

Localized Policy

The topics in this section provide overview information about the different types of localized policies, the components of localized policies, and how to configure localized policies using Cisco SD-WAN Manager or the CLI.

- QoS For Router Generated Cisco SD-WAN Manager Traffic, on page 1
- Overview of Localized Policies, on page 2
- Configure policies using a configuration group, on page 3
- Configure Localized Policy for IPv4 Using the CLI, on page 20
- Configure Localized Policy for IPv6 Using the CLI, on page 22
- Localized Data Policy Configuration Examples, on page 23
- Configure Localized Policy Using Cisco SD-WAN Manager , on page 23
- QoS For Router Generated Cisco SD-WAN Manager Traffic, on page 40
- Information About QoS For Router-Generated Cisco SD-WAN Manager Traffic, on page 40
- Restrictions For QoS For Router Generated Cisco SD-WAN Manager Traffic, on page 41
- Configure QoS for router-generated Cisco SD-WAN Manager traffic using a CLI template, on page 41
- Verify QoS for Router Generated Cisco SD-WAN Manager Traffic Using CLI, on page 42
- Troubleshooting QoS For Router Generated Cisco SD-WAN Manager Traffic, on page 43

QoS For Router Generated Cisco SD-WAN Manager Traffic

Table 1: Feature History

Feature Name	Release Information	Description
QoS for Router Generated Cisco SD-WAN Manager Traffic	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature helps you to prioritize or queue router-generated Cisco SD-WAN Manager traffic based on your specific requirements. Use QoS policies and class maps to route Cisco SD-WAN Manager traffic through a queue of your choice.

Overview of Localized Policies

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

Types of localized policies

Localized control policy

Control policy operates on the control plane traffic in the Cisco IOS XE Catalyst SD-WAN overlay network, influencing the determination of routing paths through the overlay network. Localized control policy is policy that is configured on a Cisco IOS XE Catalyst SD-WAN device (hence, it is local) and affects BGP and OSPF routing decisions on the site-local network that the device is part of.

In addition to participating in the overlay network, a Cisco IOS XE Catalyst SD-WAN device participates in the network at its local site, where it appears to the other network devices to be simply a regular router. As such, you can provision routing protocols, such as BGP and OSPF, on the Cisco IOS XE Catalyst SD-WAN device so that it can exchange route information with the local-site routers. To control and modify the routing behavior on the local network, you configure a type of control policy called route policy on the devices. Route policy applies only to routing performed at the local branch, and it affects only the route table entries in the local device's route table.

Localized control policy, which you configure on the devices, lets you affect routing policy on the network at the local site where the device is located. This type of control policy is called route policy. This policy is similar to the routing policies that you configure on a regular driver, allowing you to modify the BGP and OSPF routing behavior on the site-local network. Whereas, centralized control policy affects the routing behavior across the entire overlay network, route policy applies only to routing at the local branch.

Localized data policy

Data policy operates on the data plane in the Cisco IOS XE Catalyst SD-WAN overlay network and affects how data traffic is sent among the Cisco IOS XE Catalyst SD-WAN devices in the network. The Cisco Catalyst SD-WAN architecture defines two types of data policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on a Cisco IOS XE Catalyst SD-WAN device.

Localized data policy, so called because it is provisioned on the local Cisco IOS XE Catalyst SD-WAN device, is applied on a specific router interface and affects how a specific interface handles the data traffic that it is transmitting and receiving. Localized data policy is also referred to as access lists (ACLs). With access lists, you can provision class of service (CoS), classifying data packets and prioritizing the transmission properties for different classes. You can configure policing.

For IPv4, you can configure QoS actions.

You can apply IPv4 access lists in any VPN on the router, and you can create access lists that act on unicast and multicast traffic. You can apply IPv6 access lists only to tunnel interfaces in the transport VPN (VPN 0).

You can apply access lists either in the outbound or inbound direction on the interface. Applying an IPv4 ACL in the outbound direction affects data packets traveling from the local service-side network into the IPsec tunnel toward the remote service-side network. Applying an IPv4 ACL in the inbound direction affects data packets exiting from the IPsec tunnel and being received by the local Cisco IOS XE Catalyst SD-WAN device.

For IPv6, an outbound ACL is applied to traffic being transmitted by the router, and an inbound ACL is applied to received traffic.

Explicit and implicit access lists

Access lists that you configure using localized data policy are called *explicit* ACLs. You can apply explicit ACLs in any VPN on the router.

Router tunnel interfaces also have *implicit ACLs*, which are also referred to as *services*. Some of these are present by default on the tunnel interface, and they are in effect unless you disable them. Through configuration, you can also enable other implicit ACLs. On Cisco IOS XE Catalyst SD-WAN devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

Perform QoS actions

With access lists, you can provision quality of service (QoS) which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. See Forwarding and QoS Overview.

Configure policies using a configuration group

Use this task to provision localized policies, such as Access Control Lists (ACLs), Quality of Service (QoS), and Route Policies, on Cisco IOS XE Catalyst SD-WAN devices using a centralized configuration group approach.

-

Before you begin

- A configuration group must be created.
- A Transport & Management profile must be configured.

Follow these steps to configure policies using a configuration group:

Procedure

Step 1 Configure **Objects and Policies** using a configuration group. For more information, refer to Configure objects and policies using a configuration group, on page 5.

Step 2 Configure **Forwarding Classes and QoS** using a configuration group. For more information, refer to

Step 3 Configure ACLs using a configuration group. For more information, refer to Configure ACLs using a configuration group, on page 11.

Step 4 Configure route policy using a configuration group. For more information, refer to Configure Route Policy Using a Configuration Group, on page 15.

The localized policy is saved to the configuration group and is ready to be applied to the target devices.

What to do next

Deploy the configuration group to the target devices to push the localized policy settings to the network. For more information, Deploy a Configuration Group.

Configure Forwarding Classes and QoS using a policy group

Use this task to define forwarding classes and Quality of Service (QoS) maps within a policy group to prioritize network traffic and ensure efficient bandwidth utilization on your Cisco IOS XE Catalyst SD-WAN devices.

Before you begin

A policy group must be created.

Follow these steps to configure forwarding classes and QoS using a policy group:

Procedure

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

Step 2 Select the desired policy group and click **Edit**.

Step 3 Click **Application Priority and SLA**.

Step 4 Click **Add Traffic Policy** or select an existing policy to edit.

Step 5 Click **Advanced Layout** to switch to the advanced view.

Step 6 Click **QoS Queue**.

Step 7 Click **Add QoS Policy** to define the QoS queue parameters.

