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 vManage or the CLI.

- Overview of Localized Policies, on page 1
- Components of Localized Policies, on page 3
- Configure Localized Policy Using Cisco vManage , on page 12
- Configure Localized Policy for IPv4 Using the CLI, on page 19
- Configure Localized Policy for IPv6 Using the CLI, on page 21
- Localized Data Policy Configuration Examples, on page 22

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 vManage 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 SD-WAN overlay network and affects how data traffic is sent among the Cisco vEdge devices in the network. The Cisco 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.

Components of Localized Policies

Components of Access Lists

Following are the structural components required to configure access lists.

```
policy
   implicit-acl-logging
   log-frequency number
   mirror mirror-name
      remote-dest ip-address source ip-address
   policer policer-name
      rate bandwidth
      burst bytes
      exceed action
policy ipv6
   access-list list-name
      sequence number
         match match-parameters
         action
            drop
            user counter-name
            log
            accept
               class class-name
               mirror mirror-name
               policer policer-name
     default-action (accept | drop)
vpn vpn-id
   interface interface-name
      ipv6 access-list list-name (in | out)
```

Lists

The localized policy uses the following types of lists to group related items. You configure lists under the **policy lists** command hierarchy on Cisco vEdge devices.

In Cisco vManage, you can configure lists from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Create Groups of Interest**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Lists** > **Data Prefix**

List Type	Description	CLI Command
AS paths	List of 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 in quotation marks (" "). To configure multiple AS paths in a single list, include multiple **as-path** options, specifying one AS path in each option.	**as-path-list** *list-name* **as-path** *path-list*

List Type	Description	CLI Command
Communities	List of one or more communities. In **community**, you can specify: • *aa*:*nn*: Autonomous system 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.	**community-list** *list-name* **community** [*aa*:*nn* | **internet** | **local-as** | **no-advertise** | **no-export**]
Data prefixes	List of 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.	**data-prefix-list** *list-name* **ip-prefix** *prefix/length*
Extended communities	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 autonomous system 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 autonomous system 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.	**ext-community-list** *list-name* **community** [**rt** (*aa*:*nn* | *ip-address*) | **soo** (*aa*:*nn* | *ip-address*)]
Class Map	List of one or more classes.	**class** *class map*
Mirror	List of one or more mirror parameters. 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.	**mirror** *mirror-name* **remote-dest** *ip-address* **source** *ip-address*

List Type	Description	CLI Command
Policier	List of one or more policier parameters, such as burst, exceed, and rate. *rate* is the maximum traffic rate. It can be a value from 0 through 264 – 1 bits per second. *burst* is the maximum traffic burst size. It can be a value from 15000 to 1000000 bytes. *exceed* is the action to take when the burst size or traffic rate is exceeded. *action* can be *drop* (the default) or *remark*. The *drop* action is equivalent to setting the packet loss priority (PLP) bit to low. The *remark* action sets the PLP bit to high. In a centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the *match plp* option.	**policer** *policer-name* **rate** *bandwidth* **burst** *bytes* **exceed** *action*
Prefixes	List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. Specify the IP prefixes as follows: • *prefix/length*—Exactly match a single prefix–length pair. • **0.0.0.0/0**—Match any prefix–length pair. • **0.0.0.0/0 le** *length*—Match any IP prefix whose length is less than or equal to *length*. For example, **ip-prefix 0.0.0.0/0 le 16** matches all IP prefixes with lengths from /1 through /16. • **0.0.0.0/0 ge** *length*—Match any IP prefix whose length is greater than or equal to *length*. For example, **ip-prefix 0.0.0.0 ge 25** matches all IP prefixes with lengths from /25 through /32. • **0.0.0.0/0 ge** *length1* **le** *length2*, or **0.0.0.0 le** *length2* **ge** *length1*—Match any IP prefix whose length is greater than or equal to *length1* and less than or equal to *length2*. For example, **ip-prefix 0.0.0.0/0 ge 20 le 24** matches all /20, /21, /22, /23, and /24 prefixes. Also, **ip-prefix 0.0.0.0/0 le 24 ge 20** matches the same prefixes. If *length1* and *length2* are the same, a single IP prefix length is matched. For example, **ip-prefix 0.0.0.0/0 ge 24 le 24** matches only /24 prefixes.	**prefix-list** *list-name* **ip-prefix** *prefix/length*

QoS Parameters

In Cisco vManage, you can configure QoS parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configuring Forwarding Classes/QoS**

  or

- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Configuring Forwarding Classes/QoS**

This section explains how to configure QoS parameters from the CLI.

To configure QoS parameters on a device, first define a classification. In Cisco vManage:

```
Device(config)# policy class-map class class-name queue number
```

class-name is the name of the class. It can be a text string from 1 through 32 characters long.

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:

```
Device(config)# policy cloud-qos
```

To enable QoS parameters for traffic that the Cisco vEdge device receives from service-side interfaces:

```
Device(config)# policy cloud-qos-service-side
```

Next, configure scheduling:

```
Device(config)# policy qos-scheduler scheduler-name
Device(config-qos-scheduler)# class percentage
Device(config-qos-scheduler)# buffer-percent percentage
Device(config-qos-scheduler)# drops (red-drop | tail-drop)
Device(config-qos-scheduler)# scheduling (llq | wrr)
```

scheduler-name is the name of the QoS scheduler. It can be a text string from 1 through 32 characters long.

class-name is the name of the forwarding class and can be a text string from 1 through 32 characters long. The common class names correspond to the per-hop behaviors AF (assured forwarding), BE (best effort), and EF (expedited forwarding).

