



Policy groups

- [Feature history for policy groups, on page 1](#)
- [Policy groups, on page 2](#)
- [Add policy group, on page 4](#)
- [Policy group workflows, on page 6](#)
- [Objects and profiles, on page 8](#)
- [Policy validation for Cisco Catalyst SD-WAN, on page 11](#)
- [Troubleshooting policy group validations, on page 12](#)

Feature history for policy groups

Table 1: Feature history

Feature Name	Release Information	Description
Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature provides a simple, reusable, and structured approach for configuring policies in Cisco Catalyst SD-WAN. You can create a policy group, that is, a logical grouping of policies that is applied to one or more sites or devices at the site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. You can configure policies based on features that are required, recommended, or uniquely used, and then combine them to complete a policy configuration. The Deploy Policy Group workflow in Cisco Catalyst SD-WAN provides a guided method to select previously created policy groups and deploy them to sites or devices at the site that is managed by configuration groups.
Policy validation in Cisco SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1.1	This feature ensures network reliability and operational efficiency by automatically validating Cisco Catalyst SD-WAN policies for accuracy, platform compliance, and alignment with network requirements before deployment.

Feature Name	Release Information	Description
Device Tagging for Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1.1	With this feature you can add devices to a policy group configuration workflow using tags.

Policy groups

A policy group is a collection of policies and policy parameters that

- provides a simple, reusable, and structured approach for configuring policies and policy objects in Cisco IOS XE Catalyst SD-WAN devices
- allows you to configure basic and necessary policies with defaults to get your systems up and running through a simplified workflow, and
- can be associated with one or more sites or a single device at the site in the network and deployed on devices managed by configuration groups.

Policy group configuration options

Policy groups allow you to configure policies using different approaches:

- **Basic configuration:** Configure the basic and necessary policies with defaults through a simplified workflow
- **Advanced layout:** Switch to complete control and configure detailed policy parameters such as service-level agreement (SLA) class, Quality of Service (QoS) Maps, and Match-Action parameters pertaining to the traffic policy

After you've configured a policy group, you can deploy it on Cisco IOS XE Catalyst SD-WAN devices.

Policy group benefits

- Simplified user experience through an intuitive UI that allows you to quickly configure the basic policies that are required to get your Cisco Catalyst SD-WAN deployments up and running.
- Option to edit policy groups based on the changing needs of your network and save the configuration. You can choose to deploy these changes only when needed - during maintenance windows or in off-production hours.
- A **Preview CLI** option to preview the difference in configuration for relevant devices such as Cisco IOS XE Catalyst SD-WAN device and Cisco SD-WAN Controller in one location.
- Workflows to deploy policy groups.

Supported devices for policy groups

This feature is supported only on Cisco IOS XE Catalyst SD-WAN devices.

Configure prerequisites for policy groups

Before you begin

Before you begin configuring policy groups, ensure that these requirements are met:

- Minimum software version for Cisco IOS XE Catalyst SD-WAN devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Minimum software version for Cisco SD-WAN Manager: Cisco Catalyst SD-WAN Manager Release 20.12.1

- Ensure that these devices are deployed and managed using a configurations group. For more information about creating configuration groups, see [Configuration Groups and Feature Profiles](#).

Follow these steps to configure RBAC for policy groups and application priority policies:

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the Cisco SD-WAN Manager menu, choose Administration > Manage Users > User Groups .

Ensure that the granular role-based access control (RBAC) for policy groups is specified by expanding it. With specific permissions to the usergroup, ensure that you are able to access policy groups from Configuration > Policy Groups . |
| Step 2 | Click Add User Group . |
| Step 3 | Enter User Group Name . |
| Step 4 | Select the Read or Write check box against the Policy Group and Device feature that you want to assign to a user group. |
| Step 5 | Click Add . |
| Step 6 | From the Cisco SD-WAN Manager menu, choose Administration > Manage Users > User Groups .

