
Policies

Use the Policies screen to create and activate centralized and localized control and data policies for vSmart controllers and vEdge routers.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Policies, and the following:
 - Custom Options—Click to display, create, and edit a components for use in policy. For centralized policy, the components are CLI policies, lists, topologies, and traffic policies. For localized policy, the components are CLI policies, lists, forwarding class/QoS definitions, access control lists (ACLs), and route policies.
- Centralized Policy tab—Create a centralized policy. When you first open the Policies screen, the Centralized Policy tab is selected.
 - Add Policy—Click to create a centralized policy using a policy configuration wizard.
- Localized Policy tab—Create a localized policy.
 - Add Policy—Click to create a localized policy using a policy configuration wizard.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the policies table with the most current data.
- Show Table Columns icon—Click to display or hide columns from the policies table. By default, all columns are displayed.
- Policies table—To re-arrange the columns, drag the column title to the desired position.



Menu

Policies Table

CloudExpress Tasks Alarms Help User Profile

Cisco vManage

CONFIGURATION | POLICIES

Centralized Policy Localized Policy

Add Policy

Search Options

Total Rows: 3

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
gap_policy	gap_policy	UI Policy Builder	true	admin	08172017T003048611	16 Aug 2017 5:30:48 P...	...
mediatek_policy	mediatek_policy	UI Policy Builder	false	admin	08172017T003114617	16 Aug 2017 5:31:14 P...	...
pnc_policy	pnc_policy	UI Policy Builder	false	admin	08172017T003123414	16 Aug 2017 5:31:23 P...	...

G00425

Configure Centralized Policy

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

For more information about the centralized policy components, see [Configuring Centralized Control Policy](#). For information about application-aware routing policy components, see [Configuring Application-Aware Routing](#).

To start the wizard, select the Centralized Policy tab and click Add Policy. The Create Groups of Interest screen is displayed.



Configure Groups of Interest (Lists)

In the Create Groups of Interest screen:

1. In the left pane, select the type of list to use with the localized policy. It can be one of the following:
 - Application
 - Color
 - Data Prefix
 - Policer
 - Prefix
 - Site
 - SLA Class
 - TLOC
 - VPN
2. In the right pane, click the New button. The New List portion of the screen opens.
3. Enter a name for the list, and enter or select the components to include in the list.
Note that the application lists Google_Apps and Microsoft_Apps are preconfigured, and you cannot edit or delete them.
4. Click Add to create the new list.
5. Repeat Steps 1 through 4 to create additional lists.
6. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.
7. Click Next to move to Configure Topology in the wizard.

Configure Topology and VPN Membership

When you first open the Configure Topology and VPN Membership screen, the Topology tab is selected by default.

To configure topology and VPN membership:

1. To configure a topology policy component:
 1. In the Topology tab, click the Add Topology drop-down.
 2. Select the desired network topology.
 3. Enter a name and description for the topology, and select the VPN list to which the topology applies.



4. Click the New button, and enter the information for the topology component.
 5. Enter a name for the topology component, and enter or select the components to include in it.
 6. Click Save.
2. To configure a VPN membership policy component:
 1. In the VPN Membership tab, click Add VPN Membership Policy.
 2. In the Update VPN Membership Policy popup, enter a name and description of the VPN membership, and select site lists and VPN lists. To create new lists, click Add List.
 3. Click Save.
 3. To edit, copy, or delete an existing topology or VPN membership policy, select it and click the Edit, Copy, or Trash Bin icon in the Action column.
 4. Click Next to move to Configure Traffic Rules in the wizard.

Configure Traffic Rules

When you first open the Traffic Rules screen, the Application-Aware Routing tab is selected by default.

To configure traffic rules:

1. In the Application-Aware Routing tab, select the desired policy type—Application-Aware Routing, Traffic Data, or Cflowd.
2. Click the Add Policy drop-down.
3. To import an existing policy, select Import Existing. In the Import Existing Data Policy popup, select the name of the file containing the data policy. Then click Import.
4. To create a new policy, select Create New, and in the left pane, click Sequence Type.
5. For an application-aware routing policy:
 1. In the right pane, click Sequence Rule.
 2. Add the match and action rules.
 3. Add additional sequences as needed. Drag and drop sequences to re-order them
 4. Click Save Application-Aware Routing Policy.
6. For a traffic data policy:
 1. From the Add Data Policy popup, select the policy type.
 2. In the right pane, click Sequence Rule.



