel on the right. The Certificate Parameter fields are displayed.
2. Enter/Select values in the **Certificate Parameter** fields as described below.

> **Note:** Only the fields below will be updated in the certificate during re-enrollment.

Field	Description
Organization	Enter the legal name of the organization requesting the certificate re-enrollment.
Organization Unit	Enter the department or division within the organization

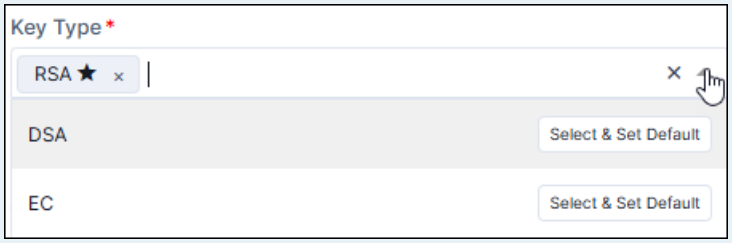
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Locality	Enter the city or locality where the organization is registered or operates.
Street Address	Enter the street name and number associated with the organization’s registered location.
State	Enter the state or province of the organization’s address.
Country	Enter the two-letter ISO country code (e.g., *US*, *IN*) representing the organization’s location.
Postal Code	Enter the postal or ZIP code corresponding to the organization’s address.
Email Address	The contact email address associated with the certificate request, typically used for validation or notifications.
*** Key Type**	Select the cryptographic algorithm used to generate the private and public key pair (For example: *RSA*, *ECDSA*).
*** Hash Function**	Select the hashing algorithm to be used during CSR generation (For example: *SHA-256*, *SHA-384*)
*** Validity Unit**	Select the unit of time used to specify the certificate’s validity period (*Days, Months, Years*).
*** Validity in Days**	This field is displayed if the **Validity Unit** = **Days**. Enter the number in the field and then hit the Enter key for the value to be selected.
*** Validity in Months**	This field is displayed if the **Validity Unit** = **Months**. Enter the number in the field and then hit the Enter key for the value to be selected.
*** Validity in Years**	This field is displayed if the **Validity Unit** = **Years**. Enter the number in the field and then hit the Enter key for the value to be selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- While entering values for multi-select fields, it is mandatory to make any one of the values as default, by clicking the **Select & Set Default** button next to the value. See the image below.



- Each field type text-box, multi-select, dropdown, checkbox and others can be customized by selecting the (settings) icon next to the field. See to the section Field Customizations for more details

3. [*Optional*] Click + Add Custom Field button to include additional custom fields.
   The **Add Custom Field** pop-up is displayed.
4. Enter/Select the values in the **Add Custom Field** pop-up as described in the table below.

Field	Description
Include this Custom Field as a Certificate Attribute	Enable or disable the toggle button to include or exclude the custom field as a certificate attribute.
Store this field value in an encrypted format	Enable or disable the toggle button to store the field value in an encrypted or non-encrypted format.
***Field Name**	Provide a field name for the custom field in alphanumeric format.
***Field Type**	Select a field type for the custom field. The available types are: • Label • Text Box • Text Area • Radio Button • Checkbox • Select Box • Multi-select Box

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Field Value	Specify a default value for the field. The value can be modified according to the field type. For fields that accept multiple entries, use a comma-separated format.
**: Mandatory field*	

5. Click the **Add** button in the **Add Custom Field** pop-up to enable the value in the Vendor Template form.

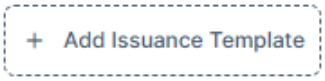
> **Note:** After adding custom fields, a (Settings) icon will appear to customize the field type, and a (Delete) icon will be available to remove the field from the form.

6. Click 

(**Preview**) to view the form information.

> **Note:** Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option, next to Preview. Variables can be inserted into text content and at runtime, they are replaced with actual values.

7. Click the **Save Template** dropdown next to the **Issuance Template** header, then select **Save as New** to create a new template and save this configuration as a reusable template for future use.
   The **Save as Template** pop-up is displayed.
8. Enter the **Template Name** and enter a template **Description.** (Template names can include alphanumeric and the - (dash), _ (underscore), and space special characters.)
9. Click **Save** on the pop-up.
   The Vendor template is saved successfully.
10. [*Optional*] Add another template, if required. Click 

and follow the steps above.
11. Click **Next**.
    The third step, the **Approval** page is displayed.

Field Customizations for Issuance Templates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. **Label**

   There is no customization for labels.

2. **Text Box** - The customizations fields for Text Box are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Place holder	Enter the temporary text displayed inside the text box before the user enters any value. It provides a hint or example of what the user should type in that field.
Validation	Select or enter the customRegEx. Validation defines the rules that the input must meet before it can be submitted.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

Note: If any one of the toggle buttons are enabled Hide Field, Read Only, or Set as mandatory, then the other two toggle buttons remain disabled.

3. **Text Area** - The customizations fields for Text Area are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

4. **Radio Button** - The customizations fields for Radio Button are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

5. **Checkbox** - The customizations fields for Checkbox are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

6. **Select Box** - The customizations fields for Select Box are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

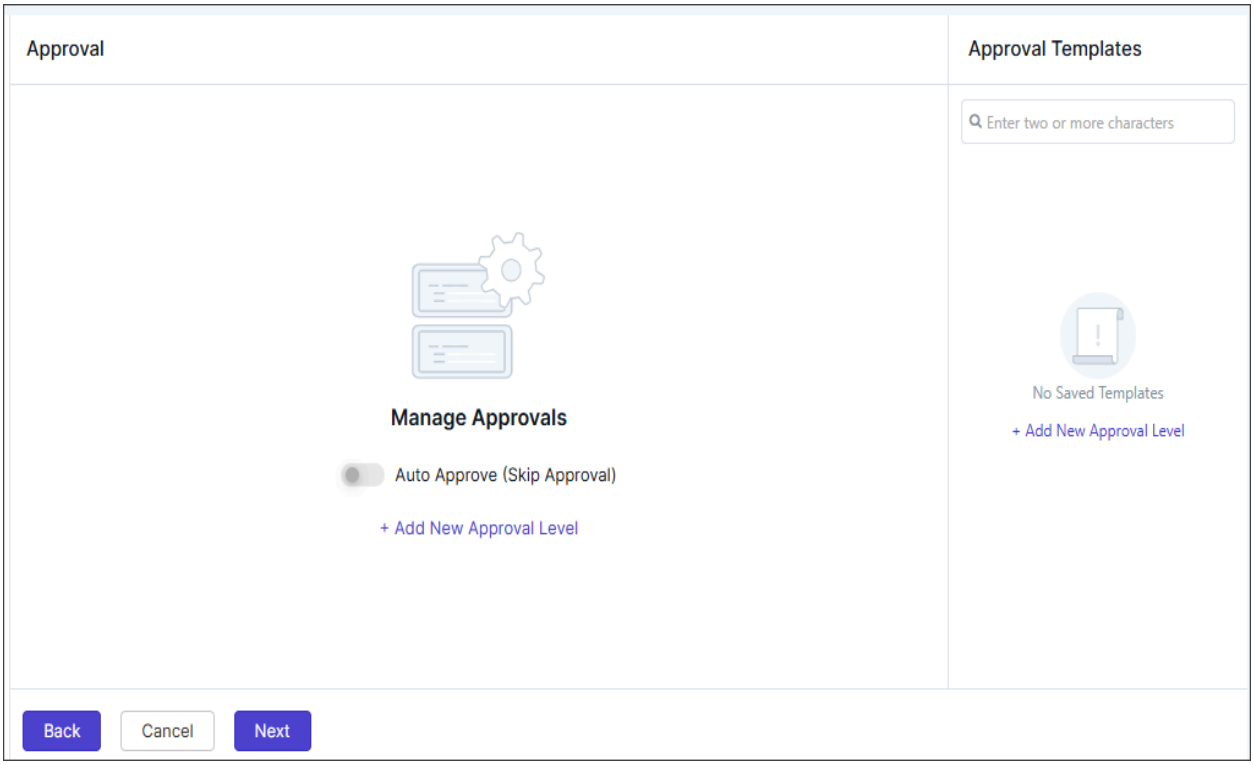
7. **Multi-select Box** - The customizations fields for Multi-select Box are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

Setting Approval

The Approval step allows you to manage the approval workflow before onboarding execution. You can choose to enable auto-approval or define approval levels, which can be configured as explained below.



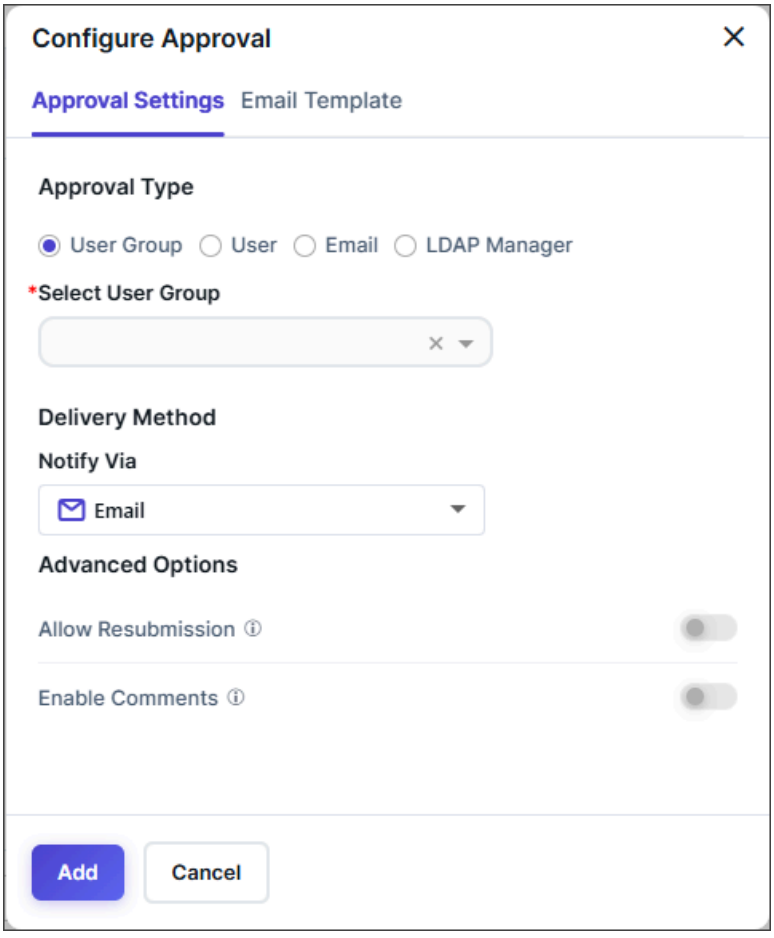
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Auto-Approval

1. Enable the **Auto Approve (Skip Approval)** toggle button.
2. Click **Next.**
   The fourth step, **Pre Issuance Task** page is displayed.

Adding New Approval Level

1. Click **+ Add New Approval Level**
   The **Configure Approval** pop-up is displayed with the **Approval Settings** tab (selected by default) and the **Email Template** tab.



2. From the **Approval Settings** tab, configure the Approval Settings based on the **Approval Type** radio button selection as described below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. If the **Approval Type** = **User Group**, enter/select the fields in the table below.

Field	Description
***Select User Group**	Select the User group(s) from the multi-select dropdown.
**: Mandatory field*	

b. If the **Approval Type** = **User**, enter/select the fields in the table below.

Field	Description
***Select User**	Select the User(s) from the multi-select dropdown.
**: Mandatory field*	

c. If the **Approval Type** = **Email**, enter/select the fields in the table below.

Field	Description
***Select Email**	Enter a valid email address. Use either comma-separated email IDs, or a single variable like ${template_email}.
**: Mandatory field*	

d. If the **Approval Type** = **LDAP Manager**, enter/select the fields in the table below. This option enables approval based on the manager information retrieved from the LDAP directory.