Table 2: QoS Queue

Field	Description
Queuing Model	Choose a value from the drop-down list for the queuing model.
Policy Name	Provide a name for the policy.
Interface	Specify a value for the interface.
Forwarding class	Choose a value for the forwarding class from the drop-down list.
Bandwidth %	Specify the maximum bandwidth. The range is 1–99.
Drops	Choose a value for the drop type from the following options: • **Random Early** • **Tail**
Scheduling type	Specify how to prioritize data packets for transmission to the destination by configuring the schedule type. The default is Weighted Round Robin (WRR).

Step 8 Click **Save**.

The forwarding classes and QoS maps are saved to the policy group and are ready to be applied to the target devices.

What to do next

Deploy the policy group to the target devices to push the QoS settings to the network. For more information, Deploy Policy Group Workflow.

Configure objects and policies using a configuration group

Use this task to define reusable policy objects, such as AS Path lists, community lists, and prefix lists, within a configuration group. These objects serve as the building blocks for your localized policies.

Before you begin

Follow these steps to configure policy objects within a configuration group:

Procedure

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

Step 2 Select the desired configuration group and click **Edit**

Step 3 Click **Objects and Profiles**.

Step 4 Perform one of the following tasks based on your requirements:

- Configure an AS Path list using a configuration group, on page 6.
- Configure Standard Community using a configuration group, on page 6.
- Configure Data Prefix using a configuration group, on page 7.
- Configure Extended Community using a configuration group, on page 8.
- Configure Class Map using a configuration group, on page 9.
- Configure Policer using a configuration group, on page 10.
- Configure Prefix using a configuration group, on page 11.

The policy objects are saved to the configuration group and are available to be referenced in your policy sequences.

What to do next

After defining your policy objects, you can reference them while configuring policies such as Access Control Lists (ACLs) or Route Policies. For more information, refer to Configure policies using a configuration group, on page 3.

Configure an AS Path list using a configuration group

Use this task to create a list of BGP AS paths that you can reference in route policies to control route acceptance, preference, or advertisement.

Before you begin

- A configuration group must be created.
- A Transport and Management profile must be configured.

Follow these steps to configure an AS Path list:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
Step 2 Click **Objects and Profiles**
Step 3 Select the **AS Path** policy object.
Step 4 Click **Add AS Path**.
Step 5 Enter a **Name** and **Description** for the AS Path list.
Step 6 Enter the AS path number in the **AS path list ID** field. The range is 1 to 65535.
Step 7 Enter the AS path in the **AS path list** field, separating AS numbers with a comma. You can write each AS as a single number or as a regular expression.
Step 8 Click **Save**.

The AS Path list is saved to the configuration group and is ready to be referenced in route policy configurations.

What to do next

Deploy the configuration group to the target devices to push the localized policy settings to the network. For more information, Deploy a Configuration Group.

Configure Standard Community using a configuration group

Use this task to create a list of standard or expanded BGP communities that you can reference in route policies to control route acceptance or advertisement.

Before you begin

- A configuration group must be created.
- A Transport and Management profile must be configured.

Follow these steps to configure a community list:

Procedure

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

Step 2 Click **Objects and Profiles**.

Step 3 Select the **Standard Community** policy object.

Step 4 Click **Add Standard Community**.

Step 5 Enter a **Name** and **Description** for the Standard Community.

Step 6 In the **Standard Community** field, enter one or more communities separated by commas. You can use formats such as aa:nn (AS number and network number), internet, local-as, no-advertise, or no-export.

The format example is given in the field.

Field	Description
Standard Community	• *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **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.

Step 7 Click **Save**.

The community list is saved to the configuration group and is ready to be referenced in route policy configurations.

What to do next

Deploy the configuration group to the target devices to push the localized policy settings to the network. For more information, Deploy a Configuration Group.

Configure Data Prefix using a configuration group

Use this task to create a list of IP prefixes that you can reference in data policies to permit or restrict traffic based on source or destination addresses.

Before you begin

- A configuration group must be created.
- A Transport and Management profile must be configured.

Follow these steps to configure a data prefix list:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
Step 2 Click **Objects and Profiles**.
Step 3 Select the **Data Prefix** policy object.
Step 4 Click **Add Data Prefix**.
Step 5 Enter a **Name** and **Description** for Data Prefix.
Step 6 In the **Data Prefix** field, enter one or more IP prefixes separated by commas. You can enter IP prefixes for IPv4 or IPv6.
Step 7 Click **Save**.

The data prefix list is saved to the configuration group and is ready to be referenced in data policy configurations.

What to do next

Deploy the configuration group to the target devices to push the localized policy settings to the network. For more information, Deploy a Configuration Group.

Configure Extended Community using a configuration group

Use this task to create a list of BGP extended communities that you can reference in route policies for advanced route control.

Before you begin

- A configuration group must be created.
- A Transport and Management profile must be configured.

Follow these steps to configure an extended community list:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
Step 2 Click **Objects and Profiles**.
Step 3 Select the **Extended Community** policy object.
Step 4 Click **Add Extended Community**.
Step 5 Enter a **Name** and **Description** for Extended Community.
Step 6 In the **Extended Community** field, enter the community details.

The format example is given in the field.

Field	Description
Extended Community	• **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • *soo* (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.

The extended community list is saved to the configuration group and is ready to be referenced in route policy configurations.

What to do next

Deploy the configuration group to the target devices to push the localized policy settings to the network. For more information, Deploy a Configuration Group.

Configure Class Map using a configuration group

Use this task to create a class map within a configuration group to define forwarding classes and map them to specific queues for Quality of Service (QoS) management.

Before you begin

- A configuration group must be created.
- A Transport and Management profile must be configured.

Follow these steps to configure a class map:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
Step 2 Click **Objects and Profiles**.
Step 3 Select the **Class Map** policy object.
Step 4 Click **Add Class Map**.
Step 5 Enter a **Name** and **Description** for Class Map.
Step 6 Select the required **Queue** from the drop-down list..
Step 7 Click **Save**.

The class map is saved to the configuration group and is ready to be referenced in QoS policy configurations.

What to do next

Deploy the configuration group to the target devices to push the localized policy settings to the network. For more information, Deploy a Configuration Group.

Configure Policer using a configuration group

Use this task to define policing parameters, such as rate and burst size, to control traffic flow and prevent network congestion

Before you begin

- A configuration group must be created.
- A Transport and Management profile must be configured

Follow these steps to configure a policer:

Procedure

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

Step 2 Click **Objects and Profiles**.

Step 3 Select the **Policer** policy object.

Step 4 Click **Add Policer**.

Step 5 Enter a **Name** and **Description** for Policer.

Step 6 In the **Burst (bytes)** field, enter the maximum traffic burst size in bytes.

Step 7 In the **Exceed** drop-down list, choose the action **Drop** or **Remark**.

Step 8 In the **Rate (bps)**, enter the maximum traffic rate in bits per second (bps).

The following table describe the options for configuring the policer.

