Localized Policy

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

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.

Overview of Localized Policies

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.

Types of Localized Policies

Localized Control Policy

Control policy operates on the control plane traffic in the Cisco 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 vEdge 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 vEdge 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 vEdge 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 Catalyst SD-WAN overlay network and affects how data traffic is sent among the Cisco vEdge 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 vEdge device.

Localized data policy, so called because it is provisioned on the local Cisco vEdge 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 and provision packet mirroring.

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 vEdge 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 vEdge 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.

Mirror Data Packets

Once packets are classified, you can configure access lists to send a copy of data packets seen on a Cisco vEdge device to a specified destination on another network device. The Cisco vEdge devices support 1:1 mirroring; that is, a copy of every packet is sent to the alternate destination.

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 Mirror

1. In the group of interest list, click **Mirror**.
2. Click **New Mirror List**. The Mirror List popup displays.
3. Enter a name for the list.

4. In the **Remote Destination IP** field, enter the IP address of the destination for which to mirror the packets.
5. In the **Source IP** field, enter the IP address of the source of the packets to mirror.
6. Click **Add**.

   To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets. Mirroring applies to unicast traffic only. It does not apply to multicast traffic.

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**.

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 vEdge 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 vEdge device, you must enable QoS scheduling and shaping. To enable QoS parameters for traffic that the Cisco vEdge device receives from transport-side interfaces:

To enable QoS parameters for traffic that the Cisco vEdge 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.
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 vEdge 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 BGP, 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.

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 1:

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)

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.
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 SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1.
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.

Match Condition	Description
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.
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.

Match Condition	Description
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.
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, mirror, 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 vEdge 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.
Mirror List	Specifies the name of mirror . It is defined with a **policy mirror** 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 SD-WAN Release 20.5.1, **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.
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.
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 SD-WAN Release 20.5.1, **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 vEdge 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 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.

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.

Configure Localized Policy for IPv4 Using the CLI

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

1. Create lists of IP prefixes as needed:

```
vEdge(config)# policy
vEdge(config-policy)# lists data-prefix-list list-name
vEdge(config-data-prefix-list)# ip-prefix prefix/length
```

2. If you configure a logging action, configure how often to log packets to the syslog files:

```
vEdge(config)# policy log-frequency number
```

3. 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:

```
vEdge(config)# policy class-map
vEdge(config-class-map)# class class-name queue number
vEdge(config)# policy qos-scheduler scheduler-name
vEdge(config-qos-scheduler)# class class-name
vEdge(config-qos-scheduler)# bandwidth-percent percentage
vEdge(config-qos-scheduler)# buffer-percent percentage
vEdge(config-qos-scheduler)# drops drop-type
vEdge(config-qos-scheduler)# scheduling type
```

```
vEdge(config)# policy qos-map map-name qos-scheduler scheduler-name
```

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

```
vEdge(config)# policy rewrite-rule rule-name
vEdge(config-rewrite-rule)# class class-name loss-priority
dscp dscp-value layer-2-cos number
```

class-name is one of the classes defined under a **qos-scheduler** command.

5. Define mirroring parameters (for unicast traffic only):

```
vEdge(config)# policy mirror mirror-name
vEdge(config-mirror)# remote-dest ip-address source ip-address
```

6. Define policing parameters:

```
vEdge(config)# policy policer policer-name
vEdgeconfig-policer)# rate bandwidth
vEdge(config-policer)# burst bytes
vEdge(config-policer)# exceed action
```

7. Create an access list instance:

```
vEdge(config)# policy access-list list-name
```

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

```
vEdge(config-access-list)# sequence number
vEdge(config-sequence)#
```

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).

9. Define match parameters for packets:

```
vEdge(config-sequence-number)
# match match-parameter
```

10. Define actions to take when a match occurs:

```
vEdge(config-sequence)# action drop
vEdge(config-sequence)# action count counter-name
vEdge(config-sequence)# action log
vEdge(config-sequence)# action accept class class-name
```

```
vEdge(config-sequence)# action accept mirror mirror-name
vEdge(config-sequence)# action accept policer policer-name
vEdge(config-sequence)# action accept set dscp value
vEdge(config-sequence)# action accept set next-hop ipv4-address
```

11. Create additional numbered sequences of match–action pairs within the access list, as needed.
12. 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:

    ```
    vEdge(config-policy-name)
    # default-action accept
    ```

13. Apply the access list to an interface:

    ```
    vEdge(config)# vpn vpn-id interface interface-name
    vEdge(config-interface)# access-list list-name (in | out)
    ```

    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. For QoS, apply a DSCP rewrite rule to the same egress interface:

    ```
    vEdge(config)# vpn vpn-id interface interface-name rewrite-rule rule-name
    ```

14. You can apply a policer directly to an interface, which has the effect of policing all packets transiting the interface, rather than policing only the selected packets that match the access list. You can apply the policer to either inbound or outbound packets:

    ```
    vEdge(config)# vpn vpn-id  interface interface-name
    vEdge(config-interface)# policer policer-name (in | out)
    ```

Configure Localized Policy for IPv6 Using the CLI

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

1. Define mirroring parameters (for unicast traffic only):

   ```
   vEdge(config)# policy mirror mirror-name
   vEdge(config-mirror)# remote-dest ip-address source ip-address
   ```

2. Define policing parameters:

   ```
   vEdge(config)# policy policer policer-name
   vEdge(config-policer)# rate bandwidth
   vEdge(config-policer)# burst bytes
   vEdge(config-policer)# exceed action
   ```

3. Create an access list instance:

   ```
   vEdge(config)# policy ipv6 access-list list-name
   ```

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

   ```
   vEdge(config-ipv6-access-list)# sequence number
   vEdge(config-sequence)#
   ```

   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).

5. Define match parameters for packets:

```
vEdge(config-sequence-number)# match match-parameter
```

6. Define actions to take when a match occurs:

```
vEdge(config-sequence)# action drop
vEdge(config-sequence)# action count counter-name
vEdge(config-sequence)# action log
vEdge(config-sequence)# action accept class class-name
vEdge(config-sequence)# action accept mirror mirror-name
vEdge(config-sequence)# action accept policer policer-name
```

7. Create additional numbered sequences of match–action pairs within the access list, as needed.

8. 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:

```
vEdge(config-policy-name)# default-action accept
```

9. Apply the access list to an interface:

```
vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# ipv6 access-list list-name (in | out)
```

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.

Mirroring Example

This example illustrates how to configure a mirror instance to automatically send a copy of certain types of data packet to a specified destination for analysis. After you configure the mirror instance, include it in an access list. Here, "mirror-m1" is configured with the host at source address 10.20.23.16 and destination host at 10.2.2.11. The mirror instance is then included in the access list "acl2," which is configured so that data packets originating from the host at source address 10.20.24.17 and going to the destination host at 10.20.25.18 are mirrored to the destination host at 10.2.2.11 with the source address of the originating host as 10.20.23.16.

```
policy
 mirror m1
  remote-dest 10.2.2.11 source 10.20.23.16
 !
!

vm5# show running-config policy access-list acl2
policy
 access-list acl2
  sequence 1
   match
```

```
    source-ip      10.20.24.17/32
    destination-ip 10.20.25.18/32
   !
   action accept
    mirror m1
   !
  !
  default-action drop
 !
!
```

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
  !
  !
```

QoS For Router Generated Cisco SD-WAN Manager Traffic

Table 2: 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-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-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.