Field	Description
***Select LDAP Server**	Specifies which LDAP server to connect to for fetching user and manager details. Choose an existing LDAP server from the dropdown list or enter the connection URL manually.
***Customize LDAP Query** - Allows you to define or modify the LDAP query parameters used to identify the user and their manager. When enabled, additional fields appear to customize how LDAP attributes are queried.	
User Filter Attribute	Defines the LDAP attribute used to locate the requesting user
User Return Attribute	Specifies which LDAP attribute should be retrieved from the user's record to identify their manager.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Manager Filter Attribute	Defines the LDAP attribute used to locate the manager's record in LDAP.
Manager Return Attribute	Specifies which attribute value from the manager's record should be returned and used as the approver's identifier (For example: email address).
**: Mandatory field*	

e. In the **Delivery Method** section, select the values as follows:

Field	Description
Notify Via	The dropdown has the value **Email** selected by default.

f. In the **Advanced Options** section, select the values as follows:

Field	Description
Allow Resubmission	Enable the toggle button to allow resubmission of the policy request. The button is disabled by default.
Enable Comments	Enable the toggle button to allow approvers to add comments to the policy request. The button is disabled by default.
**: Mandatory field*	

3. From the **Email Template** tab, enter/select the information as follows:

Field	Description
Template Name	Choose an email template to customize approval notifications
Email Templates	Enable the toggle buttons to use any of the templates below: • Approval Request Template • Approval Confirmation Template • Approval Rejection Template

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

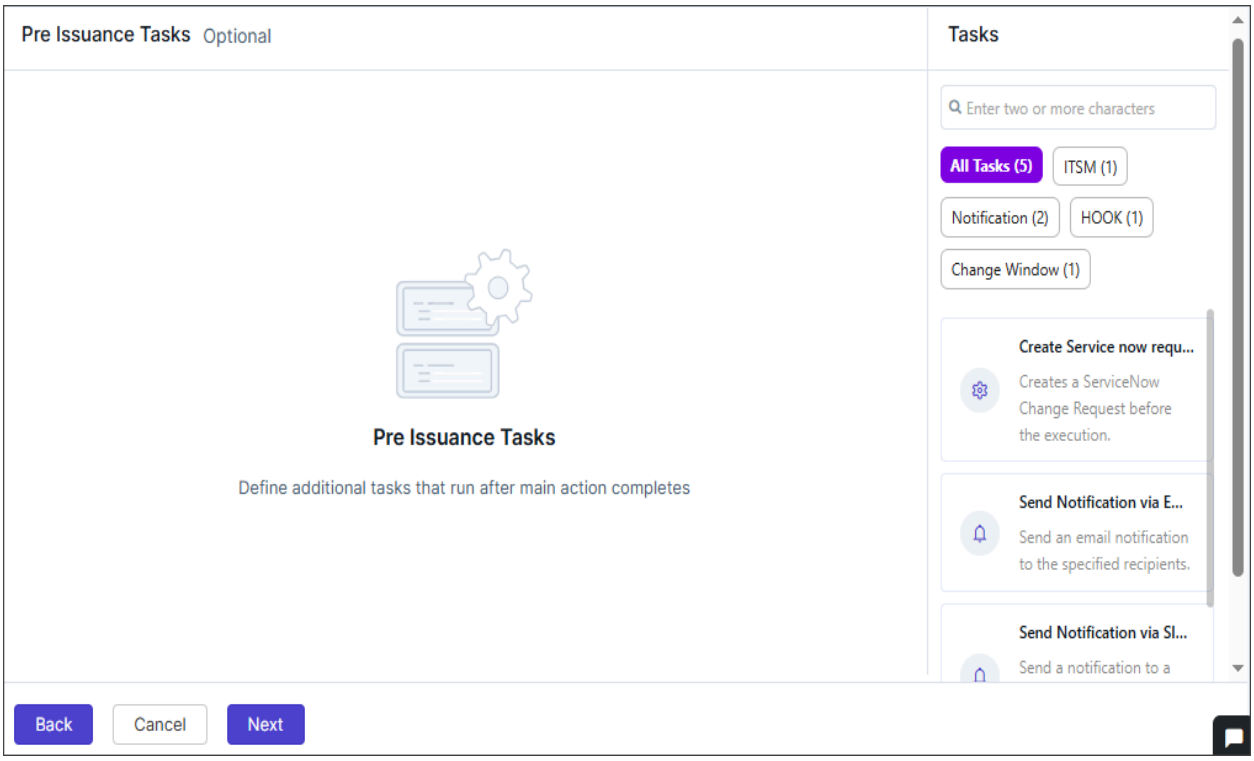
Field	Description
	To customize the email templates, a. Enable the toggle button of the respective email template b. Click the arrow icon next to the toggle button to expand/display the email contents. c. Edit the **Email Subject**, **CC** (Carbon Copy), and **Email Content**. **Note:** Users can copy predefined variables (For example: ${user.firstName}, ${user.lastName}) from the  option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.
**: Mandatory field*	

4. Click **Add**.
   The Approval template is displayed with the Edit and Delete icons and the option to further Add New Approval levels.
5. Click the **Save Template** dropdown next to the **Approval** header, then select **Save as New** to create a new template and save this configuration as a reusable template for future use.
   The Save as Template pop-up is displayed.
6. Enter the **Template Name** and enter a template **Description.** (Template names can include alphanumeric and the - (dash), _ (underscore), and space special characters.)
7. Click **Save** on the pop-up.
   The Approval level template is saved successfully.
8. Click **Next**.
   The fourth step, the **Pre Issuance Task**page is displayed.

Configuring Pre Issuance Tasks

This is an optional fourth step that lets you configure tasks to execute before certificate issuance. A Task panel is available on the right with five tasks as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



1. **ITSM** - Create a ServiceNow Change Request before the execution.
2. **Notifications**
   a. **Send Notification via Email** - Send an email notification to the specified recipients.
   b. **Send Notification via Slack** - Send a notification to a Slack channel using the configured webhook URL.
3. **Hook Execution** - Initiates the execution of the selected hook.
4. **Configure Change Window** - Allows users to configure a change window during which the policy tasks should be executed.

ITSM - Create a ServiceNow Change Request

Enter the following fields to configure the ServiceNow Change Request.

Field	Description
Configuration tab	
***Configuration tab* - ServiceNow Instance**	
Configure ServiceNow Instance	Select or configure the type of ServiceNow instance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Configuration tab* - Change Request Fields**	
Type	Defines the type of ServiceNow request to be created (For example: Normal, Emergency, Standard). Select the value from the dropdown.
Priority	Specifies the urgency level or importance of the change request. Select the value from the dropdown (1-Critical, 2-High, 3-Moderate, 4-Low).
Short Description	A brief summary or title describing the purpose of the change request.
Description	A detailed explanation of the change request, including context or justification.
Category	Classifies the change under a specific functional or operational category.
Risk	Select the potential risk level associated with implementing the change. Select the value from the dropdown (VeryHigh, High, Moderate, Low, None).
Impact	Specifies the extent to which the change might affect users, services, or infrastructure. Select the value from the dropdown (1-High, 2-Medium, 3-Low).
Urgency	Reflects how quickly the change needs to be addressed or implemented. Select the value from the dropdown (1-High, 2-Medium, 3-Low).
Assignment Group	The ServiceNow group responsible for reviewing and implementing the change.
CAB Required	Specifies whether the change requires approval from the Change Advisory Board (CAB). Select value **True** or **False**.
Wait for State Change	Determines whether AppViewX should pause workflow execution until the ServiceNow change request reaches a specific state. Select value **True** or **False**.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Notifications - Send Notification via Email

Enter the following fields to set up notifications for Email or Slack.

Field	Description
Configuration tab	
***Recipient Type**	Select either or all of the following: • User Group • User • Email
***User Group**	This field is enabled when **Recipient Type = User Group**. Select single or multiple user groups.
***User**	This field is enabled when **Recipient Type = User** Select single or multiple users.
***Email**	This field is enabled when **Recipient Type = Email.** Enter a valid email address. Use either comma-separated email IDs, or a single variable like **${template_email}**.
***Template Name**	Select the email template name.
***Email Subject**	This field is enabled when **Notify Via = Email**. Enter the subject for the email. Use the **Variables** option to add database values as variables.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Notifications - Send Notification via Slack

Enter the following fields to set up notifications for Email or Slack.

Field	Description
Configuration tab	
***Slack Channel**	This field is enabled when **Notify Via = Slack**. Select the slack channel.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Hook Execution

Enter the following fields to configure the hooks.

Field	Description
Configuration tab	
***Configuration tab* - Hook** (Select a hook from the available inventory that you want to execute.)	
Task Name	Displays the default name of the task (*Hook Execution*). You can rename it if needed for clarity in the workflow.
Select Hook	Choose the specific hook (script or API integration) to be executed within the workflow.
***Configuration tab* - Expose Variables**	
Do you want to expose hook response as variables for following tasks?	Toggle this option to expose the hook's response as variables for use in subsequent workflow tasks. Enables or disables the ability to pass hook output values as input variables to later tasks in the workflow.
Output Variable Mapping	Map output variables from the hook response to custom keys for easier reference in subsequent tasks. Paste the expected JSON response from the hook to view and select available variables. **Fields:** • **Variable Key:** Enter a custom key name for the variable. • **Output Variable:** Select the output variable path from the JSON response (options include `$.output`, `$.path`, `$.type`). To add variables, click  button.
Expected Response Format	Paste a sample JSON response from the hook in the `output {}` section. This helps AppViewX identify available response parameters for variable mapping and validation.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Configuring Change Window

This page allows users to define a specific **change window** a scheduled timeframe during which policy-related tasks can be executed.

Field	Description
Configuration tab	
Change Window Configuration	Configure when policy changes are allowed to run. Use the **Preview Windows** option to visualize the scheduled change windows based on the selected configuration.
***Mode Selection**	Choose the frequency or recurrence pattern for the change window. The options available are as follows: • **Daily:** Executes policy tasks during the defined window each day. • **Weekly:** Executes tasks on specific days of the week. • **Monthly:** Executes tasks on specified dates or weeks within a month. • **User Defined:** Allows users to define a custom schedule or window duration.
Daily Schedule Settings	This section is enabled when **Mode Selection = Daily**. Enter the values in the following fields: • ***Start Time** (HH:MM) • ***End Time** (HH:MM)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Weekly Schedule Settings	This section is enabled when **Mode Selection = Weekly**. Enter the values in the following fields: • ***Day of the Week** - (select Monday, Tuesday etc.) • **End Day of Week** (Optional) (select Monday, Tuesday etc.) • ***Start Time** (HH:MM) • ***End Time** (HH:MM)
Monthly Schedule Settings	This section is enabled when **Mode Selection = Monthly**. Enter the values in the following fields: • ***Day of the Month** - (select date between 1-31) • **End Day of Month** (Optional) (select date between 1-31) • ***Start Time** (HH:MM) • ***End Time** (HH:MM)
Custom Date & Time	This section is enabled when **Mode Selection = User Defined**. Enter the values in the following fields: • ***Explicit Start Time** (YYYY-MM-DDTHH:MM:SSZ) • ***Explicit End Time** (YYYY-MM-DDTHH:MM:SSZ)
***Missed Window Policy**	Determines the system behavior if a task misses its scheduled change window. Options include: • **Run Next Window:** The task will automatically run during the next available window. • **Skip:** The missed task will be skipped without execution. • **Fail Immediately:** The task will fail immediately if it cannot execute within the defined window.
Allow Override	Enables authorized users or groups to allow execution outside the defined change window.
Override Type	This field is enabled when **Allow Override** toggle is enabled. Select from **User Group** or **User**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
User Group	This field is enabled when **Allow Override** toggle is enabled and **Override Type = User Group** Select **User Group** from the dropdown.
User	This field is enabled when **Allow Override** toggle is enabled and **Override Type = User** Select **User** from the dropdown.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