Ensure that the granular RBAC for the application priority policy is specified by expanding it. With the set permissions to the usergroup, ensure that you are able to access the application priority policy from Configuration > Policy Groups . |
| Step 7 | Click Add User Group . |
| Step 8 | Enter User Group Name . |
| Step 9 | Select the Read or Write check box against these features that you want to assign to a user group: <ul style="list-style-type: none">• Feature Profile > Application Priority > Qos Policy• Feature Profile > Application Priority > Traffic Policy• Feature Profile > Policy Object > App List• Feature Profile > Policy Object > SLA Class• Feature Profile > Policy Object > TLOC• Feature Profile > Policy Object > App Probe |

- **Feature Profile > Policy Object > Preferred Color Group**
- **Feature Profile > Policy Object > Class**
- **Feature Profile > Policy Object > Data Prefix**
- **Feature Profile > Policy Object > Data Ipv6**
- **Feature Profile > Policy Object > Policer**

Step 10 Click **Add**.

Restrictions for policy groups

Policy groups have several restrictions that impact configuration and deployment capabilities:

- The Application Priority and SLA workflow does not support custom applications.
- Before deploying policy groups to devices, they must first be managed by a configuration group.
- The forwarding class in localized policy is not supported.
- An error occurs when a duplicate parcel name (for example, Site27-VPN1) exists in another configuration group. Verify existing parcel names across all groups and modify the intended name to ensure exclusivity. Use descriptive naming conventions to prevent conflicts.

Add policy group

Create a policy group that can be deployed to devices to manage application priority, security policies, and other network configurations.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > + Add Policy Group**.

Step 2 Enter a **Policy Group Name**, choose a **Solution** from the drop-down list and provide a description (optional).

Table 2: Policy group parameters

Field	Description
Policy Group Name	Specify the name of the policy group. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
Description	Provide a description for the policy group. It can contain up to 2048 characters including spaces.

Field	Description
Policy	
Application Priority & SLA	Choose an application priority for the policy group from the drop-down list. Click Create New to create a new application priority.
Embedded Security	Choose an embedded security policy from the drop-down list. Click Create New to create a new embedded security policy by selecting a configuration group, creating firewall policies, and other configuration settings.
Secure Internet Gateway	Configure the Secure Internet Gateway (SIG) tunnels before you apply a data policy for redirecting application traffic to an SIG. Select a Secure Internet Gateway (SIG) policy from the drop-down list. Click Create New to create a new SIG policy.
DNS Security	Select a DNS Security policy from the drop-down list. Click Create New to create a new DNS Security policy.

Step 3 Click **Create**.

Note

If you have already created a policy group, click the policy group from the list of available policy groups to edit.

Step 4 Click **Save** to save your configuration.

Step 5 Click the pencil icon to select or unselect devices to associate or dissociate with the policy group.

Note

Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, click **+Add** adjacent to **Associated** field to select or unselect devices to associate or dissociate with the policy group. In the associate devices workflow, you can choose devices based on **Regions** and not just **Sites**.

Step 6 Click **Deploy** to select sites and deploy the policy group.

The policy group is created and deployed to the selected devices. To delete a policy group, select the ellipsis icon (...) to the right of the policy group and click **Delete**.



Note

Dissociating policies from policy groups do not remove the policies from the device. If you intend to remove a policy or configuration from a device, then you need to remove the policy from the policy group and redeploy to that device so that the deployment ensures that the policy is removed from that device. You can move the device to a new empty policy group with no policy profiles to refresh the controller state and to remove stale entries. Until that is done, mere dissociation will not remove any policies from the device.

Policy group workflows

A policy group workflow is a configuration management feature that

- guides you in creating a policy group for one or more sites or a single device at the site in the network that is managed by configuration groups in Cisco Catalyst SD-WAN, and
- provides you with an improved configuration and troubleshooting experience.

Policy group workflow features

The workflow has the following features:

- allows you to review the various configuration values on a single page within the workflow, and
- helps you easily identify and fix incorrect values that appear highlighted in red.

Deploy policy group workflow

You can access the workflow by choosing **Workflows > Deploy Policy Group** menu in Cisco SD-WAN Manager.

The **Deploy Policy Group** workflow enables you to associate devices with a previously created policy group and deploy the policy group to the selected devices. You can review device configurations to further add Site IDs and other variables that must be provided as part of a policy group before deploying the policy group.

An asterisk that is adjacent to a field name helps you identify the mandatory values within the workflow.

After deploying a policy group, any subsequent changes to the policy group will cause the Cisco SD-WAN Controller to appear in the deployment preview, even if no changes are being deployed to the controller itself.