Field	Description
Burst (bytes)	Specifies the maximum traffic burst size. Range is from 15000 to 10000000.
Exceed	Specifies an 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 PLP to high. The default option is **Drop**.
Rate	Specifies the maximum traffic rate. It can be a value from 8 through 2^{64} bps (8 through 100000000000).

Step 9 Click **Save**.

The policer is saved to the configuration group and is ready to be referenced in data policy or ACL configurations.

What to do next

Deploy the configuration group to the target devices to push the localized policy settings to the network. For more information, Deploy a Configuration Group.

Configure Prefix using a configuration group

Use this task to create a list of IP prefixes that you can reference in policies to match specific network traffic or routes.

Before you begin

- A configuration group must be created.
- A Transport and Management profile must be configured.

Follow these steps to configure a prefix list:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
Step 2 Click **Objects and Profiles**.
Step 3 Select the **Prefix** policy object.
Step 4 Click **Add Prefix**.
Step 5 Enter a **Name** and **Description** for Prefix.
Step 6 In the **Prefix** field, enter one or more IP prefixes separated by commas. You can enter IP prefixes for IPv4 or IPv6.
Step 7 Under **Add Prefix**, enter the prefix for the list. Optionally, click the **Choose a file** link to import a prefix list.
Step 8 Click **Save**.

The prefix list is saved to the configuration group and is ready to be referenced in control or data policy configurations.

What to do next

Deploy the configuration group to the target devices to push the localized policy settings to the network. For more information, Deploy a Configuration Group.

Configure ACLs using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

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

Step 2 Create and configure an Ethernet Interface feature in a Transport & Management profile.

Step 3 Click the plus (+) adjacent to the Ethernet Interface feature to display the Add Feature pane.

Step 4 Add a ACL IPv4 or ACL IPv6 feature to the Ethernet Interface feature.

The following table describe the options for configuring the ACL IPv4 feature.

Table 3: ACL IPv4

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.
Condition	Specifies the ACL condition. The options are: • DSCP • Packet Length • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • ICMP Message (Only in Cisco Catalyst SD-WAN Manager Release 20.15.1)
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: • Counter • DSCP • Log • Next Hop • Service Chain • Policer

The following table describe the options for configuring the ACL IPv6 feature.

Table 4: ACL IPv6

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.

Field	Description
Condition	Specifies the ACL condition. The options are: • Next Header • Packet Length • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Traffic Class • ICMP Message (Only in Cisco Catalyst SD-WAN Manager Release 20.15.1)
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: • Counter • Log • Next Hop • Traffic Class • Service Chain • Policer

Table 5: Match parameters

Match Condition	Description
Class	Name of a class defined with a **policy class-map** command.
Destination Data Prefix	Name of a data-prefix-list list.
Destination Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
DSCP	Specifies the DSCP value. The range is 0 through 63.
Protocol	Specifies the internet protocol number. The range is 0 through 255.

Match Condition	Description
ICMP Message	When you select a Protocol value as 1 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. When you select a Next Header value as 58 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1. For **`icmp-msg`** and **`icmp6-msg`** message types, refer to the ICMP Message Types/Codes and Corresponding Enumeration Values table in the Centralized chapter.
Packet Length	Specifies the length of the packet. The range can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).
Source Data Prefix	Specifies the name of a **data-prefix-list** list.
PLP	Specifies the Packet Loss Priority (PLP) (**high** | **low**). By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Source Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
TCP	**syn**

Table 6: Action parameters

Action Condition	Description
Accept	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the **action** portion of the access list.
Counter	Name of a counter. To display counter information, use the **show policy access-lists counters** command on the Cisco IOS XE Catalyst SD-WAN device.
Drop	Discards the packet. This is the default action.

Description	Value or Range
Class	Specifies the name of a QoS class. It can also be defined with a **policy class-map** command.
Policer	Specifies the name of a policer defined with a **policy policer** command.
DSCP	Specifies the packet's DSCP value. The range is 0 through 63.

Description	Value or Range
Next Hop	Specifies the IPv4 address. It sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco vManage Release 20.5.1 and Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, **Use Default Route when Next Hop is not available** field is available next to Next Hop action parameter.

What to do next

Also see Deploy a configuration group.

Configure Route Policy Using a Configuration Group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

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

Step 2 Create and configure a Route Policy in a Transport & Management profile.

Table 7: Route Policy

Field	Description
Routing Sequence Name	Specifies the name of the routing sequence.
Protocol	Specifies the internet protocol. The options are IPv4, IPv6, or Both.

Field	Description
Condition	Specifies the routing condition. The options are: • **Address** • **AS Path List** • **Community List** • **Extended Community List** • **BGP Local Preference** • **Metric** • **Next Hop** • **OMP Tag** • **OSPF Tag**
Action Type	Specifies the action type. The options are **Accept** or **Reject**.
Accept Condition	Specifies the accept condition type. The options are: • **AS Path** • **Community** • **Local Preference** • **Metric** • **Metric Type** • **Next Hop** • **OMP Tag** • **Origin** • **OSPF Tag** • **Weight**

What to do next

Also see Deploy a configuration group.

Match Parameters

Access List Parameters

Access lists can match IP prefixes and fields in the IP headers.

In the CLI, you configure the match parameters with the **policy access-list sequence match** command.

Each sequence in an access-list must contain one match condition.

Match class in ACL is not supported. You can use rewrite policy to configure DSCP values.

For access lists, you can match these parameters:

Match Condition	Description
Class	Name of a class defined with a **policy class-map** command.
Destination Data Prefix	Name of a data-prefix-list list.
Destination Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
DSCP	Specifies the DSCP value. The range is 0 through 63.
Protocol	Specifies the internet protocol number. The range is 0 through 255.
ICMP Message	When you select a Protocol value as 1 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. When you select a Next Header value as 58 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1. For **`icmp-msg`** and **`icmp6-msg`** message types, refer to the ICMP Message Types/Codes and Corresponding Enumeration Values table in the Centralized chapter.
Packet Length	Specifies the length of the packet. The range can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).
Source Data Prefix	Specifies the name of a **data-prefix-list** list.
PLP	Specifies the Packet Loss Priority (PLP) (**high** | **low**). By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Source Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
TCP	**syn**

Route Policy Parameters

For route policies, you can match these parameters:

Match Condition	Description
Address	Specifies the name of a **Prefix-List** list.

Match Condition	Description
AS Path List	Specifies one or more BGP AS path lists. You can write each AS as a single number or as a regular expression. To specify more than one AS number in a single path, include the list in quotation marks (" "). To configure multiple AS numbers in a single list, include multiple **AS Path** options, specifying one AS path in each option.
Community List	List of one of more BGP communities. In **Community List**, you can specify: • *aa*:*nn*: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **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. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach 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.
Extended Community List	Specifies the list of one or more BGP extended communities. In **community**, you can specify: • **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.
BGP Local Preference	Specifies the BGP local preference number. The range is 0 through 4294967295.
Metric	Specifies the route metric value. The range is 0 through 4294967295.
Next Hop	Specifies the name of an IP prefix list.
OMP Tag	Specifies the OMP tag number. The range is 0 through 4294967295.
Origin	Specifies the BGP origin code. The optionss are: EGP (default), IGP, Incomplete. **Note** Match origin is available only for Cisco vEdge devices not on Cisco IOS XE Catalyst SD-WAN devices.
OSPF Tag	Specifies the OSPF tag number. The range is 0 through 4294967295.
Peer	Specifies the peer IP address.