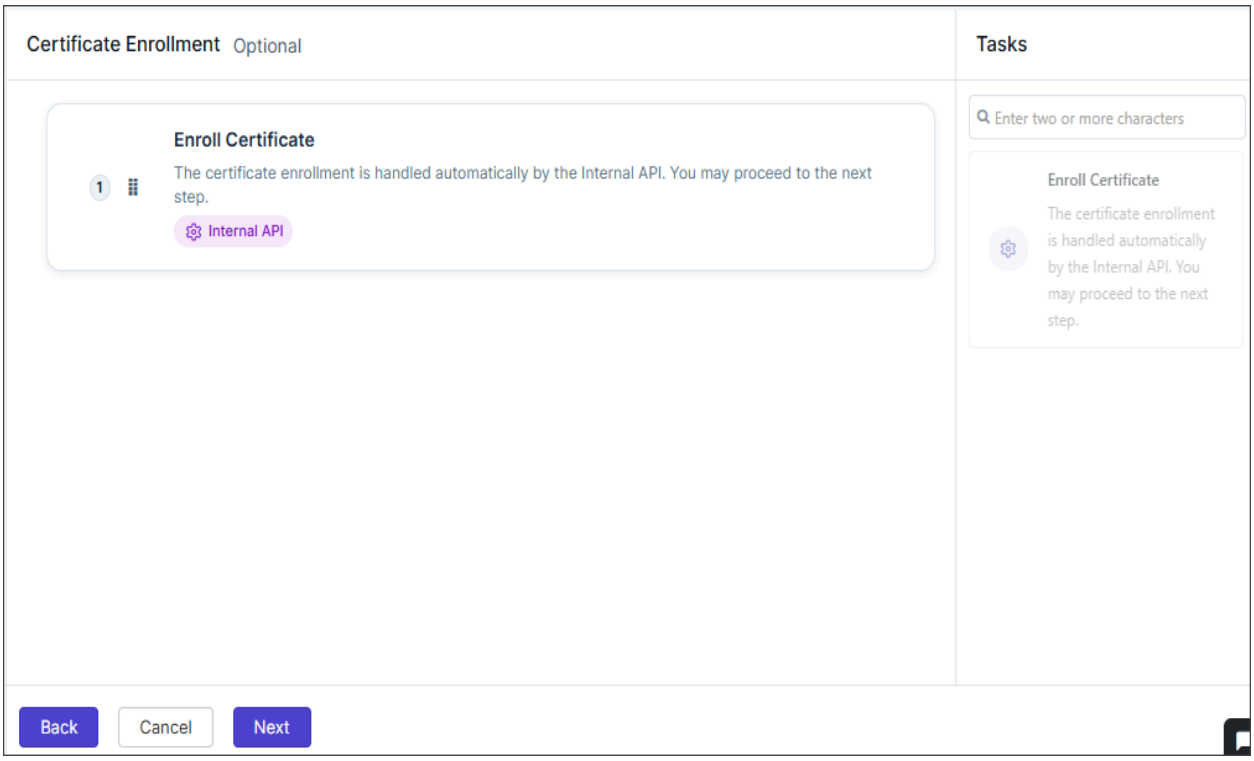
Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Certificate Enrollment

This is an optional fifth step where the certificate enrollment is handled automatically by the Internal API. You may proceed to the next step. There are no actions required on this page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

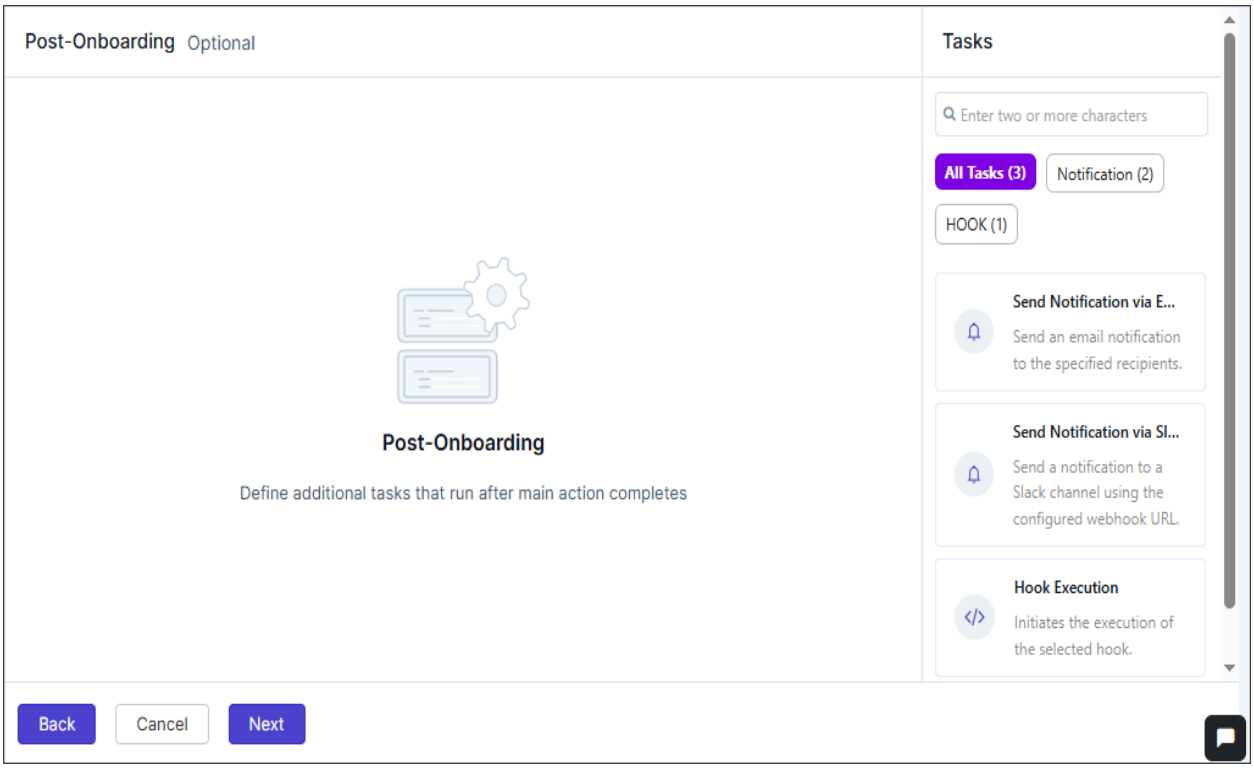


• Click the **Next** button to move to the next step, **Post-Onboarding**.

Configuring Post Issuance Settings

The sixth step in the enroll certificate process is to configure tasks to execute after certificate issuance. These are additional tasks that run after the main action completes. The Task panel on the right has the following tasks to be configured:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



1. Send Notifications via Email (For details, click here)
2. Send Notifications via Slack (For details, click here)
3. Email certificates in zip format (see section below)
4. Hook Execution (For details, click here)

Email Certificates in Zip Format

This task is used to configure an email containing the certificates packaged in a ZIP file to be sent to the requester.

Field	Description
Configuration tab	
***Certificate Type**	Select any of the following certificate types: • PEM (*.crt) • PEM (*.cer) • DER (*.crt) • DER (*.cer) • PKCS#7 Binary (*.p7b) • PKCS#7 PEM (*.p7b)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• PKCS#12 (*.p12) • PKCS#12 (*.pfx) • JKS (*.jks)
Include Root and Intermediate	This checkbox is enabled only for the following certificate types. • PEM (*.crt) • PEM (*.cer) • DER (*.der) If the checkbox is selected, the certificate chain will be included and sent via email.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

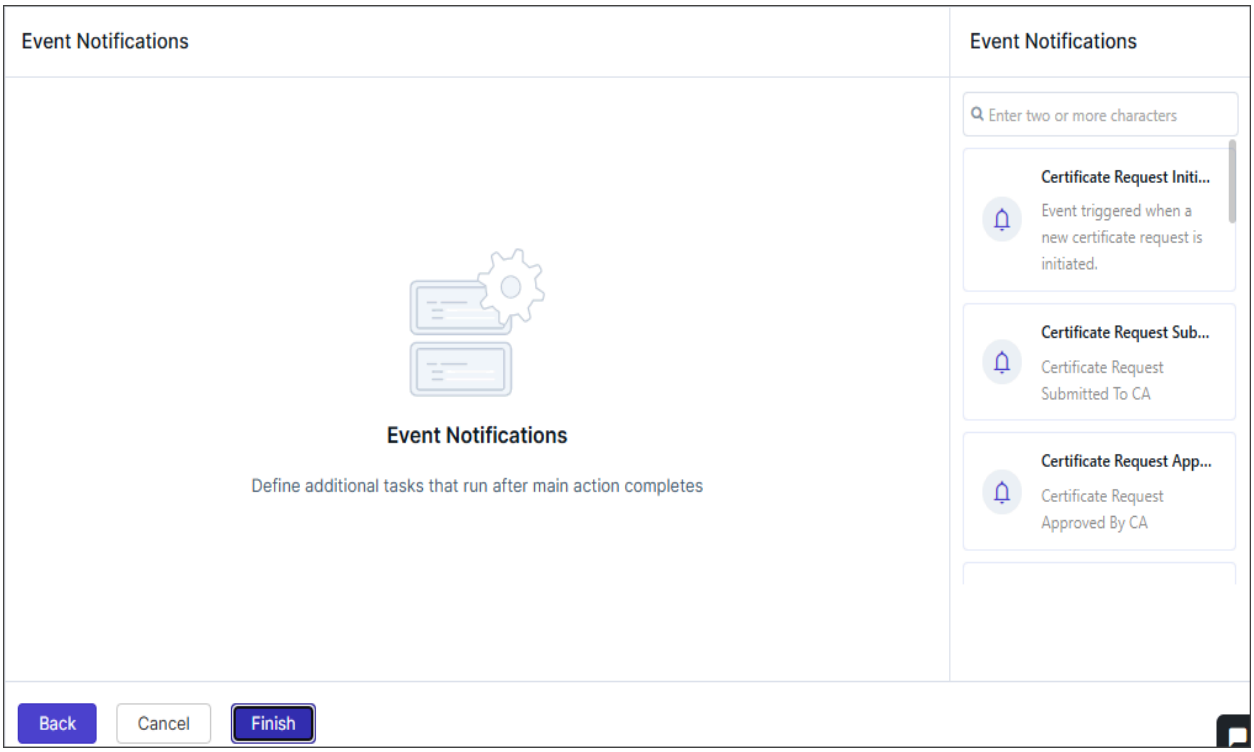
Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Configuring Event Notifications

The final step in the enroll certificate process is to send email notifications to users, groups, or external recipients on certificate enrollment lifecycle events.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



1. Certificate Request Initiated (Event triggered when a new certificate request is initiated.)
2. Certificate Request Submitted To CA (
3. Certificate Request Approved By CA

To configure any of the above emails,

1. From the notification panel on the right, click any of the specific emails to be configured. The <email_name> pop-up is displayed.
   The <email_name> pop-up is displayed.

   Note: All the email templates have the same fields, see to the table below to configure any of the emails.

2. Enter the following details in the email configuration pop-up.

Field	Description
***Notify Via**	Select from the following: • Email • Slack

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Recipient Type**	This field is enabled when **Notify Via = Email**. Select either or all of the following: • User Group • User • Email
***Slack Channel**	This field is enabled when **Notify Via = Slack**. Select the slack channel.
***User Group**	This field is enabled when **Notify Via = Email** and **Recipient Type = User Group**. Select single or multiple user groups.
***User**	This field is enabled when **Notify Via = Email** and **Recipient Type = User** Select single or multiple users.
***Email**	This field is enabled when **Notify Via = Email** and **Recipient Type = User Email.** Enter a valid email address. Use either comma-separated email IDs, or a single variable like **${template_email}**.
***Template Name**	This field is enabled when **Notify Via = Email**. Select the email template name.
***Email Subject**	This field is enabled when **Notify Via = Email**. Enter the subject for the email. Use the **Variables** option to add database values as variables.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.
**: Mandatory field*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

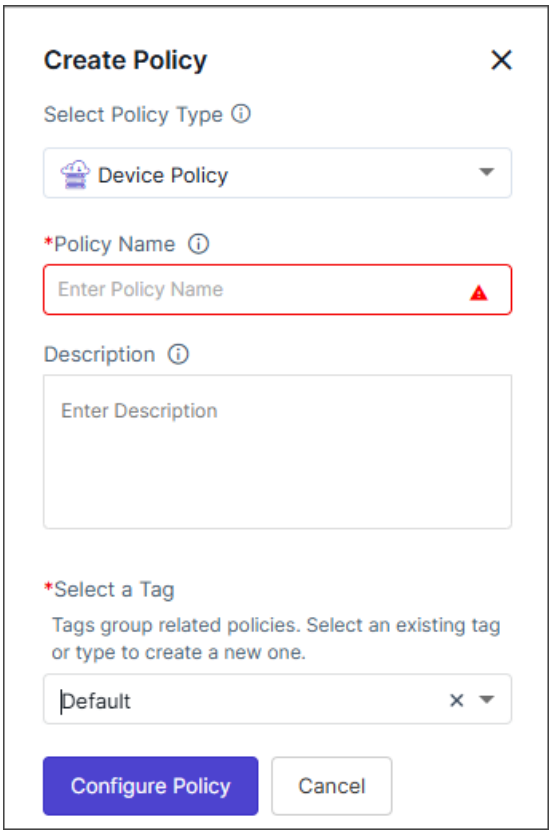
Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the Variables option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

3. Click **Add**.
   The email templates are created successfully.
4. Click **Finish** at the bottom of the screen to complete the enroll certificate policy creation.

