

Policy Basics

- Policy Overview, on page 1
- Policies in Cisco vManage, on page 3

Policy Overview

Table 1: Feature History

Feature	Release Information	Description
Policy Enforcement Failure	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature aims to detect when a policy download fails and raises an alarm (policy-enforcement-status). Additionally, this feature introduces new **service-path** show commands.

Policy influences the flow of data traffic and routing information among Cisco vEdge deviceCisco IOS XE Catalyst SD-WAN devices in the overlay network.

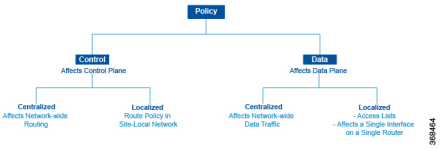
Policy comprises:

- Routing policy—which affects the flow of routing information in the network's control plane.
- Data policy—which affects the flow of data traffic in the network's data plane.

To implement enterprise-specific traffic control requirements, you create basic policies, and deploy advanced features that are activated by means of the policy configuration infrastructure.

Just as the Cisco Catalyst SD-WAN overlay network architecture clearly separates the control plane from the data plane and control between centralized and localized functions, the Cisco Catalyst SD-WAN policy is cleanly separated. Policies apply either to control plane or data plane traffic, and they are configured either centrally on Cisco SD-WAN Controllers or locally on Cisco vEdge deviceCisco IOS XE Catalyst SD-WAN devices. The following figure illustrates the division between control and data policy, and between centralized and local policy.

Figure 1: Policy Architecture



Control and Data Policy

Control policy is the equivalent of routing protocol policy, and data policy is equivalent to what are commonly called access control lists (ACLs) and firewall filters.

Centralized and Localized Policy

The Cisco Catalyst SD-WAN policy design provides a clear separation between centralized and localized policy. In short, centralized policy is provisioned on the centralized Cisco SD-WAN Controllers in the overlay network, and the localized policy is provisioned on Cisco vEdge devices, which sit at the network edge between a branch or enterprise site and a transport network, such as the Internet, MPLS, or metro Ethernet.

Centralized Policy

Centralized policy refers to policy provisioned on Cisco SD-WAN Controllers, which are the centralized controllers in the Cisco Catalyst SD-WAN overlay network. Centralized policy comprises two components:

- Control policy, which affects the overlay network–wide routing of traffic
- Data policy, which affects the data traffic flow throughout the VPN segments in the network

Centralized control policy applies to the network-wide routing of traffic by affecting the information that is stored in the Cisco SD-WAN Controller's route table and that is advertised to the Cisco vEdge devices. The effects of centralized control policy are seen in how Cisco vEdge devices direct the overlay network's data traffic to its destination.

Note The centralized control policy configuration itself remains on the Cisco SD-WAN Controller and is never pushed to local devices.

Centralized data policy applies to the flow of data traffic throughout the VPNs in the overlay network. These policies can permit and restrict access based either on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol) or on VPN membership. These policies are pushed to the selected Cisco vEdge devices.

Localized Policy

Localized policy refers to a policy that is provisioned locally through the CLI on the Cisco vEdge devices, or through a Cisco SD-WAN Manager device template.

Localized control policy is also called as route policy, which affects (BGP and OSPF) routing behavior on the site-local network.

Localized data policy allows you to provision access lists and apply them to a specific interface or interfaces on the device. Simple access lists permit and restrict access based on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol), in the same way as with centralized data policy. Access

lists also allow provisioning of class of service (CoS), policing, and mirroring, which control how data traffic flows out of and in to the device's interfaces and interface queues.

The design of the Cisco Catalyst SD-WAN policy distinguishes basic and advanced policies. Basic policy allows you to influence or determine basic traffic flow through the overlay network. Here, you perform standard policy tasks, such as managing the paths along which traffic is routed through the network, and permitting or blocking traffic based on the address, port, and DSCP fields in the packet's IP header. You can also control the flow of data traffic into and out of a Cisco vEdge device 's interfaces, enabling features such as class of service and queuing, mirroring, and policing.