Action parameters

Access List parameters

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify or police accepted packets.

In the CLI, you configure the action parameters with the **policy access-list sequence action** command.

Each sequence in an access list can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

Action Condition	Description
Accept	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the **action** portion of the access list.
Counter	Name of a counter. To display counter information, use the **show policy access-lists counters** command on the Cisco IOS XE Catalyst SD-WAN device.
Drop	Discards the packet. This is the default action.

For a packet that is accepted, the following actions can be configured:

Description	Value or Range
Class	Specifies the name of a QoS class. It can also be defined with a **policy class-map** command.
Policer	Specifies the name of a policer defined with a **policy policer** command.
DSCP	Specifies the packet's DSCP value. The range is 0 through 63.
Next Hop	Specifies the IPv4 address. It sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco vManage Release 20.5.1 and Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, **Use Default Route when Next Hop is not available** field is available next to Next Hop action parameter.

Route Policy parameters

Each sequence in a localized control policy can contain one action condition.

When a route matches the conditions in the match portion of a route policy, the route can be accepted or rejected:

For a packet that is accepted, the following actions can be configured:

Description	Value or Range
Aggregator	Set sthe AS number in which a BGP route aggregator is located and the IP address of the route aggregator. The range is 1 through 65535.

Description	Value or Range
As Path	Sets an AS number or a series of AS numbers to exclude from the AS path or to prepend to the AS path. The range is 1 through 65535.
Atomic Aggregate	Sets the BGP atomic aggregate attribute.
Community	Sets the BGP community value. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the Community **Additive** option field is available. Additive option appends the communities to the existing communities of the route.
Local Preference	Sets the BGP local preference. The range is 0 through 4294967295.
Metric	Sets the metric value. The range is 0 through 4294967295.
Metric Type	Sets the metric type. The options are type1 or type2.
Next Hop	Sets the IPv4 address. It sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco vManage Release 20.5.1 and Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, **Use Default Route when Next Hop is not available** field is available next to Next Hop action parameter.
OMP Tag	Sets the OMP tag for OSPF to use. The range is 0 through 4294967295.
Origin	Sets the BGP origin code. The options are: EGP (default), IGP, Incomplete.
Originator	Sets the IP address from which the route was learned.
OSPF Tag	Sets the OSPF tag value. The range is 0 through 4294967295.
Weight	Sets the BGP weight. The range is 0 through 4294967295.

Configure Localized Policy for IPv4 Using the CLI

Following are the high-level steps for configuring an access list using the CLI on Cisco IOS XE Catalyst SD-WAN devices:

1. Create lists of IP prefixes as needed:

```
Device(config)# policy lists data-prefix-list ipv4_prefix_list
Device(config-data-prefix-list-ipv4_prefix_list)
# ip-prefix 192.168.0.3/24
```

2. For QoS, configure the **class-map ios**:

```
Device(config)# class-map match-any class1
Device(config)#  match qos-group 1
class-map match-any class6
match qos-group 6
class-map match-any class7
match qos-group 7
```

```
class-map match-any class4
match qos-group 4
class-map match-any class5
match qos-group 5
class-map match-any class2
match qos-group 2
class-map match-any class3
match qos-group 3
class-map match-any class1
match qos-group 1
end
```

Note queue2 is optional here since we are using **class-default**.

3. For QoS, define rewrite rules to overwrite the DSCP field of a packet's outer IP header, if desired:

```
Device(config)# policy rewrite-rule rule1
Device(config-rewrite-rule-rule1)# class class1 low dscp 3
Device(config-rewrite-rule-rule1)# class class2 high dscp 4
Will be a table to map class-id → QoS-Group, QID, DSCP, Discard-Class
```

4. For QoS, map each forwarding class to an output queue, configure a QoS scheduler for each forwarding class, and group the QoS schedulers into a QoS map:

```
Device(config)# policy class-map class class1 queue 1
<0..7>[1]
```

5. For Qos map configuration, merge with interface shaping configuration, if shaping is configured.

   If shaping is not configured, you can apply the **policy-map** generated for the **qos-map**.

```
Device(config)# policy-map qos_map_for_data_policy
<name:string
Device(config-pmap)# class class1 name:string
Device(config-pmap-c)# bandwidth percentage
Device(config-pmap-c)# random-detect
```

6. Configure a WAN interface without a shaping configuration:

```
Device(config)# policy-map qos_map_for_data_policy name:string
Device(config-pmap)# class class1 name:string
Device(config-pmap-c)# bandwidth percentage
Device(config-pmap-c)# random-detect
```

7. Configure a WAN interface with a shaping configuration:

```
Device(config)# policy-map shaping_interface
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 100000000(rate-in-bps)
Device(config-pmap-c)# service-policy qos_map_for_data_policy
```

8. Associate a **service-policy** to a Cisco IOS XE Catalyst SD-WAN device:

```
Device(config)# sdwan interface GigabitEthernet 1
Device(config-if)# rewrite-rule rule1
Device(config-if)# service-policy output qos_map_for_data_policy
```

9. Define policing parameters:

```
Device(config)# policy policer policer_On_gige
Device(config-policer-policer_On_gige)# rate ?
Description: Bandwidth for 1g interfaces: <8..1000000000>bps; for 10g interfaces:
```

```
<8..10000000000>bps
Possible completions:<0..2^64-1>
Device(config-policer-policer_On_gige)# burst
Description: Burst rate, in bytes
Possible completions:<15000..10000000>
Device(config-policer-policer_On_gige)# exceed drop
```

10. Associate an access list set to policer:

```
Device(config)# policy access-list ipv4_acl
Device(config-access-list-ipv4_acl)# sequence 100
Device(config-sequence-100)# match dscp 10
Device(config-match)# exit
Device(config-sequence-100)# action accept
Device(config-sequence-100)# action count dscp_10_count
Device(config-sequence-100)# policer policer_On_gige
Device(config-sequence-100)# action drop
vm5(config-action)#
```

11. Associate an access list to a LAN or a WAN interface:

```
Device(config)# sdwan interface GigabitEthernet5
Device(config-interface-GigabitEthernet5)# access-list ipv4_acl
Device(config-interface-GigabitEthernet5)# commit
```

Configure Localized Policy for IPv6 Using the CLI

Following are the high-level steps for configuring an access list using the CLI:

1. Define policing parameters:

```
Device(config)# policy policer policer_On_gige
Device (config-policer-policer_On_gige)# rate ?
Description: Bandwidth for 1g interfaces: <8..1000000000>bps;for 10g interfaces:
<8..10000000000>bps Possible completions: <0..2^64-1>
Device(config-policer-policer_On_gige)# burst
Description: Burst rate, in bytes Possible completions:<15000..10000000>
Device(config-policer-policer_On_gige)# exceed drop
```

2. Create an access list instance:

```
Device (config)# policy ipv6 access-list ipv6_access_list
```

3. Create a series of match–action pair sequences:

```
Device(config-access-list-ipv6_access_list)# sequence 100
```

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

4. Define match parameters for packets:

```
Device(config-sequence-100)# match traffic-class 10
Device(config-match)# exit
```

5. Define actions to take when a match occurs:

```
Device(config-sequence-100)# action accept count traffic_class10_count
Device(config-sequence-100)# action drop
Device(config-sequence-100)# action accept class class1
Device(config-sequence-100)# action accept policer policer_On_gige
```

6. Create additional numbered sequences of match–action pairs within the access list, as needed.
7. If a packet does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching packets to be accepted, configure the default action for the access list:
8. Apply the access list to an interface:

```
Device(config)# sdwan interface GigabitEthernet5
Device(config-interface-GigabitEthernet5)
# ipv6 access-list ipv6_access_list in
Device(config-interface-GigabitEthernet5)
# commit
```

Applying the access list in the inbound direction (**in**) affects packets being received on the interface. Applying it in the outbound direction (**out**) affects packets being transmitted on the interface.

Localized Data Policy Configuration Examples

This topic provides some straightforward examples of configuring localized data policy to help you get an idea of how to use policy to influence traffic flow across the Cisco Catalyst SD-WAN domain. Localized data policy, also known as access lists, is configured directly on the local Cisco vEdge devices.

QoS

You can configure quality of service (QoS) to classify data packets and control how traffic flows out of and in to the interfaces on a Cisco vEdge device and on the interface queues. For examples of how to configure a QoS policy, see Forwarding and QoS Configuration Examples.

ICMP Message Example

This example displays the configuration for localized data policy for ICMP messages.

```
policy
access-list acl_1
 sequence 100
  match
   protocol 1
   icmp-msg administratively-prohibited
  !
  action accept
   count administratively-prohibited
  !
  !
```

Configure Localized Policy Using Cisco SD-WAN Manager

To configure localized policies, use the Cisco SD-WAN Manager policy configuration wizard. The wizard is a UI policy builder that consists of five windows 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 **Next** at the bottom of the window. To return to a component, click **Back** at the bottom of the window.

To configure localized policies using Cisco SD-WAN Manager, use the steps identified in the procedures that follow this section.

Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Select **Localized Policy**.
3. Click **Add Policy**.

The **Create Groups of Interest** page is displayed.

Configure groups of interest for localized policy

In **Create Groups of Interest**, create lists of groups to use in a localized policy:

In Create Groups of Interest, create new groups of list types as described in the following sections to use in a localized policy:

Configure As Path

1. In the group of interest list, click **AS Path**.
2. Click **New AS Path List**.
3. Enter a name for the list.
4. Enter the AS path, separating AS numbers with a comma.
5. Click **Add**.

   AS Path list specifies one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list separated by commas. To configure multiple AS paths in a single list, include multiple **as-path** options, specifying one AS path in each option.

Configure Community

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.

1. In the group of interest list, click **Community**.
2. Click **New Community List**.

3. Enter a name for the community list.
4. In the **Add Community** field, enter one or more data prefixes separated by commas in any of the following formats:
   - *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535.
   - **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.
5. Click **Add**.

Configure Data Prefix

1. In the **Group of Interest** list, click **Data Prefix**.
2. Click **New Data Prefix List**.
3. Enter a name for the list.
4. Enter one or more IP prefixes.
5. Click **Add**.

   A data prefix list specifies one or more IP prefixes. You can specify both unicast and multicast addresses. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

Configure Extended Community

1. In the group of interest list, click **Extended Community**.
2. Click **New Extended Community List**.
3. Enter a name for the list.
4. Enter the BGP extended community in the following formats:
   - **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address.
   - **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP

communities in a single list, include multiple **community** options, specifying one community in each option.

5. Click **Add**.

Configure Class Map

1. In the group of interest list, click **Class Map**.
2. Click **New Class List**.
3. Enter a name for the class.
4. Select a required queue from the **Queue** drop-down list.
5. Click **Save**.

Configure Policer

1. In the group of interest list, click **Policer**.
2. Click **New Policer List**.
3. Enter a name for the list.
4. In the **Burst (bps)** field, enter maximum traffic burst size. It can be a value from 15000 to 10000000 bytes.
5. In the **Exceed** field, select the action to take when the burst size or traffic rate is exceeded. Select **Drop** (the default) to set the packet loss priority (PLP) to low. Select **Remark** to set the PLP to high.
6. In the **Rate (bps)** field, enter the maximum traffic rate. It can be value from 8 through 2^{64} bps (8 through 100000000000).
7. Click **Add**.

Note When you define policers within localized policy lists, the device applies all defined policers to all localized policies. This happens because localized policies do not recognize which policers are referenced in templates. The device sends all policers through the Localized Policy CLI to ensure proper functionality.

Configure Prefix

1. In the group of interest list, click **Prefix**.
2. Click **New Prefix List**.
3. Enter a name for the list.
4. In the **Internet Protocol** field, click either **IPv4** or **IPv6**.
5. Under **Add Prefix**, enter the prefix for the list. (An example is displayed.) Optionally, click the green **Import** link on the right-hand side to import a prefix list.

6. Click **Add**.

Click **Next** to move to **Configure Forwarding Classes/QoS** in the wizard.

Configure Forwarding Classes/QoS

When you first open the **Forwarding Classes/QoS** page, **QoS Map** is selected by default:

QoS Map

To create a new QoS mapping:

1. In **QoS**, click the **Add QoS Map** drop-down.
2. Select **Create New**.
3. Enter a name and description for the QoS mapping.
4. Click **Add Queue**. The **Add Queue** popup appears.
5. Select the queue number from the **Queue** drop-down.
6. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types.
7. Enter the **Forwarding Class**.
8. Click **Save Queue**.

To import an existing QoS mapping:

1. In **QoS**, click the **Add QoS Map** drop-down.
2. Select **Import Existing**. The **Import Existing Application QoS Map Policy** popup displays.
3. Select a **QoS Map** policy.
4. Click **Import**.

To view or copy a QoS mapping or to remove the mapping from the localized policy, click **...** and select the desired action.

For hardware, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for low-latency queuing (LLQ), so any class that is mapped to queue 0 must be configured to use LLQ. The default scheduling method for all is weighted round-robin (WRR).