3. Add the match and action rules.
4. Add additional sequences as needed. Drag and drop sequences to re-order them
5. Click Save Data Policy.
7. For cflowd policy:
 1. To configure the cflowd template, enter values for the active flow timeout, inactive flow timeout, flow refresh interval, and sampling interval.
 2. To configure a collector list, click Add New Collector. Enter the VPN ID where the collector is located, its IP address, port number, transport protocol, and source interface. Click Add.
 3. Click Save Cflowd Policy.
8. Click Next to move to Apply Policies to Sites and VPNs in the wizard.

Apply Policy to Sites and VPNs

In the Apply Policies to Sites and VPNs screen:

1. Enter a name for the policy. 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.
2. Enter a description of the policy. This field is mandatory, and it can contain any characters and spaces. It can contain up to 2048 characters.
3. Click New Site List and VPN List.
4. Select the site list and VPN list, and click Add.
5. Click Preview to view the configured policy. The policy is displayed in CLI format.
6. Click Save Policy. The Configuration ► Policies screen is then displayed, and the policies table includes the newly created policy.

Configure Localized Policy

You configure localized policy with a configuration wizard. The wizard is a UI policy builder that consists of five screens to configure and modify the following localized policy components:

- Groups of interest, also called lists
- Forwarding classes to use for QoS
- Access control lists (ACLs)
- Route policies



- Policy settings

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

For more information about the localized policy components, see [Configuring Localized Data Policy for IPv4](#) and [Configuring Localized Data Policy for IPv6](#).

To start the wizard, select the Localized Policy tab and click Add Policy. The Create Groups of Interest screen is displayed.

Configure Groups of Interest (Lists)

In the Create Groups of Interest screen:

1. In the left pane, select the type of list to use with the localized policy. It can be one of the following:
 - AS Path
 - Community
 - Data Prefix
 - Extended Community
 - Mirror
 - Policer
 - Prefix
2. In the right pane, click the New button. The New List portion of the screen opens.
3. Enter a name for the list, and enter or select the components to include in the list.
4. Click Add to create the new list.
5. Repeat Steps 1 through 4 to create additional lists.
6. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.
7. Click Next to move to Configure Forwarding Classes/QoS in the wizard. When you first open this screen, the QoS tab is selected by default.

Configure Forwarding Classes for QoS

When you first open the Forwarding Classes/QoS screen, the QoS tab is selected by default.

To configure forwarding classes for use by QoS:



1. To create a new QoS mapping:
 1. In the QoS tab, click the Add QoS drop-down.
 2. Select Create New.
 3. Enter a name and description for the QoS mapping.
 4. Click Add Queue. The Add Queue popup displays.
 5. Select the queue number from the Queue drop-down.
 6. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types. Enter the forwarding class.
 7. Click Save.
2. To import an existing QoS mapping:
 1. In the QoS tab, click the Add QoS drop-down.
 2. Select Import Existing.
 3. Select a QoS mapping.
 4. Click Import.
3. To view or copy a QoS mapping or to remove the mapping from the localized policy, click the More Actions icon to the right of the row, and select the desired action.
4. To configure policy rewrite rules for the QoS mapping:
 1. In the QoS tab, click the Add Rewrite Policy drop-down..
 2. Select Create New.
 3. Enter a name and description for the rewrite rule.
 4. Click Add Rewrite Rule. The Add Rule popup displays.
 5. Enter the class name and DSCP value, and select the priority level.
 6. Click Save.
5. To import an existing rewrite rule:
 1. In the QoS tab, click the Add Rewrite Policy drop-down..
 2. Select Import Existing.
 3. Select a rewrite rule.
 4. Click Import.
6. Click Next to move to Configure Access Lists in the wizard.



Configure ACLs

To configure access control lists (ACLs):

1. To create a new IPv4 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv4 ACL Policy.
2. To create a new IPv6 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv6 ACL Policy.
3. Enter a name and description for the ACL.
4. In the left pane, click Add ACL Sequence. An Access Control List box is displayed in the left pane.
5. Double-click the Access Control List box, and type a name for the ACL.
6. In the right pane, click Add Sequence Rule to create a single sequence in the ACL. The Match tab is selected by default.
7. Click a match condition.
8. On the left, enter the values for the match condition.
9. On the right enter the action or actions to take if the policy matches.
10. Repeat Steps 6 through 8 to add match–action pairs to the ACL.
11. To rearrange match–action pairs in the ACL, in the right pane drag them to the desired position.
12. To remove a match–action pair from the ACL, click the X in the upper right of the condition.
13. Click Save Match and Actions to save a sequence rule.
14. To rearrange sequence rules in an ACL, in the left pane drag the rules to the desired position.
15. To copy, delete, or rename an ACL sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.
16. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
 1. Click Default Action in the left pane.
 2. Click the Pencil icon.
 3. Change the default action to Accept.
 4. Click Save Match and Actions.
17. Click Next to move to Configure Route Policy in the wizard.