Additionally, any modifications to the Application Priority and SLA policy are automatically pushed to all Cisco IOS XE Catalyst SD-WAN devices associated with the policy group, as well as the Cisco SD-WAN Controllers, regardless of which devices are selected in the deployment workflow. This behavior differs from NGFW, DNS Security, and SIG policies, where changes are only deployed to the selected Cisco IOS XE Catalyst SD-WAN device.

Cisco SD-WAN Controller tasks for policy group deployments

Starting with Cisco Catalyst SD-WAN Manager Release 26.1.1.1, deploying a policy group triggers a Cisco SD-WAN Controller task during the subsequent deployment in any of these scenarios:

- A device that was previously part of a classic centralized policy is newly associated with any policy group.
- A device is removed from a policy group that had Application Priority and SLA policies deployed.
- A device associated with the policy group is included in an existing Cisco SD-WAN Controller policy configuration, even if neither of the preceding conditions applies.

Only the Cisco SD-WAN Controller intent for the current policy groups, as well as the intent for any policy group involved in a device migration is included in the CLI generation.

From SD-WAN Manager 26.2.x, when you deploy a policy group, Cisco SD-WAN Manager excludes controllers from the CLI preview if no CLI differences exist for the controllers.

Policy group deployment previews in multitenant environments

Starting with Cisco Catalyst SD-WAN Manager Release 26.1.1.1, in multitenant environments, Cisco SD-WAN Manager no longer provides a preview diff for centralized policies, topology groups, policy groups, or device templates.

Instead, Cisco SD-WAN Manager shows the complete generated configuration as new. This configuration matches what is applied to the device because multitenant environments deploy the full configuration during each deployment.

In single-tenant environments, the preview diff behavior remains unchanged. Cisco SD-WAN Manager continues to show only the configuration differences.

Add devices to a policy group using rules

Before you begin

From SD-WAN Manager 26.1.1.1, you can add devices to a policy group using tags.

Ensure that you have added tags to devices. For more information about tagging, refer to the Device tagging section in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

Follow these steps to add devices to a policy group using rules:

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the Cisco SD-WAN Manager menu, choose Configuration > Policy Groups . |
| Step 2 | Select a policy group from the available list. |
| Step 3 | Click the + Add option adjacent to Associated in the Deployment area. |
| Step 4 | Click Manage rule . You can select Modify rules or Remove rules . In the Rules section, choose values for the following options: <ul style="list-style-type: none">a) Rule name: Enter a unique name for the rule. Rule names cannot be duplicated once you create it.b) Rule Conditions: Choose one of the two rules and configure the conditions: Match All or Match Any.c) Choose one of these operators:<ul style="list-style-type: none">• Equals• Not equals• Contains• Not contains• Starts with• End with |

Note

You cannot create a new rule if it conflicts with an existing rule.

Step 5 Click **Apply**.

Based on the rule, a list of devices that will be added to or removed from the policy group appears.

Step 6 Click **Confirm** to apply the changes.

Objects and profiles

Objects and profiles provides a list of related policy objects that you can configure and call in the match or action components of a policy. Click **Objects and Profiles** to create new objects for the policy group.

In Cisco IOS XE Catalyst SD-WAN Release 17.18.x and earlier releases, **Objects and Profiles** is called **Groups of Interest**.

Configure objects and profiles

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups**.

Step 2 Click **Objects and Profiles**.

a) Configure **Application**.

From the **Application/Application family list** drop-down, choose the required applications or application families.

A few application lists are preconfigured. You cannot edit or delete these lists.

Microsoft_Apps: Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the **Entries** column.

Google_Apps: Includes Google applications, such as Gmail, Google Maps, and YouTube. To display a full list of Google applications, click the list in the **Entries** column.

b) Configure **Add App Probe Class**.

Field	Description
Probe Class Name	Enter a name for the probe class.
Forwarding Class	Choose the forwarding class from the drop-down list.
Color	Choose the color from the drop-down list.
DSCP	Enter the DSCP value.

You can add more entries if needed by clicking on + icon.

c) Configure **Color**.

Field	Description
Color List Name	Enter a name for the list.
Select Color	Choose one or more color lists types from the drop-down list.

To configure multiple colors in a single list, you can choose multiple colors from the drop-down list.

d) Configure **Community List**.

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

Field	Description
Community List Name	Enter a name of the community list.
Add Community	Enter one or more communities separated by commas. • aa : nn : Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535. For example, 65526. • internet : Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices. • local-as : Routes in this community are not advertised outside the local AS number. • no-advertise : Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • no-export : Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple community options, specifying one community in each option.

e) Configure **Data Prefix** and **Data Prefix IPv6**.