For Cisco IOS XE Catalyst SD-WAN devices, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for control traffic, and queues 1, 2, 3, 4, 5, 6 and 7 are available for data traffic. The scheduling method for all eight queues is WRR. LLQ is not supported.

To configure QoS parameters on a Cisco IOS XE Catalyst SD-WAN device, you must enable QoS scheduling and shaping. To enable QoS parameters for traffic that the Cisco IOS XE Catalyst SD-WAN device receives from transport-side interfaces:

To enable QoS parameters for traffic that the Cisco IOS XE Catalyst SD-WAN device receives from service-side interfaces:

Policy Rewrite

To configure policy rewrite rules for the QoS mapping:

1. In **Policy Rewrite**, 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 appears.
5. Select a class from the **Class** drop-down.
6. Select the priority (**Low** or **High**) from the Priority drop-down.

   Low priority is supported only for Cisco IOS XE Catalyst SD-WAN devices.
7. Enter the DSCP value (0 through 63) in the **DSCP** field.
8. Enter the class of service (CoS) value (0 through 7) in the **Layer 2 Class of Service** field.
9. Click **Save Rule**.

To import an existing rewrite rule:

1. In **QoS**, click the **Add Rewrite Policy** drop-down..
2. Select **Import Existing**. The **Import Existing Policy Rewrite** popup appears.
3. Select a rewrite rule policy.
4. Click **Import**.

Click **Next** to move to **Configure Access Lists** page.

Configure ACLs

1. In the **Configure Access Control Lists** page, configure ACLs.
2. To create a new ACL, click the **Add Access Control List Policy** drop-down. Select one from the following options:
   - **Add IPv4 ACL Policy**: Configure IPv4 ACL policy.
   - **Add IPv6 ACL Policy**: Configure IPv6 ACL policy.
   - **Import Existing**: Import existing ACL policy.
3. If you click **Add IPv4 ACL Policy**, the **Add IPv4 ACL Policy** page appears.

   or

   If you click **Add IPv6 ACL Policy**, the **Add IPv6 ACL Policy** page appears.
4. Enter a name and description for the ACL in the **ACL Policy** page.
5. In the left pane, click **Add ACL Sequence**. An **Access Control List** box is displayed in the left pane.
6. Double-click the **Access Control List** box, and type a name for the ACL.

7. In the right pane, click **Add Sequence Rule** to create a single sequence in the ACL. **Match** is selected by default.
8. Click a match condition.
9. On the left, enter the values for the match condition.
   a. 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 **...** next to the rule's name and select the desired option.

Default Action

If a packet being evaluated does not match any of the match conditions in a access list, a default action is applied to this packet. By default, the packet is dropped. 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**.
5. Click **Save Access Control List Policy**.

To configure **Device Access Policy**, see Device Access Policy.

Click **Next** to move to Configure Route Policy page.

Explicit and Implicit Access Lists

Access lists that you configure through localized data policy using the **policy access-list** command are called *explicit* ACLs. You can apply explicit ACLs to any interface in any VPN on the device.

The device's tunnel interfaces in VPN 0 also have *implicit ACLs*, which are also referred to as *services*. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through configuration, you can also enable other services. You configure and modify implicit ACLs with the **allow-service** command:

```
Device(config)# vpn 0
Device(config-vpn)# interface interface-name
Device(config-interface)# tunnel-interface
Device(config-tunnel-interface)# allow-service service-name
Device(config-tunnel-interface)# no allow-service service-name
```

On Cisco IOS XE Catalyst SD-WAN devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for Netconf, NTP, OSPF, SSHD, and STUN.



Note If a connection is initiated from a device, and if NAT is enabled on the device (for example, Direct Internet Access (DIA) is configured), return traffic is allowed by the NAT entry even if the implicit ACL has been configured as **no allow-service**. You can still block this traffic with an explicit ACL.

Do not confuse an explicit ACL with a Cisco IOS XE ACL. A Cisco IOS XE ACL does not interact with a Cisco Catalyst SD-WAN explicit and an implicit ACL and cannot override an implicit ACL or explicit ACL. Cisco IOS XE ACLs are executed later in the order of traffic processing operations.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (**allow-service** *service-name*) or deny (**no allow-service** *service-name*). Allowing a service in an implicit ACL is the same as specifying the **accept** action in an explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the **drop** action in an explicit ACL
- Whether, in an explicit ACL, the **accept** or **deny** action is configured in a policy sequence or in the default action.

The following table explains how traffic matching both an implicit and an explicit ACL is handled:

Table 8:

Implicit ACL	Explicit ACL: Sequence	Explicit ACL: Default	Result
Allow (accept)	Deny (drop)	—	Deny (drop)
Allow (accept)	—	Deny (drop)	Allow (accept)
Deny (drop)	Allow (accept)	—	Allow (accept)
Deny (drop)	—	Allow (accept)	Deny (drop)

Note During software upgrades, you can connect to a remote repository for downloading images and configure tunnel interface using **allow-service all** to implicitly permit all the services, or set up an explicit ACL to allow SCP packets. The following is a sample explicit ACL configuration:

```
policy
 access-list allow-remote-scp
  sequence 1
   match
    source-ip      10.0.0.0/32
    destination-ip 10.0.0.1/32
    source-port    22
    protocol       6
   !
   action accept
   !
  !
  default-action accept
 !
!
sdwan
 interface GigabitEthernet1
  tunnel-interface
   encapsulation ipsec
   color gold
   no allow-service dhcp
   no allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   no allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
  access-list allow-remote-scp in
 exit
```

Configure Route Policies

In **Configure Route Policies**, configure the routing policies:

1. In **Add Route Policy**, 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 policy. **Match** is selected by default.
6. Select a desired protocol from the **Protocol** drop-down list. The options are: IPv4, IPv6, or both.
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 route policy.
11. To rearrange match–action pairs in the route policy, in the right pane drag them to the desired position.
12. To remove a match–action pair from the route policy, 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 route policy, in the left pane drag the rules to the desired position.
15. To copy, delete, or rename the route policy sequence rule, in the left pane, click **...** next to the rule's name and select the desired option.
16. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
    a. Click **Default Action** in the left pane.
    b. Click the Pencil icon.
    c. Change the default action to **Accept**.
    d. Click **Save Match and Actions**.
17. Click **Save Route Policy**.
18. Click **Next** to move to **Policy Overview** page.

Match Parameters

Access List Parameters

Access lists can match IP prefixes and fields in the IP headers.

In the CLI, you configure the match parameters with the **policy access-list sequence match** command.

Each sequence in an access-list must contain one match condition.

Match class in ACL is not supported. You can use rewrite policy to configure DSCP values.

For access lists, you can match these parameters:

Match Condition	Description
Class	Name of a class defined with a **policy class-map** command.
Destination Data Prefix	Name of a data-prefix-list list.
Destination Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
DSCP	Specifies the DSCP value. The range is 0 through 63.