Create Policy for Device Onboarding

To create a new device policy:

1. Go to **(Menu) > Policy Engine > POLICY MANAGEMENT > Policies**.
   The **Policy Inventory** page is displayed with all policies displayed for Kube, Certificate, and Device.
2. Click **(+Create Policy)**.
   The **Create Policy** pop-up is displayed.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

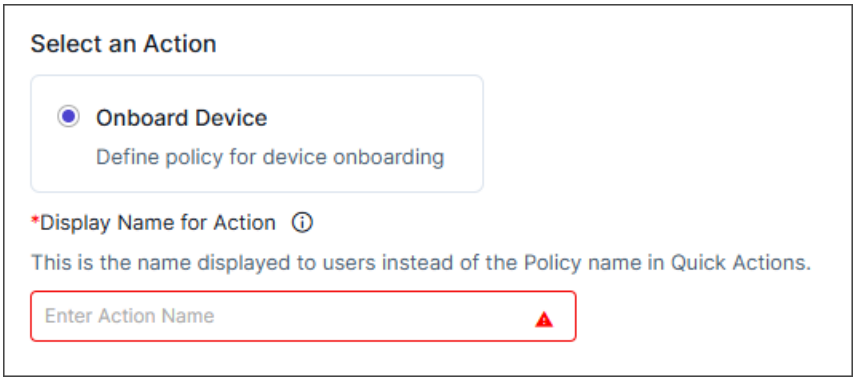
3. In the **Create Policy** pop-up, from the **Select the Policy Type** dropdown, select **Device Policy**.
   The fields for creating the device policy are displayed.
4. Enter/Select values for configuring the policy as described in the table below.

Field	Description
***Policy Name**	Enter a policy name that can include alphabets, numbers, and the special characters - (dash), _ (underscore).
Description	Enter a description for the policy.
***Select a Tag**	Select an existing tag or type to create a new one. Tags group the related policies. **Note:** Selecting the appropriate policy type allows you to group policies logically, simplifying organization and management based on specific criteria.
**: Mandatory field*	

5. Click **Configure Policy**.
   The **Create a Device Onboarding Policy in 7 Simple Steps** pop-up is displayed with a short description of each step.
6. Click **Close** on the pop-up.
   The first of the seven steps, **Action** is enabled.

Selecting Action

The Action step lets you select a specific action to trigger the policy.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Enter/select the values as described in the table below.

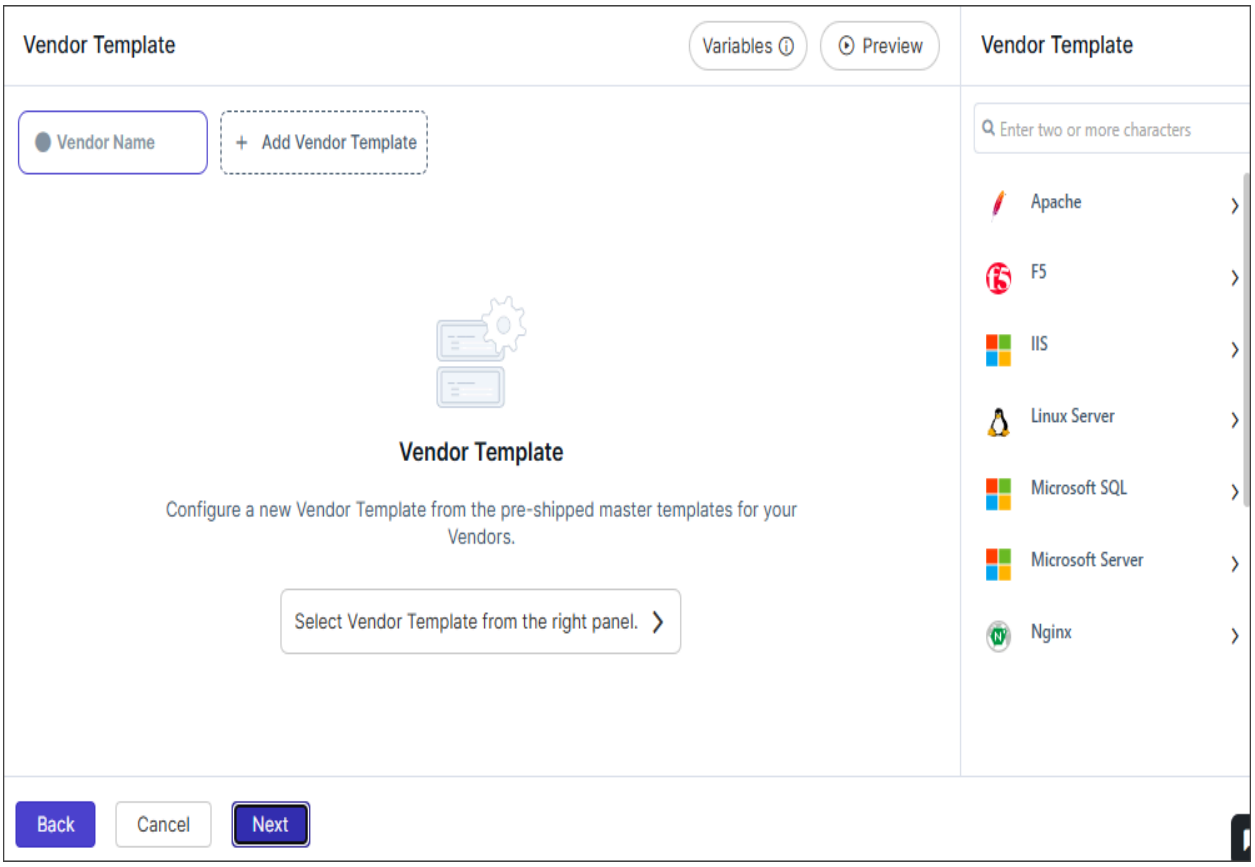
Field	Description
Select an Action	The **Onboard Device** option is selected by default (This is the policy for device onboarding)
***Display Name for Action**	Enter the action name that is to be displayed to users instead of the Policy name in Quick Actions. This field accepts alphanumeric values and special characters - (dash), _ (underscore), and space. Click the info icon to preview the Quick Actions.
**: Mandatory field*	

2. Click **Next**.
   The second step, the **Vendor Template** page is displayed.

Configuring Vendor Template

The Vendor Template step lets you configure default parameters for vendor-specific onboarding. A new Vendor Template can be configured from the pre-shipped master templates for your Vendors. Multiple templates can be added.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



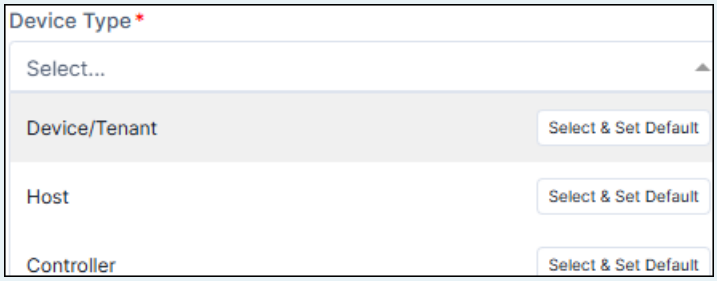
1. Select a **Vendor Template** from the right panel.
   A pre-shipped master template is displayed in the right panel.
2. Select the desired template.
   The blank template form is displayed. This page displays the vendor templates to configure default parameters for vendor-specific onboarding.

   Currently, the following vendors are supported:
   a. Linux Server
   b. Microsoft Server (MSServer, Exchange Service, Windows Gateway)
   c. IIS
   d. MS SQL
   e. F5 (ADC)
   f. Apache (Linux and Windows)
   g. Tomcat (Linux and Windows)
   h. Nginx (Server)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- While entering values for multi-select fields, it is mandatory to make any one of the values as default, by clicking the **Select & Set Default** button next to the value. See the image below.



- Each field type text-box, multi-select, dropdown, checkbox and others can be customized by selecting the **(settings)** icon next to the field. See to the section Field Customizations for more details

3. Enter field information for the vendors as described here.
4. [*Optional*] Click + Add Custom Field button to include additional custom fields.
   The **Add Custom Field** pop-up is displayed.
5. Enter/Select the values in the **Add Custom Field** pop-up as described in the table below.

Field	Description
Include this Custom Field as a Device Attribute	Enable or disable the toggle button to include or exclude the custom field as a device attribute.
Store this field value in an encrypted format	Enable or disable the toggle button to store the field value in an encrypted or non-encrypted format.
***Field Name**	Provide a field name for the custom field in alphanumeric format.
***Field Type**	Select a field type for the custom field. The available types are: • Label • Text Box • Text Area • Radio Button • Checkbox

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• Select Box • Multi-select Box
Field Value	Specify a default value for the field. The value can be modified according to the field type. For fields that accept multiple entries, use a comma-separated format.
**: Mandatory field*	

6. Click the **Add** button in the **Add Custom Field** pop-up to enable the value in the Vendor Template form.

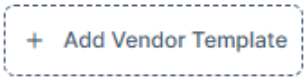
> **Note:** After adding custom fields, a (Settings) icon will appear to customize the field type, and a (Delete) icon will be available to remove the field from the form.

7. Click 

(**Preview**) to view the form information.

> **Note:** Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option, next to Preview. Variables can be inserted into text content and at runtime, they are replaced with actual values.

8. Click the **Save Template** dropdown next to the **Vendor Template** header, then select **Save as New** to create a new template and save this configuration as a reusable template for future use.
   The **Save as Template** pop-up is displayed.
9. Enter the **Template Name** and enter a template **Description.** (Template names can include alphanumeric and the - (dash), _ (underscore), and space special characters.)
10. Click **Save** on the pop-up.
    The Vendor template is saved successfully.
11. [*Optional*] Add another template, if required. Click 

and follow the steps above.
12. Click **Next**.
    The third step, the **Approval** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Customizations for Vendor Templates

1. **Label**

   There is no customization for labels.

2. **Text Box** - The customizations fields for Text Box are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Place holder	Enter the temporary text displayed inside the text box before the user enters any value. It provides a hint or example of what the user should type in that field.
Validation	Select or enter the customRegEx. Validation defines the rules that the input must meet before it can be submitted.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

Note: If any one of the toggle buttons are enabled Hide Field, Read Only, or Set as mandatory, then the other two toggle buttons remain disabled.

3. **Text Area** - The customizations fields for Text Area are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

4. **Radio Button** - The customizations fields for Radio Button are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

5. **Checkbox** - The customizations fields for Checkbox are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

6. **Select Box** - The customizations fields for Select Box are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

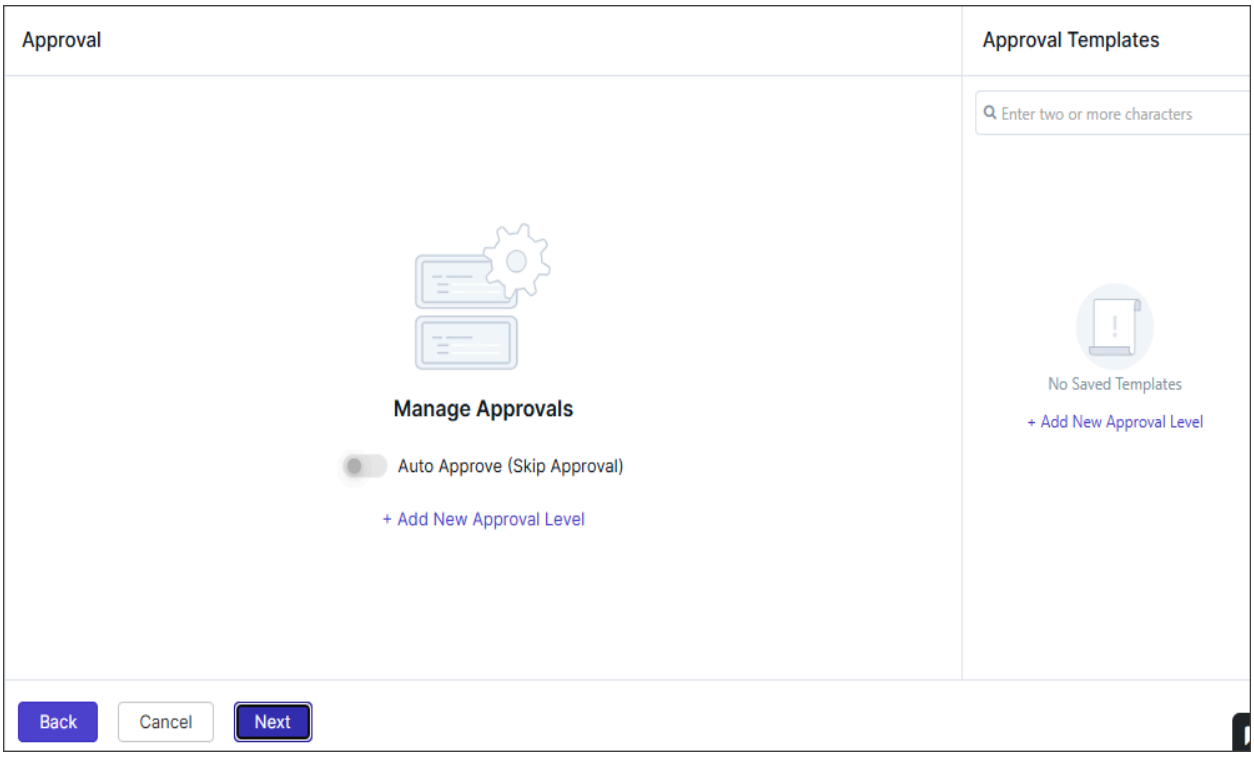
7. **Multi-select Box** - The customizations fields for Multi-select Box are as follows:

Field	Description
Hide Field	Enable the toggle button to hide the field in the form.
Read Only	Enable the toggle button to make the field a read-only (non-editable) one.
Set as mandatory	Enable the toggle button to make the field mandatory.
Label name	Enter a name for the field that will appear on the form.
Help Tooltip	Enter the informational message that appears when the user hovers over or clicks on the information icon next to the field.