Configure Route Policies

To configure a new route policy:



1. In the Add Route Policy tab, select Create New.
2. Enter a name and description for the route policy.
3. In the left pane, click Add Sequence Type. A Route box is displayed in the left pane.
4. Double-click the Route box, and type a name for the route policy.
5. In the right pane, click Add Sequence Rule to create a single sequence in the ACL. The Match tab is selected by default.
6. Click a match condition.
7. On the left, enter the values for the match condition.
8. On the right enter the action or actions to take if the policy matches.
9. Repeat Steps 6 through 8 to add match–action pairs to the route policy.
10. To rearrange match–action pairs in the route policy, in the right pane drag them to the desired position.
11. To remove a match–action pair from the route policy, click the X in the upper right of the condition.
12. Click Save Match and Actions to save a sequence rule.
13. To rearrange sequence rules in an route policy, in the left pane drag the rules to the desired position.
14. To copy, delete, or rename an route policy sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.
15. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
 1. Click Default Action in the left pane.
 2. Click the Pencil icon.
 3. Change the default action to Accept.
 4. Click Save Match and Actions.
16. Click Next to move to Policy Overview in the wizard.

Configure Policy Settings

To configure policy settings, in the Policy Overview screen:

1. Enter a name and description for the route policy.
2. To enable cflowd visibility so that a vEdge router can perform traffic flow monitoring on traffic coming to the router from the LAN, click Netflow.
3. To enable application visibility so that a vEdge router can monitor and track the applications running on the LAN, click



Application.

4. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from transport-side interfaces, click Cloud QoS.
5. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from service-side interfaces, click Cloud QoS Service Side.
6. To log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface, click Implicit ACL Logging.
7. To configure how often packets flows are logged, click Log Frequency. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.
8. Click Preview to view the full policy in CLI format.
9. Click Save Policy.

View a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click View. Policies created with the UI policy builder are displayed in graphical format. Policies created using the CLI are displayed in text format.
3. Click Cancel to return to the policies table.

For a policy created using the vManage policy configuration wizard, you can view the policy in text format:

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Preview.
3. Click Cancel to return to the policies table.

Copy a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Copy.
3. In the Policy Copy popup window, enter the policy name and a description of the policy.
4. Click Copy.

Edit a Policy

For policies created using the vManage policy configuration wizard:



1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Save Policy Changes.

For policies created using the CLI:

1. In the Custom Options drop-down, click CLI Policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Update.

Edit or Create a Policy Component

You can create individual policy components directly and then use them or import them when you are using the policy configuration wizard:

1. In the Title bar, click the Custom Options drop-down.
2. For centralized policy, select the policy component type:
 - CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.
 - Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
 - Topology—Create a hub-and-spoke, mesh, or custom topology or a VPN membership to import in the Topology screen in the policy configuration wizard.
 - Traffic Policy—Create an application-aware routing, traffic data, or cflowd policy to import in the Traffic Rules screen in the policy configuration wizard.
3. For localized policy, select the policy component type:
 - CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.
 - Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
 - Forwarding Class/QoS—Create QoS mappings and rewrite rules to import in the Forwarding Classes/QoS screen in the policy configuration wizard.
 - Access Control Lists—Create ACLs of interest to import in the Configure Access Lists screen in the policy configuration wizard.



- Route Policy—Create route policies to import in the Configure Route Policies screen in the policy configuration wizard.

Delete a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the policy.

Activate a Policy on vSmart Controllers

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Activate.
3. In the Activate Policy popup, click Activate to push the policy to all reachable vSmart controllers in the network.
4. Click OK to confirm activation of the policy on all vSmart controllers.

Additional Information

[Application-Aware Routing](#)

[Centralized Control Policy](#)

[Centralized Data Policy](#)

[Configure Policies](#)

[Localized Control Policy](#)

[Localized Data Policy](#)