Match Condition	Description
Protocol	Specifies the internet protocol number. The range is 0 through 255.
ICMP Message	When you select a Protocol value as 1 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. When you select a Next Header value as 58 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1. For `icmp-msg` and `icmp6-msg` message types, refer to the ICMP Message Types/Codes and Corresponding Enumeration Values table in the Centralized chapter.
Packet Length	Specifies the length of the packet. The range can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).
Source Data Prefix	Specifies the name of a **data-prefix-list** list.
PLP	Specifies the Packet Loss Priority (PLP) (**high** | **low**). By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Source Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
TCP	**syn**

Route Policy Parameters

For route policies, you can match these parameters:

Match Condition	Description
Address	Specifies the name of a **Prefix-List** list.
AS Path List	Specifies one or more BGP AS path lists. You can write each AS as a single number or as a regular expression. To specify more than one AS number in a single path, include the list in quotation marks (" "). To configure multiple AS numbers in a single list, include multiple **AS Path** options, specifying one AS path in each option.

Match Condition	Description
Community List	List of one of more BGP communities. In **Community List**, you can specify: • *aa*:*nn*: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **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. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach 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.
Extended Community List	Specifies the list of one or more BGP extended communities. In **community**, you can specify: • **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.
BGP Local Preference	Specifies the BGP local preference number. The range is 0 through 4294967295.
Metric	Specifies the route metric value. The range is 0 through 4294967295.
Next Hop	Specifies the name of an IP prefix list.
OMP Tag	Specifies the OMP tag number. The range is 0 through 4294967295.
Origin	Specifies the BGP origin code. The optionss are: EGP (default), IGP, Incomplete. **Note** Match origin is available only for Cisco vEdge devices not on Cisco IOS XE Catalyst SD-WAN devices.
OSPF Tag	Specifies the OSPF tag number. The range is 0 through 4294967295.
Peer	Specifies the peer IP address.

Action parameters

Access List parameters

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify or police accepted packets.

In the CLI, you configure the action parameters with the **policy access-list sequence action** command.

Each sequence in an access list can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

Action Condition	Description
Accept	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the **action** portion of the access list.
Counter	Name of a counter. To display counter information, use the **show policy access-lists counters** command on the Cisco IOS XE Catalyst SD-WAN device.
Drop	Discards the packet. This is the default action.

For a packet that is accepted, the following actions can be configured:

Description	Value or Range
Class	Specifies the name of a QoS class. It can also be defined with a **policy class-map** command.
Policer	Specifies the name of a policer defined with a **policy policer** command.
DSCP	Specifies the packet's DSCP value. The range is 0 through 63.
Next Hop	Specifies the IPv4 address. It sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco vManage Release 20.5.1 and Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, **Use Default Route when Next Hop is not available** field is available next to Next Hop action parameter.

Route Policy parameters

Each sequence in a localized control policy can contain one action condition.

When a route matches the conditions in the match portion of a route policy, the route can be accepted or rejected:

For a packet that is accepted, the following actions can be configured:

Description	Value or Range
Aggregator	Set sthe AS number in which a BGP route aggregator is located and the IP address of the route aggregator. The range is 1 through 65535.

Description	Value or Range
As Path	Sets an AS number or a series of AS numbers to exclude from the AS path or to prepend to the AS path. The range is 1 through 65535.
Atomic Aggregate	Sets the BGP atomic aggregate attribute.
Community	Sets the BGP community value. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the Community **Additive** option field is available. Additive option appends the communities to the existing communities of the route.
Local Preference	Sets the BGP local preference. The range is 0 through 4294967295.
Metric	Sets the metric value. The range is 0 through 4294967295.
Metric Type	Sets the metric type. The options are type1 or type2.
Next Hop	Sets the IPv4 address. It sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco vManage Release 20.5.1 and Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, **Use Default Route when Next Hop is not available** field is available next to Next Hop action parameter.
OMP Tag	Sets the OMP tag for OSPF to use. The range is 0 through 4294967295.
Origin	Sets the BGP origin code. The options are: EGP (default), IGP, Incomplete.
Originator	Sets the IP address from which the route was learned.
OSPF Tag	Sets the OSPF tag value. The range is 0 through 4294967295.
Weight	Sets the BGP weight. The range is 0 through 4294967295.

Configure Policy Settings

In **Policy Overview**, configure the policy settings:

1. In the **Enter name and description for your localized master policy** pane, enter name and description for the policy.
2. In the **Policy Settings** pane, select the policy application checkboxes that you want to confirgure. The options are:
   - **Netflow**: Perform traffic flow monitoring on IPv4 traffic.
   - **Netflow IPv6**: Perform traffic flow monitoring on IPv6 traffic.
   - **Application**: Track and monitor IPv4 applications.
   - **Application IPv6**: Track and monitor IPv6 applications.
   - **Cloud QoS**: Enable QoS scheduling.

- **Cloud QoS Service Side**: Enable QoS scheduling on the service side.
- **Implicit ACL Logging**: Log the headers of all the packets that are dropped because they do not match a service perform traffic flow monitoring.

3. 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.

4. Click **Preview** to view the full policy in CLI format.
5. Click **Save Policy**.

Apply Localized Policy in a Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. If you are creating a new device template:
   a. Click **Device Templates**.



Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Template** is titled as **Device**.

   b. From the **Create Template** drop-down, select **From Feature Template**.
   c. From the **Device Model** drop-down, select one of the Cisco IOS XE Catalyst SD-WAN devices.
   d. In the **Template Name** field, enter a name for the device template. 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.
   e. In the **Description** field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
   f. Continue with Step 4.
3. If you are editing an existing device template:
   a. Click **Device Templates**, and for the desired template, click **...** and select **Edit**.



Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Template** is titled as **Device**.

   b. Click **Additional Templates**. The screen scrolls to the **Additional Templates** section.
   c. From the **Policy** drop-down, select the name of a policy that you have configured.
4. Click **Additional Templates** located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.
5. From the **Policy** drop-down, select the name of the policy you configured in the above procedure.

6. Click **Create** (for a new template) or **Update** (for an existing template).

Activate a Localized Policy

1. Click **Localized Policy**, and select a policy.
2. For the desired policy, click **...** and select **Activate**.
3. In the **Activate Policy** popup, click **Activate** to push the policy to all reachable Cisco SD-WAN Controllers in the network.
4. Click **OK** to confirm activation of the policy on all Cisco SD-WAN Controllers.
5. To deactivate the localized policy, select =, and then select a policy.
6. For the desired policy, click **...** and select **Deactivate**.
7. In the **Deactivate Policy** popup, click **Deactivate** to confirm that you want to remove the policy from all reachable Cisco SD-WAN Controllers.