Field	Description
Data Prefix List Name	Enter a name for the data prefix list.
Add Data Prefix	Enter one or more data prefixes separated by commas. Does not support: 0.0.0.0/0

f) Configure **Expanded Community List**.

Field	Description
Community List Name	Enter a name for the community list.

Field	Description
Add Community	Specify details of the expanded community list that is used to filter communities using a regular expression.

g) Configure **Forwarding Class**.

Field	Description
Forwarding Class	Enter a name for the forwarding class.
Queue	Choose a value for the queue from the drop-down list.

h) Add policer.

Field	Description
Policer List Name	Enter a name for the policer list.
Burst (bytes)	Enter the maximum traffic burst size. The range is from 15,000 to 10,000,000 bytes.
Exceed	Choose the action to take when the burst size or traffic rate is exceeded. The options are: • Drop: sets the packet loss priority (PLP) to low • Remark: sets the packet loss priority (PLP) to high
Rate	Enter the maximum traffic rate, a value from 8 through 10 ¹¹ bits per second (bps).

i) Add preferred color group.

Choose the color preference and path preference for the primary, secondary, and tertiary colors.

Field	Description
Preferred Color Group Name	Enter a name for the preferred color group.
Color Preference	Choose the color preference from the drop-down list. You can choose multiple colors.
Path Preference	Choose the path preference from the drop-down list. The options are: • Direct Path • Multi Hop Path • All Paths

j) Add prefix list and prefix list IPv6.

Field	Description
Prefix List Name	Enter a name for the IPv4/IPv6 prefix list.
Add Prefix	Enter one or more IPv4/IPv6 prefixes separated by commas.

k) Add SLA class.

Field	Description
SLA Class List Name	Enter a name of the SLA class list.
Loss (%)	Enter the maximum packet loss on the connection, a value from 0 through 100.
Latency	Enter the maximum packet latency on the connection, a value from 1 through 1,000 milliseconds.
Jitter	Enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
App Probe Class	Choose the app probe class from the drop-down list or click Create New to create one.
Fallback Best Tunnel	Choose this option to enable the best tunnel criteria.

l) Add TLOC list.

Field	Description
List Name	Enter a name for the TLOC list.
TLOC IP	Specify the IP address for TLOC.
Color	Choose the color from the drop-down list.
Encapsulation	Choose the value from the drop-down list. The options are: • IPSec • GRE
Preference	Choose a preference to associate with the TLOC. The range is 0 to 4294967295.

Step 3 Click **Save**.

Policy validation for Cisco Catalyst SD-WAN

Policy validation in Cisco Catalyst SD-WAN is a process that

- automatically checks if your policies are accurate,

- ensures that policies comply with platform capabilities, and
- confirms that policies align with your network requirements.

This process helps verify that all configurations operate within supported limits before deployment.

Key features of policy validation

Centralized policy checks: From Cisco IOS XE Catalyst SD-WAN Release 26.1.1 policy validation is centrally managed, enabling quicker error detection and ensuring configurations remain within supported limits.

Enhanced device alerts: Devices send detailed alerts to Cisco SD-WAN Manager for proactive monitoring.

Filters in a sequence: Each policy sequence supports up to 64 filters, giving you flexibility to define granular traffic matching criteria.

Entries in a list: You can create and modify lists with a combined total of up to 8192 entries including existing and new entries to ensure scalability for complex network requirements.

Key terms for policy validation

Key terms for policy validation are:

- **Application list:** An [application list](#) is a collection of applications grouped together for policy matching, allowing you to apply policies to multiple applications at once.
- **Application family:** An [application family](#) refers to a category of related applications such as Cisco Webex, Microsoft Teams, and Zoom. Application categories simplify policy management and enforcement.

Troubleshooting policy group validations

When you activate or deactivate a centralized policy or deploy a controller template, some controller-related policies associated in policy groups are deployed to prevent any errors in policy. You can avoid these validation errors using any one of the following workarounds:

- Dissociate application priority and SLA policy from any of the policy groups that have devices associated.
- Dissociate devices from any policy group that has application priority and SLA policy.
- Fix the issues in the application priority and SLA policy (In this case, you need to associate the device to a configuration group that has the selected VPNs).