Setting Approval

The Approval step allows you to manage the approval workflow before onboarding execution. You can choose to enable auto-approval or define approval levels, which can be configured as explained below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



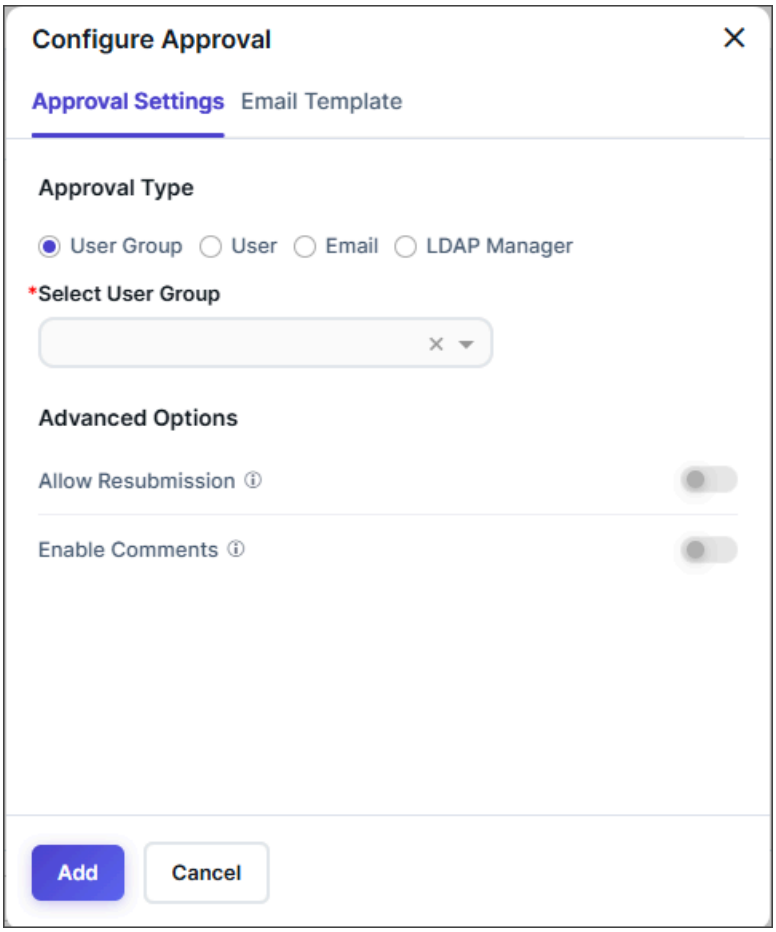
Auto-Approval

1. Enable the **Auto Approve (Skip Approval)** toggle button.
2. Click **Next.**
   The fourth step, **Pre-onboarding** page is displayed.

Adding New Approval Level

1. Click **+ Add New Approval Level**
   The **Configure Approval** pop-up is displayed with the **Approval Settings** tab (selected by default) and the **Email Template** tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



2. From the **Approval Settings** tab, configure the Approval Settings based on the **Approval Type** radio button selection as described below.

   a. If the **Approval Type** = **User Group**, enter/select the fields in the table below.

Field	Description
***Select User Group**	Select the User group(s) from the multi-select dropdown.
**: Mandatory field*	

   b. If the **Approval Type** = **User**, enter/select the fields in the table below.

Field	Description
***Select User**	Select the User(s) from the multi-select dropdown.
**: Mandatory field*	

   c. If the **Approval Type** = **Email**, enter/select the fields in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Select Email**	Enter a valid email address. Use either comma-separated email IDs, or a single variable like ${template_email}.
**: Mandatory field*	

d. If the **Approval Type** = **LDAP Manager**, enter/select the fields in the table below. This option enables approval based on the manager information retrieved from the LDAP directory.

Field	Description
***Select LDAP Server**	Specifies which LDAP server to connect to for fetching user and manager details. Choose an existing LDAP server from the dropdown list or enter the connection URL manually.
***Customize LDAP Query** - Allows you to define or modify the LDAP query parameters used to identify the user and their manager. When enabled, additional fields appear to customize how LDAP attributes are queried.	
User Filter Attribute	Defines the LDAP attribute used to locate the requesting user
User Return Attribute	Specifies which LDAP attribute should be retrieved from the user's record to identify their manager.
Manager Filter Attribute	Defines the LDAP attribute used to locate the manager's record in LDAP.
Manager Return Attribute	Specifies which attribute value from the manager's record should be returned and used as the approver's identifier (For example: email address).
**: Mandatory field*	

e. In the **Advanced Options** section, select the values as follows:

Field	Description
Allow Resubmission	Enable the toggle button to allow resubmission of the policy request. The button is disabled by default.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Enable Comments	Enable the toggle button to allow approvers to add comments to the policy request. The button is disabled by default.
**: Mandatory field*	

3. From the **Email Template** tab, enter/select the information as follows:

Field	Description
Template Name	Choose an email template to customize approval notifications
Email Templates	Enable the toggle buttons to use any of the templates below: • Approval Request Template • Approval Confirmation Template • Approval Rejection Template To customize the email templates, a. Enable the toggle button of the respective email template b. Click the arrow icon next to the toggle button to expand/display the email contents. c. Edit the **Email Subject**, **CC** (Carbon Copy), and **Email Content**. **Note:** Users can copy predefined variables (For example: ${user.firstName}, ${user.lastName}) from the  option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.
**: Mandatory field*	

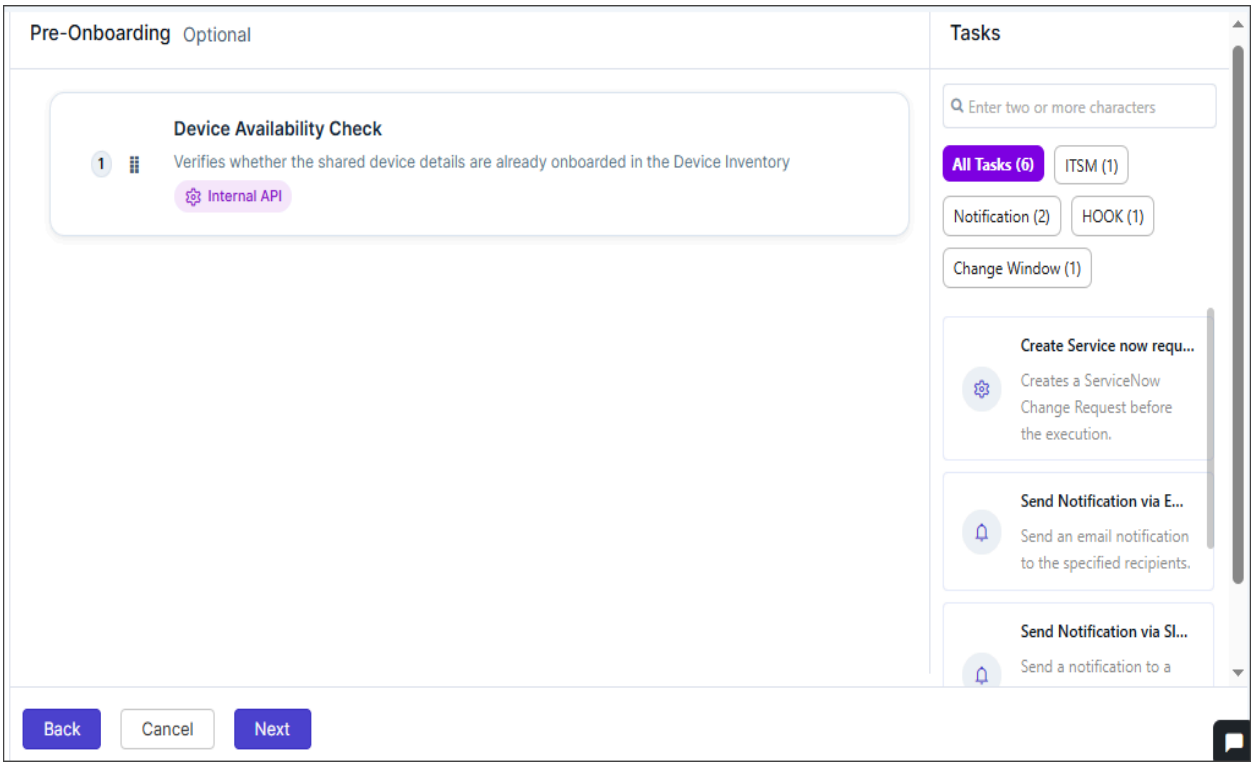
4. Click **Add**.
   The Approval template is displayed with the Edit and Delete icons and the option to further Add New Approval levels.
5. Click the **Save Template** dropdown next to the **Approval** header, then select **Save as New** to create a new template and save this configuration as a reusable template for future use.
   The Save as Template pop-up is displayed.
6. Enter the **Template Name** and enter a template **Description.** (Template names can include alphanumeric and the - (dash), _ (underscore), and space special characters.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Click **Save** on the pop-up.
   The Approval level template is saved successfully.
8. Click **Next**.
   The fourth step, the **Pre-Onboarding** page is displayed.

Configuring Pre-Onboarding Tasks

This is an optional fifth step that lets you execute scripts from the library before onboarding begins. A Task panel is available on the right with six tasks as follows:



1. **Device Availability Check** - Verifies whether the shared device details are already onboarded in the Device Inventory
2. **ITSM** - Create a ServiceNow Change Request before the execution.
3. **Notifications**
   a. **Send Notification via Email** - Send an email notification to the specified recipients.
   b. **Send Notification via Slack** - Send a notification to a Slack channel using the configured webhook URL.
4. **Hook Execution** - Initiates the execution of the selected hook.
5. **Configure Change Window** - Allows users to configure a change window during which the policy tasks should be executed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To proceed with the pre-onboarding,

1. Click **Device Availability Check** to check if the IP address of the device being onboarded is available with the vendor or not, else onboarding will fail. (This option is selected by default).
2. [*Optional*] Define additional tasks that run after the main action completes by clicking any of the tasks appearing on the right panel.
   Each task will have a separate configuration pop-up to fill out the details. See the sections below for detailed steps.
3. [*Optional*] Complete the configurations for the required tasks and click **Confirm** on the respective pop-up.
4. Click **Next**.
   The fifth step, the **Device Onboarding** page is displayed.

ITSM - Create a ServiceNow Change Request

Enter the following fields to configure the ServiceNow Change Request.

Field	Description
Configuration tab	
***Configuration tab* - ServiceNow Instance**	
Configure ServiceNow Instance	Select or configure the type of ServiceNow instance.
***Configuration tab* - Change Request Fields**	
Type	Defines the type of ServiceNow request to be created (For example: Normal, Emergency, Standard). Select the value from the dropdown.
Priority	Specifies the urgency level or importance of the change request. Select the value from the dropdown (1-Critical, 2-High, 3-Moderate, 4-Low).
Short Description	A brief summary or title describing the purpose of the change request.
Description	A detailed explanation of the change request, including context or justification.
Category	Classifies the change under a specific functional or operational category.
Risk	Select the potential risk level associated with implementing the change. Select the value from the dropdown (VeryHigh, High, Moderate, Low, None).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Impact	Specifies the extent to which the change might affect users, services, or infrastructure. Select the value from the dropdown (1-High, 2-Medium, 3-Low).
Urgency	Reflects how quickly the change needs to be addressed or implemented. Select the value from the dropdown (1-High, 2-Medium, 3-Low).
Assignment Group	The ServiceNow group responsible for reviewing and implementing the change.
CAB Required	Specifies whether the change requires approval from the Change Advisory Board (CAB). Select value **True** or **False**.
Wait for State Change	Determines whether AppViewX should pause workflow execution until the ServiceNow change request reaches a specific state. Select value **True** or **False**.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Notifications - Send Notification via Email

Enter the following fields to set up notifications for Email or Slack.