View Localized Policies

To view localized policies:

1. Click **Localized Policy**, and select a policy.
2. For a policy created using the UI policy builder or using the CLI, click **...** and select **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 **...** and select **Preview**. This policy is displayed in text format.

Copy, Edit, and Delete Policies

To copy a policy:

1. Click **Localized Policy**, and select a policy.
2. For the desired policy, click **...** and select **Copy**.
3. In the Policy Copy popup window, enter the policy name and a description of the policy.



Note Starting with the Cisco IOS XE Release 17.2, 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.

4. Click **Copy**.

To edit policies created using the Cisco SD-WAN Manager policy configuration wizard:

1. For the desired policy, click **...** and select **Edit**.
2. Edit the policy as needed.
3. Click **Save Policy Changes**.

To edit polices created using the CLI method:

1. From the **Custom Options** drop-down, under Localized Policy, select **CLI Policy**.
2. For the desired policy, click **...** and select **Edit**.
3. Edit the policy as needed.
4. Click **Update**.

To delete policies:

1. Click **Localized Policy**, and select a policy.
2. For the desired policy, click **...** and select **Delete**.
3. Click **OK** to confirm deletion of the policy.

QoS For Router Generated Cisco SD-WAN Manager Traffic

Table 9: Feature History

Feature Name	Release Information	Description
QoS for Router Generated Cisco SD-WAN Manager Traffic	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature helps you to prioritize or queue router-generated Cisco SD-WAN Manager traffic based on your specific requirements. Use QoS policies and class maps to route Cisco SD-WAN Manager traffic through a queue of your choice.

Information About QoS For Router-Generated Cisco SD-WAN Manager Traffic

Quality of Service (QoS) is a technique used to manage and prioritize network traffic to ensure that certain types of traffic are given priority over others. QoS is particularly important for router-generated Cisco SD-WAN Manager traffic, which is used for managing and monitoring network devices. For more information see, Forwarding and QoS.

You can prioritize or queue router-generated traffic based on your specific requirements. The prioritization can be achieved through the use of QoS policies and class maps.

Use the following steps to put router-generated traffic into the queue of your choice:

1. Define a class map using a CLI template: Identifies the type of traffic you want to prioritize. In this case, you create a class map to identify the router-generated traffic to queue.
2. Define a policy map using a CLI template: Defines the actions that you want to take on the traffic identified in the class map. Create a policy map that assigns a priority or places the router-generated traffic into a specific queue.

Benefits of Qos For Router Generated Cisco SD-WAN Manager Traffic

- Improved network performance: By prioritizing critical router-generated traffic over less important traffic, ensure that your network management functions operate smoothly and monitor and control network devices effectively.
- Better user experience: Queing router-generated traffic helps preventing congestion on the network and ensure that user-generated traffic does not negatively impact network management functions. The queueing can result in a better user experience.
- Increased network availability: Reduces the risk of network downtime caused by network management issues. This improves network availability and reduce the impact of any network issues on your business operations.

- Simplified network management: Simplifies network management and reduces the need for manual intervention. The simplification can save time and reduce the risk of human error.
- Efficient use of network resources: QoS policies and class maps allow you to allocate network resources efficiently, ensuring that critical router-generated traffic flow efficiently, minimizing the impact on other network traffic.

Restrictions For QoS For Router Generated Cisco SD-WAN Manager Traffic

- The QoS for router generated Cisco SD-WAN Manager traffic feature is supported only on Cisco IOS XE Catalyst SD-WAN devices.
- Configuring QoS for router generated Cisco SD-WAN Manager traffic is possible only using a CLI template.
- With this feature, you can prioritize, using a queue, only for the traffic that devices generate forCisco SD-WAN Manager. Other data and management plane traffic continue to take Queue 0 by default.

Configure QoS for router-generated Cisco SD-WAN Manager traffic using a CLI template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

Define a class map and map to a queue number

1. Using a localized policy, define a class-map and map the class-map to a queue number :

   policy class-map class *Queue_1* **queue** *2*
2. Commit the changes.

Here's the complete configuration example for defining a class map and mapping it to a queue number:

```
config-t
policy class-map class Queue_1 queue 2
!
```

Enable QoS for router-generated Cisco SD-WAN Manager traffic

This section provides example CLI configurations to enable QoS for router generated Cisco SD-WAN Manager traffic:

1. Enter config-policy mode:

   policy

2. Use a forwarding class and use the class map that you mapped to a queue that you want to prioritize:

   vmanage-traffic-forwarding-class *queue_name*
3. Commit the changes.

   QoS for router generated Cisco SD-WAN Manager traffic is enabled.

Here's the complete configuration example for enabling Qos for router generated Cisco SD-WAN Manager traffic:

```
config-t
policy
vmanage-traffic-forwarding-class Queue_1
!
```

Verify QoS for Router Generated Cisco SD-WAN Manager Traffic Using CLI

The following is sample output from the **show policy-map interface** command using the **GigabitEthernet 1** keyword:

```
Device# show policy-map interface GigabitEthernet 1

  Service-policy output: shape_GigabitEthernet1

    Class-map: class-default (match-any)
      8619 packets, 5056404 bytes
      5 minute offered rate 113000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 8619/5056404
      shape (average) cir 4200000, bc 16800, be 16800
      target shape rate 4200000

      Service-policy : qosmap

        queue stats for all priority classes:
          Queueing
          priority level 1
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 565/95064

        Class-map: Queue0 (match-any)
          565 packets, 95064 bytes
          5 minute offered rate 4000 bps, drop rate 0000 bps
          Match: qos-group 0
          police:
              rate 30 %
              rate 1260000 bps, burst 39375 bytes
            conformed 565 packets, 95064 bytes; actions:
              transmit
            exceeded 0 packets, 0 bytes; actions:
              drop
            conformed 4000 bps, exceeded 0000 bps
          Priority: Strict, b/w exceed drops: 0
```

```
  Priority Level: 1

Class-map: Queue_1 (match-any)
  8050 packets, 4961100 bytes                                  ------------------->
  5 minute offered rate 111000 bps, drop rate 0000 bps
  Match: qos-group 1
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 8050/4961100
  bandwidth remaining ratio 10

Class-map: Queue_2 (match-any)
  4 packets, 240 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 2
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 4/240
  bandwidth remaining ratio 10
```

In this example, **Class-map** for the respective queues displays the number, size, and the rate of packet transfer from the router to the destination. You can see a change in the Queue_1 and keep track of the packet transfer.

Troubleshooting QoS For Router Generated Cisco SD-WAN Manager Traffic

Problem

Unable to commit changes using the CLI

Possible Causes

There could be typos or incorrect queue names entered while committing the changes. For example, if you type queuee 2 instead of queue 2, the following error is displayed: Aborted: illegal reference 'policy vmanage-traffic-forwarding-class'

Solution

Enter the right queue name that you want the Cisco SD-WAN Manager traffic from the router to flow through.