Advanced features of Cisco Catalyst SD-WAN policy offer specialized policy-based network applications. Examples of these applications include the following:

- Service chaining, which redirects data traffic to shared devices in the network, such as firewall, intrusion detection and prevention (IDS), load balancer, and other devices, before the traffic is delivered to its destination. Service chaining obviates the need to have a separate device at each branch site.
- Application-aware routing, which selects the best path for traffic based on real-time network and path performance characteristics.
- Cflowd, for monitoring traffic flow.
- Converting a Cisco vEdge device into a NAT device, to allow traffic destined for the Internet or other public network can exit directly from the Cisco vEdge device.

By default, no policy of any kind is configured on Cisco vEdge devices, either on the centralized Cisco SD-WAN Controllers or the local Cisco vEdge devices. When control plane traffic, which distributes route information, is unpolicied:

- All route information that OMP propagates among the Cisco vEdge devices is shared, unmodified, among all Cisco SD-WAN Controllers and all Cisco vEdge devices in the overlay network domain.
- No BGP or OSPF route policies are in place to affect the route information that Cisco vEdge device s propagate within their local site network.

When data plane traffic is unpolicied, all data traffic is directed towards its destination based solely on the entries in the local Cisco vEdge device's route table, and all VPNs in the overlay network can exchange data traffic.

Policies in Cisco vManage

Use the Policies screen to create and activate centralized and localized control and data policies for Cisco Catalyst SD-WAN Controllers and Cisco vEdge devices.

Figure 2: Policy Configuration

This screen allows you to perform several tasks related to policies in Cisco SD-WAN Manager:

- View centralized or localized policies
- Copy, edit, or delete policies
- Create and edit policy components
- Activate and deactivate a centralized policy on Cisco Catalyst SD-WAN Controllers

Create and Manage Policies Using Cisco SD-WAN Manager

View Centralized or Localized Policies

To view centralized or localized policies, do the following:

1. From the **Centralized Policy** or **Localized Policy** tab, select a policy.
2. For a policy created using the UI policy builder or using the CLI, click **More Actions** and click **View**. The policy created using the UI policy builder is displayed in graphical format while the policy created using the CLI method is displayed in text format.
3. For a policy created using the Cisco SD-WAN Manager policy configuration wizard, click **More Actions** and click **Preview**. This policy is displayed in text format.

Copy, Edit, and Delete Policies

1. To copy a policy:
   a. From the **Centralized Policy** or **Localized Policy** tab, select a policy.
   b. Click **More Actions** and click **Copy**.
   c. In the Policy Copy popup window, enter the policy name and a description of the policy.

Note If you are upgrading to 18.4.4 version, data policy names need to be under 26 characters.

Note Starting with the Cisco SD-WAN release 19.3 , 127 characters are supported for policy names for the following policy types:

- Central route policy
- Local route policy
- Local Access Control lOst (ACL)
- Local IPv6 ACL
- Central data policy
- Central app route policy
- QoS map
- Rewrite rule

All other policy names support 32 characters.

   d. Click **Copy**.

2. To edit policies created using the Cisco SD-WAN Manager policy configuration wizard:
   a. Click **More Actions** and click **Edit**.

b. Edit the policy as needed.

c. Click **Save Policy Changes**.

3. To edit polices created using the CLI method:

a. In the **Custom Options** drop-down, click **CLI Policy**.

b. Click **More Actions** and click **Edit**.

c. Edit the policy as needed.

d. Click **Update**.

4. To delete policies:

a. From the **Centralized Policy** or **Localized Policy** tab, select a policy.

b. Click **More Actions** and click **Delete**.

c. Click **OK** to confirm deletion of the policy.

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 policies, select the **Centralized Policy** tab and then select a policy component:

- 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 policies, select the **Localized Policy** tab and then select a policy component:

- 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.

Activate a Centralized Policy on Cisco vSmart Controllers

1. In the title bar, click the **Custom Options** drop-down.
2. In the **Centralized Policy** tab, and then select a policy.
3. Click **More Actions** and click **Activate**.
4. In the **Activate Policy** popup, click **Activate** to push the policy to all reachable Cisco Catalyst SD-WAN Controllers in the network.
5. Click **OK** to confirm activation of the policy on all Cisco Catalyst SD-WAN Controllers.
6. To deactivate the centralized policy, select the = tab, and then select a policy.
7. 6. Click **More Actions** and click **Deactivate**.
8. In the **Deactivate Policy** popup, click **Deactivate** to confirm that you want to remove the policy from all reachable Cisco Catalyst SD-WAN Controllers.