Field	Description
Configuration tab	
***Recipient Type**	Select either or all of the following: • User Group • User • Email

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***User Group**	This field is enabled when **Recipient Type = User Group**. Select single or multiple user groups.
***User**	This field is enabled when **Recipient Type = User** Select single or multiple users.
***Email**	This field is enabled when **Recipient Type = Email.** Enter a valid email address. Use either comma-separated email IDs, or a single variable like **${template_email}**.
***Template Name**	Select the email template name.
***Email Subject**	This field is enabled when **Notify Via = Email**. Enter the subject for the email. Use the **Variables** option to add database values as variables.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Notifications - Send Notification via Slack

Enter the following fields to set up notifications for Email or Slack.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Configuration tab	
***Slack Channel**	This field is enabled when **Notify Via = Slack**. Select the slack channel.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Hook Execution

Enter the following fields to configure the hooks.

Field	Description
Configuration tab	
***Configuration tab* - Hook** (Select a hook from the available inventory that you want to execute.)	
Task Name	Displays the default name of the task (*Hook Execution*). You can rename it if needed for clarity in the workflow.
Select Hook	Choose the specific hook (script or API integration) to be executed within the workflow.
***Configuration tab* - Expose Variables**	
Do you want to expose hook response as variables for following tasks?	Toggle this option to expose the hook's response as variables for use in subsequent workflow tasks.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enables or disables the ability to pass hook output values as input variables to later tasks in the workflow.
Output Variable Mapping	Map output variables from the hook response to custom keys for easier reference in subsequent tasks. Paste the expected JSON response from the hook to view and select available variables. **Fields:** • **Variable Key:** Enter a custom key name for the variable. • **Output Variable:** Select the output variable path from the JSON response (options include `$.output`, `$.path`, `$.type`). To add variables, click  button.
Expected Response Format	Paste a sample JSON response from the hook in the `output {}` section. This helps AppViewX identify available response parameters for variable mapping and validation.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Configuring Change Window

This page allows users to define a specific **change window** a scheduled timeframe during which policy-related tasks can be executed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Configuration tab	
Change Window Configuration	Configure when policy changes are allowed to run. Use the **Preview Windows** option to visualize the scheduled change windows based on the selected configuration.
***Mode Selection**	Choose the frequency or recurrence pattern for the change window. The options available are as follows: • **Daily:** Executes policy tasks during the defined window each day. • **Weekly:** Executes tasks on specific days of the week. • **Monthly:** Executes tasks on specified dates or weeks within a month. • **User Defined:** Allows users to define a custom schedule or window duration.
Daily Schedule Settings	This section is enabled when **Mode Selection = Daily**. Enter the values in the following fields: • ***Start Time** (HH:MM) • ***End Time** (HH:MM)
Weekly Schedule Settings	This section is enabled when **Mode Selection = Weekly**. Enter the values in the following fields: • ***Day of the Week** - (select Monday, Tuesday etc.) • **End Day of Week** (Optional) (select Monday, Tuesday etc.) • ***Start Time** (HH:MM) • ***End Time** (HH:MM)
Monthly Schedule Settings	This section is enabled when **Mode Selection = Monthly**. Enter the values in the following fields: • ***Day of the Month** - (select date between 1-31) • **End Day of Month** (Optional) (select date between 1-31) • ***Start Time** (HH:MM) • ***End Time** (HH:MM)
Custom Date & Time	This section is enabled when **Mode Selection = User Defined**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

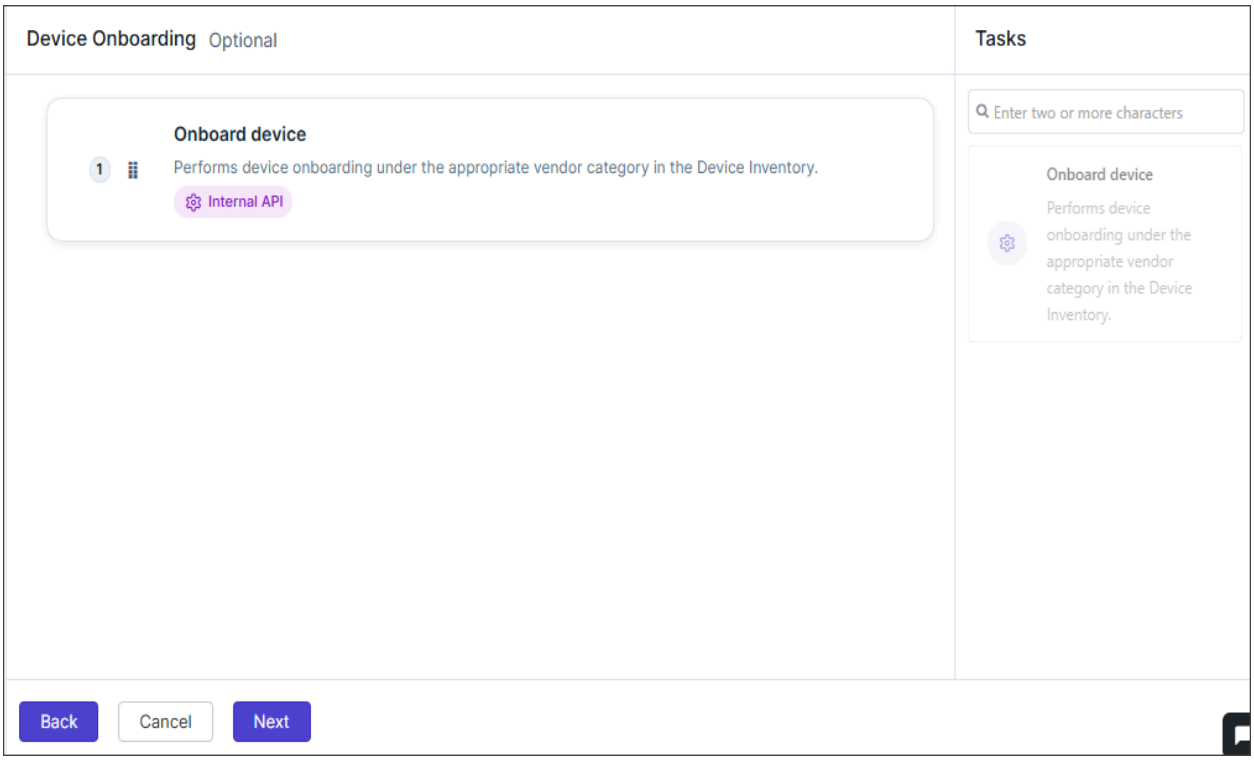
Field	Description
	Enter the values in the following fields: • ***Explicit Start Time** (YYYY-MM-DDTHH:MM:SSZ) • ***Explicit End Time** (YYYY-MM-DDTHH:MM:SSZ)
***Missed Window Policy**	Determines the system behavior if a task misses its scheduled change window. Options include: • **Run Next Window:** The task will automatically run during the next available window. • **Skip:** The missed task will be skipped without execution. • **Fail Immediately:** The task will fail immediately if it cannot execute within the defined window.
Allow Override	Enables authorized users or groups to allow execution outside the defined change window.
Override Type	This field is enabled when **Allow Override** toggle is enabled. Select from **User Group** or **User**.
User Group	This field is enabled when **Allow Override** toggle is enabled and **Override Type = User Group** Select **User Group** from the dropdown.
User	This field is enabled when **Allow Override** toggle is enabled and **Override Type = User** Select **User** from the dropdown.
General Settings tab (Configure general execution settings for this task)	
Continue On Failure	Determines whether the policy execution should complete even after the task fails. The toggle button is disabled by default.
**: Mandatory field*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the Variables option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

Onboarding Device

This is an optional fifth step that lets you perform the device onboarding under the appropriate vendor category in the Device Inventory, using an internal API. The device is added into AppViewX inventory via the immediate or scheduled methods. There are no actions required on this page.

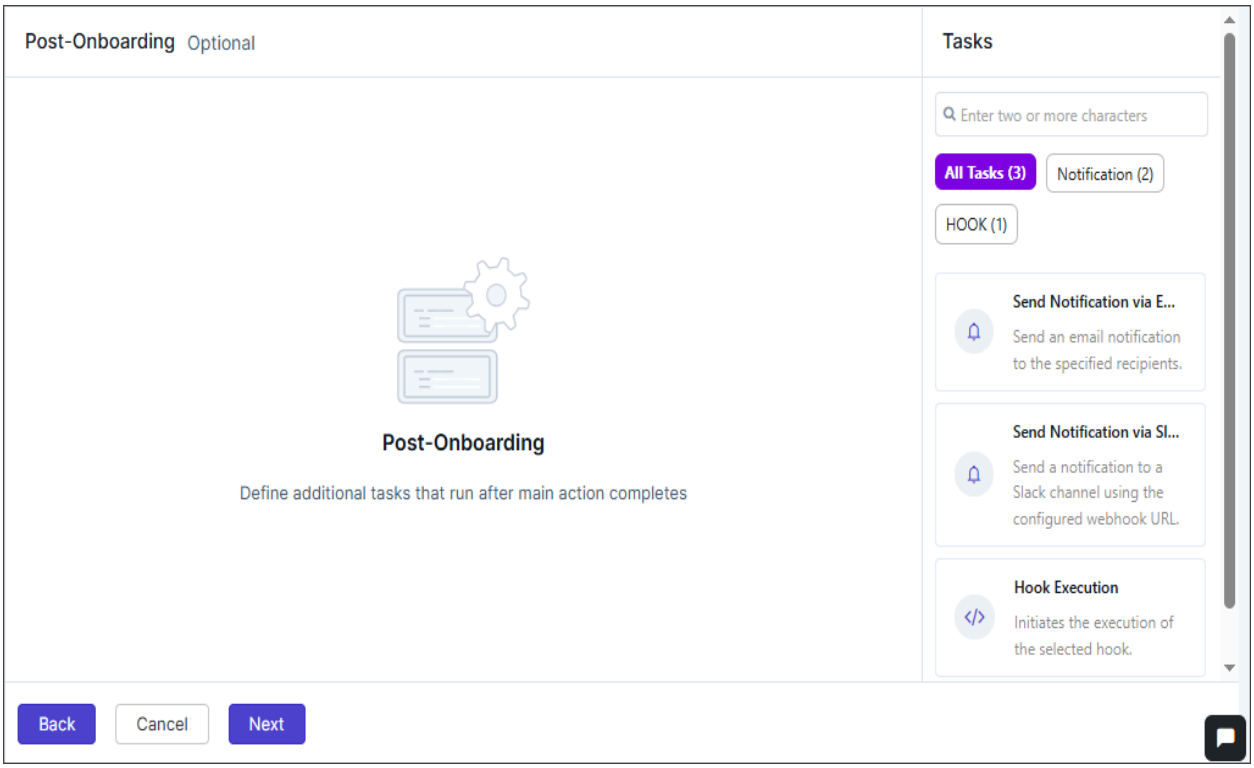


- Click the **Next** button to move to the next step, **Post-Onboarding**.

Configuring Post-Onboarding Tasks

This is an optional sixth step that execute scripts after onboarding completes (validation, reporting). These are additional tasks that run after main action completes. The Task panel on the right has the following tasks to be configured:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

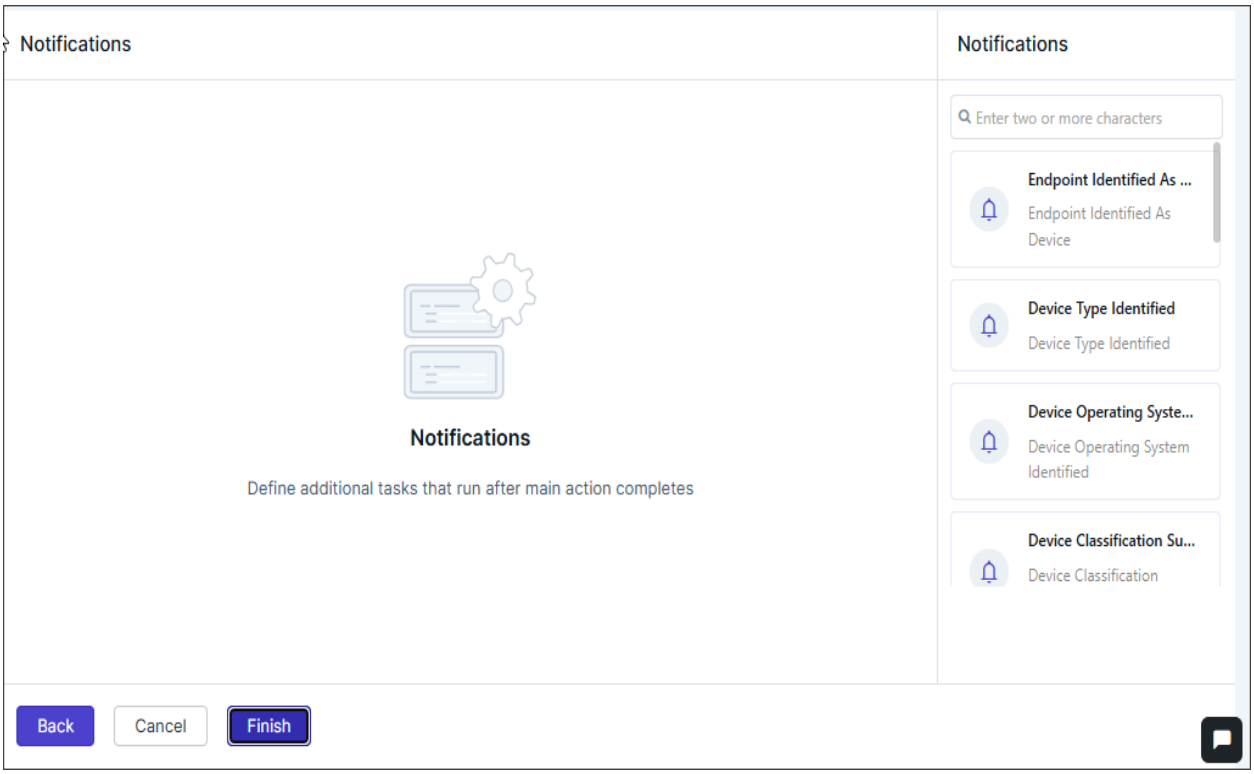


1. Send Notifications via Email (For details, click here)
2. Send Notifications via Slack (For details, click here)
3. Hook Execution (For details, click here)

Configuring Email Notifications

The final step in the Device Onboarding process is to send email notifications to users, groups, or external recipients. These are additional tasks that run after the main action completes. The Notification panel on the right has the following emails to be configured:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



1. Endpoint Identified As Device
2. Device Type Identified
3. Device Operating System Identified
4. Device Classification Success

To configure any of the above emails,

1. From the notification panel on the right, click any of the specific emails to be configured. The <email_name> pop-up is displayed.
   The <email_name> pop-up is displayed.

   Note: All the email templates have the same fields, see to the table below to configure any of the emails.

2. Enter the following details in the email configuration pop-up.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Notify Via**	Select from the following: • Email • Slack
***Recipient Type**	This field is enabled when **Notify Via = Email**. Select either or all of the following: • User Group • User • Email
***Slack Channel**	This field is enabled when **Notify Via = Slack**. Select the slack channel.
***User Group**	This field is enabled when **Notify Via = Email** and **Recipient Type = User Group**. Select single or multiple user groups.
***User**	This field is enabled when **Notify Via = Email** and **Recipient Type = User** Select single or multiple users.
***Email**	This field is enabled when **Notify Via = Email** and **Recipient Type = User Email.** Enter a valid email address. Use either comma-separated email IDs, or a single variable like **${template_email}**.
***Template Name**	This field is enabled when **Notify Via = Email**. Select the email template name.
***Email Subject**	This field is enabled when **Notify Via = Email**. Enter the subject for the email. Use the **Variables** option to add database values as variables.
***Message Content**	Enter the message content for the email or slack. Use the **Variables** option to add database values as variables.
**: Mandatory field*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Users can copy predefined variables (e.g., ${user.firstName}, ${user.lastName}) from the 

option on the top-right of the pop-up. Variables can be inserted into text content and at runtime, they are replaced with actual values.

3. Click **Add**.
   The email templates are created successfully.
4. Click **Finish** at the bottom of the screen to complete the device policy creation.

Creating a Cluster Policy Using Policy Engine

Use **Policy Engine** for a smarter, rule-based approach to policy creation. Predefined templates make it quick and easy to create and manage policies.

Prerequisites:

- Ensure CA integration is completed.
- Ensure you configured organization PKI standards as CA Policy.
- Ensure the Group is created.

To create a cluster policy:

1. Go to **(Menu) > KUBE+ > GROUPS & POLICIES > Cluster Policy**.
   On the **Cluster Policy** page, the existing policies (if any) are listed.
2. Click **+Create Policy** in the command bar.
   The **Cluster Policy** popup opens.
3. Under the **Policy Engine** section, click **+Create Policy**.
4. In the **Welcome to Policy Engine** popup, click **Get Started**.
5. In the **Create Policy** window:

   a. Select **Kube Cluster Policy** from the Policy Type dropdown.

   b. Fill in the policy details:

Policy Details - Field and Description Table

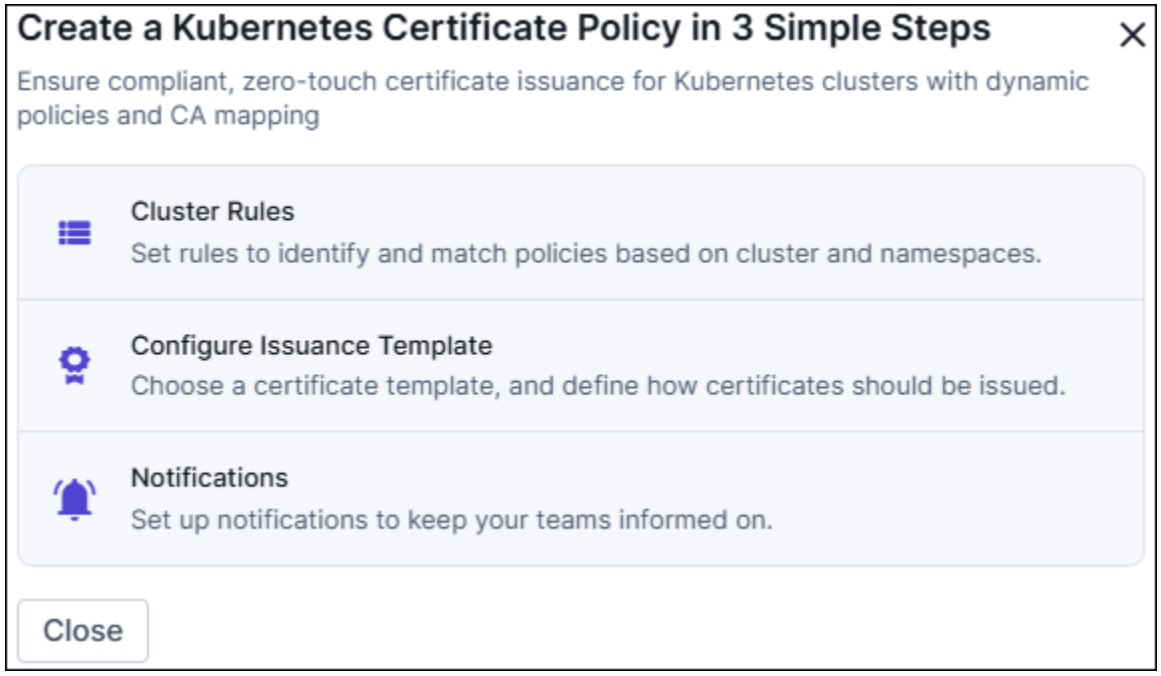
Field	Description
***Policy Name**	Enter a unique policy name to be associated with one or more clusters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Enter a policy name that can include lowercase alphanumeric and the special characters -.
Description	Optionally, provide a brief description of the policy for clarity and reference.
***Select a Tag**	Choose a tag to categorize and manage the policy.
**: Mandatory field*	

6. Click **Configure Policy**.

   The **Create a Kube Cluster Policy in 3 Simple Steps** popup displayed:



   - You may close it.
   - To avoid seeing it again, check **Don't Show Again**, then click **Close**.

7. Configuring the Policy as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. In the **Cluster Rules** page:
   - A default template is displayed. You can:
     - Use the existing template.
     - Modify and save it.
     - Save it as a new template.
   - Templates are listed under **Cluster Rule Templates** in the right panel.
   - Select a template to apply it to your rule.

b. The field in the **Cluster Rules** are:

Cluster Rules - Field and Description Table

Field	Description
Policy Application Scope	• **Cluster Wide** - Cluster wide global policy. • **Namespace Specific** - Policy to be applied for a specific namespace or a project within a cluster.
Policy Rules	Enable or disable the following rules as needed: • **Onboarding Rule** - Automatically map the policy by evaluating the configured rules when new clusters or namespaces are detected. If not enabled, the policy will not be mapped automatically but still can be mapped manually in KUBE+. • **Namespace Exclusion for Certificate Discovery** - Skip specified namespaces during the certificate discovery process. • **Off-boarding Rule** - Execute defined actions when clusters are removed from KUBE+.

8. Click **Next**.
9. In the **Issuance Template** page:
   - Select a certificate template from the right panel.
   - In the **Import Issuance Template** popup, click **Confirm**.
   - (Optional) Click **+ Add CA** to add more CAs, and fill in the required fields.
10. Click **Next**.
11. (Optional) Configure Notifications as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. On the **Notification (Optional)** page, click **+ Add Notification**.

b. In the **Configure Notification** panel, fill in the following:

Notification Settings Tab

Notification Settings - Field and Description Table

Field	Description
Recipient	Select recipients. The options are: • **User Group** - select this checkbox and add user groups from the dropdown list. • **User** - select this checkbox and add users from the dropdown list. • **Email** - enter the email address with comma separated.
Delivery Method	Select delivery methods. The options are: • ***Notify Via** - Bydefault Email option is selected. • **Notify Me** - Enable this toggle button to notify you when the policy is executed.

Message Template tab

Message Template - Field and Description Table

Field	Description
Email Template	Select a emal template from the dropdown list.
Email Subject	Enter the email subject. You can include variable to replace the value. To know about the variables, click Variables.
Email Content	Enter the email content for the bosy of the email. You can also use variables.

c. Click **Add**.

12. Click **Finish**.
13. In the **Submit Policy** confirmation popup, click **Confirm**.
    The cluster policy is added to the Cluster Policy inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

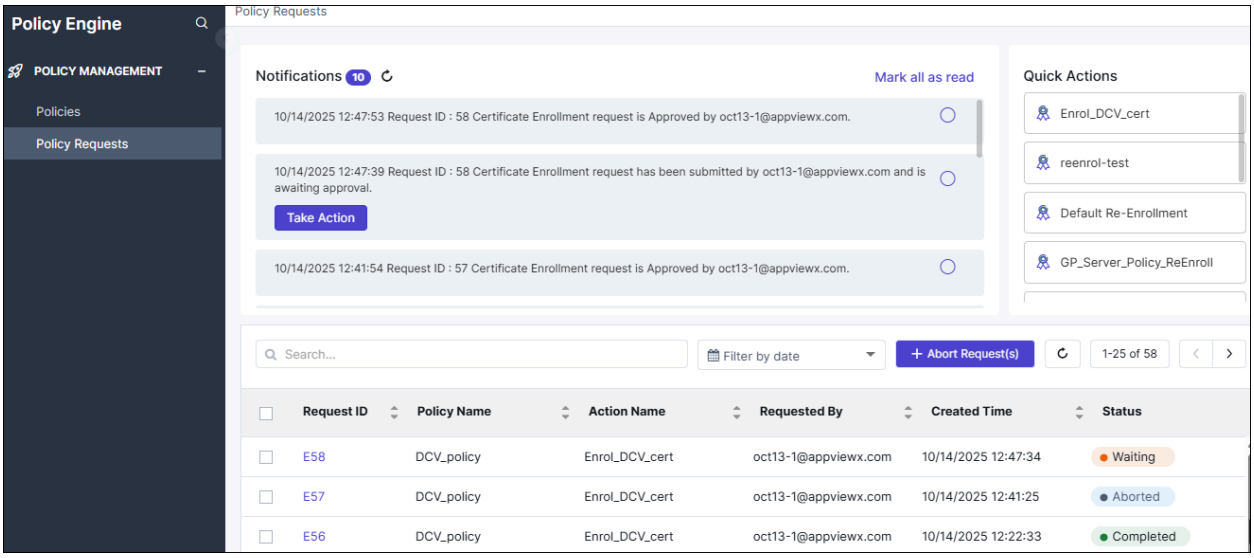
Related Information

- **Modifying Cluster Policy**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 5: Policy Requests

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

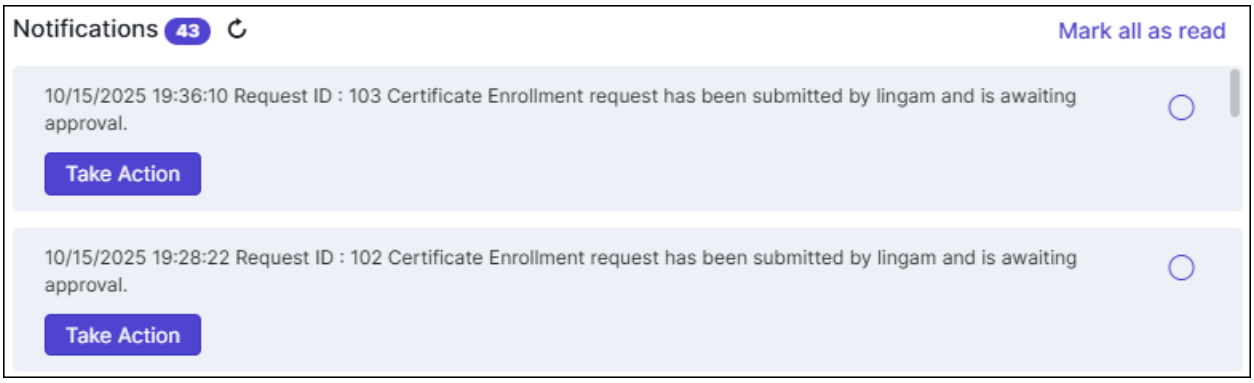


Notifications

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 Engine > POLICY MANAGEMENT > Policy Requests**.

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



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

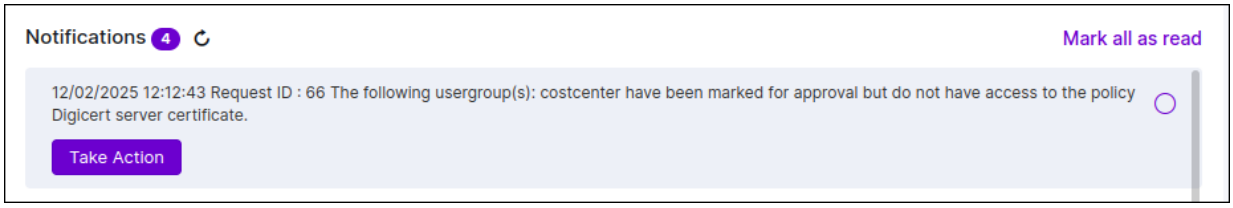
Understanding Notifications for User Roles

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**

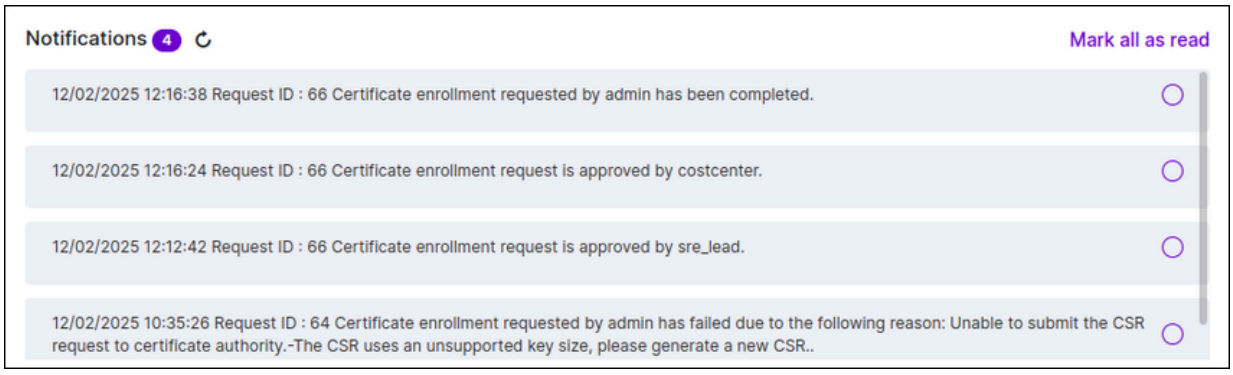
  Sent when the approver accepts/rejects the request.

- **Failure Notifcation**

  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.



Approver

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

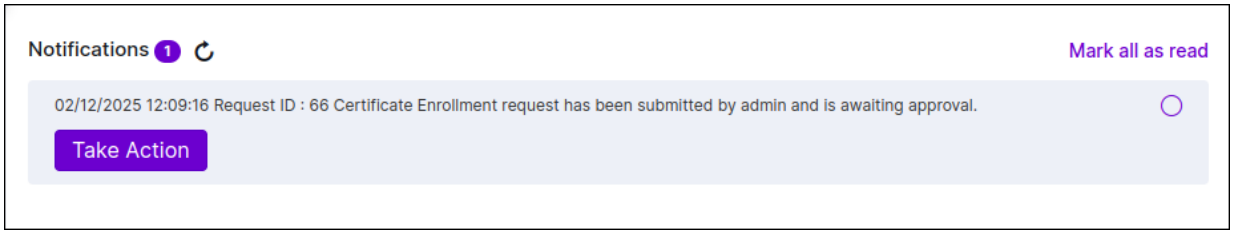
The approver will receive notifications for the following events:

- **Pending Approval Notification**

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

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

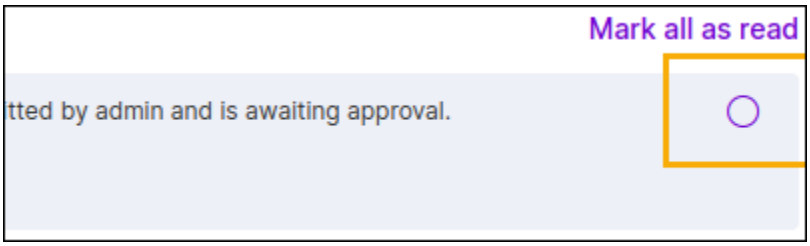
  You will be redirected to the request ID's timeline, where you can approve/reject the request.



Managing Notifications

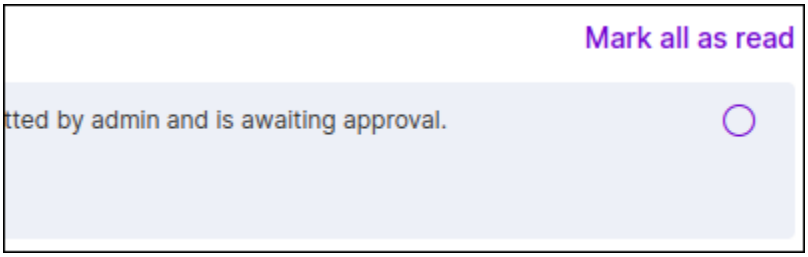
Marking individual notifications as read

To mark an individual notification as click ○ corresponding to the notification.



Marking all notifications as read

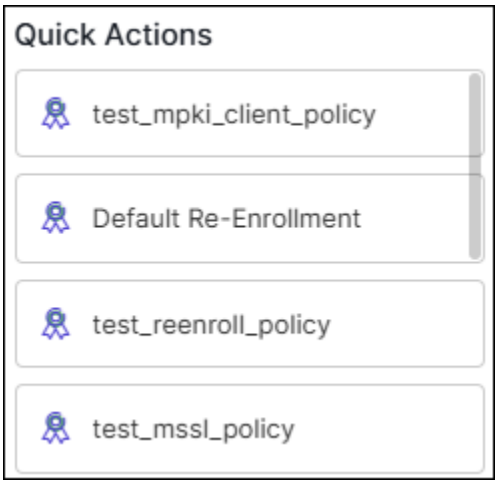
To mark all notifications as read, click **Mark all as read**.



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.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



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
In Progress	Policy execution is in progress.
Waiting	Policy execution is pending approval or is waiting for certificate issuance.
Rejected	Policy execution request has been rejected by the approver.
Failed	Policy execution has encountered a system error or a failure scenario.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status	Description
Aborted	Policy execution request has been aborted.
Completed	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.

- **Certificate Request Creation**

  The request proceeds to the Certificate Request Creation stage. This stage displays details such as the Common Name (CN) for which the certificate is being requested. An entry will be made in the Certificate inventory before approvals.

- **Enroll Certificate**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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.

- **Email Notification**

  Email Notification completed successfully.

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 Engine 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**

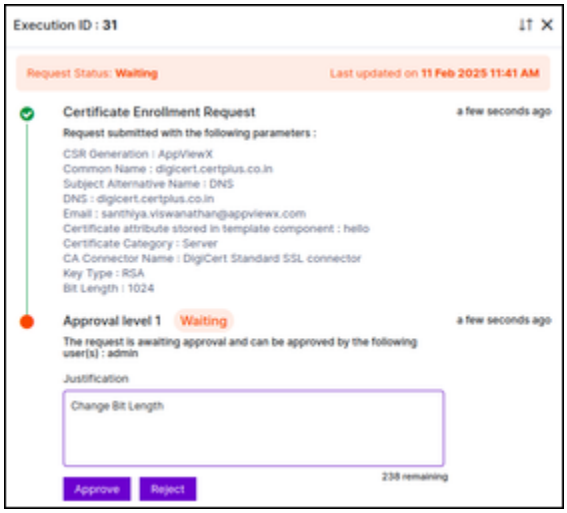
  If the **Notify user groups via email** post-action is configured, this stage sends an email notification to the selected user group(s), ensuring that relevant users are informed about the certificate issuance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Actions

- **Approve and reject**

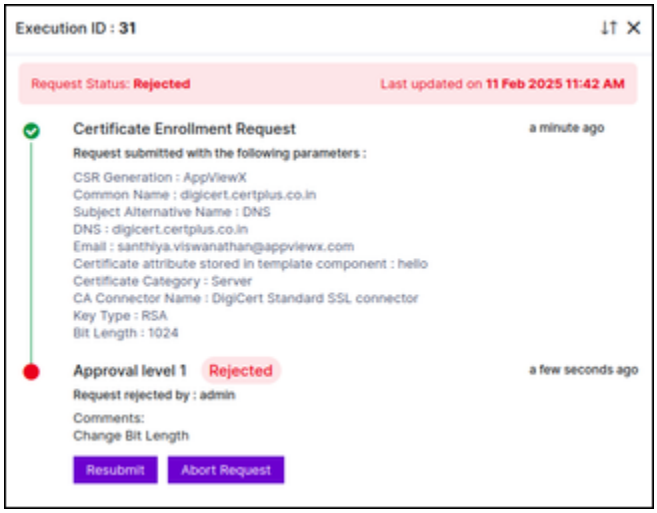
  Approvers with policy access can either approve or reject a request. If the **Allow Comments** option is enabled in the policy, approvers can provide comments explaining their decision. If the request contains incorrect details or does not meet the required criteria, the approver can reject it. However,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



- **Resubmit**

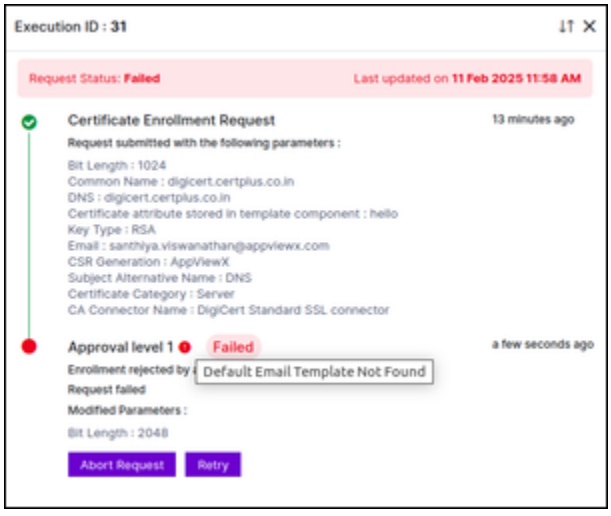
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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.



- **Abort**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If a policy request is no longer required, it can be aborted to prevent further processing. However, once the request reaches the implementation stage (For example: 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**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

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.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 6: FAQs

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

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

Copyright © 2025 AppViewX, Inc. All Rights Reserved.