The bandwidth percentage is the percentage of the interface's bandwidth to allocate to the forwarding class. The sum of the bandwidth on all forwarding classes on an interface should not exceed 100 percent.

The buffer percentage is the percentage of the interface's buffering capacity to allocate to the forwarding class. The sum of the buffering capacity of all forwarding classes on an interface should not exceed 100 percent.

Packets that exceed the bandwidth or buffer percentage are dropped either randomly, using random early detection (**red-drop**), or from the end of the queue (**tail-drop**). Low-latency queuing (LLQ) cannot use random early detection.

The algorithm to schedule interface queues can be either low-latency queuing (**llq**) or weighted round-robin (**wrr**).

Then, assign the scheduler to a QoS map:

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

map-name is the name of the QoS map, and *scheduler-name* is the name of the scheduler you configured above. Each name can be a text string from 1 through 32 characters long.

Finally, to configure a rewrite rule to overwrite the DSCP field of a packet's outer IP header:

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

rule-name is the name of the rewrite rule. It can be a text string from 1 through 32 characters long.

class-name is the name of a class you configured with the **qos-scheduler class** command. The packet loss priority (PLP) can be either **high** or **low**. To have a DSCP value overwrite the DSCP field of the packet's outer IP header, set a value from 0 through 63. To include an 802.1p marking in the packet, specify a number from 0 through 7.

Sequences

An access list contains sequences of match–action pairs. The sequences are numbered to set the order in which a packet is analyzed by the match–action pairs in the access lists.

In Cisco vManage, you configure sequences from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Add Access Control List Policy** > **Add ACL Sequence**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Add Access Control List Policy** > **Add ACL Sequence**

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

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

Match Parameters

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

In the Cisco vManage, you configure match parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Add Access Control List Policy** > **Add ACL Sequence** > **Add Sequence Rule** > **Match**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Add Access Control List Policy** > **Add ACL Sequence** > **Add Sequence Rule** > **Match**

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.

For access lists, you can match these parameters:

Description	**Value or Range**	**CLI Command**
Classification map	Name of a class defined with a **policy class-map** command.	**class** *class-name*
Group of destination prefixes	Name of a **data-prefix-list** list.	**destination-data-prefix-list** *list-name*
Individual destination prefix	IP prefix and prefix length	**destination-ip** *prefix/length*
Destination port number .	0 through 65535; specify 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 [-])	**destination-port** *number*
DSCP value	0 through 63	**dscp** *number*
Internet Protocol number	0 through 255	**protocol** *number*

Description	Value or Range	CLI Command
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.	For `icmp-msg` and `icmp6-msg` message types, refer to the ICMP Message Types/Codes and Corresponding Enumeration Values table n the Centralized chapter.	`icmp-msg` *value* `icmp6-msg` *value*
Packet length	Length of the packet. *number* 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 [-])	**packet-length** *number*
Group of source prefixes	Name of a **data-prefix-list** list.	**source-data-prefix-list** *list-name*
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.	**plp**
Individual source prefix	IP prefix and prefix length	**source-ip** *prefix*/*length*
Source port number .	0 through 65535; specify 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 [-])	**source-port** *address*
TCP flag	**syn**	**tcp** *flag*

Action 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 Cisco vManage, you configure match parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Add Access Control List Policy** > **Add ACL Sequence** > **Add Sequence Rule** > **Action**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Add Access Control List Policy** > **Add ACL Sequence** > **Add Sequence Rule** > **Action**

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:

Description	Value or Range	CLI Command
Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the **action** portion of the access list.	—	**accept**
Count the accepted or dropped packets.	Name of a counter. To display counter information, use the **show policy access-lists counters** command on the Cisco vEdge device.	**count** *counter-name*
Discard the packet. This is the default action.	—	**drop**
Log the packet headers into the messages and vsyslog system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.	To display logging information, use the **show app log flow-all** , **show app log flows**, and **show log** commands on the Cisco vEdge device.	**log**

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

Description	Value or Range	CLI Command
Classify the packet.	Name of a QoS class defined with a **policy class-map** command.	**class** *class-name*
Mirror the packet.	Name of mirror defined with a **policy mirror** command.	**mirror** *mirror-name*
Police the packet.	Name of a policer defined with a **policy policer** command.	**policer** *policer-name*
Packet's DSCP value.	0 through 63.	**set dscp** *value*
Next-hop address.	IPv4 address.	**set next-hop** *ipv4-address*

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.

In Cisco vManage, you modify the default action from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Default Action**

- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Default Action**

In the CLI, you modify this behavior with the **access-list default-action accept** command.

Apply Access Lists

For an access list to take effect, you must apply it to an interface.

In Cisco vManage, you apply the access list from **Configuration** > **Templates**. You can any of the interface feature configuration templates. For example, VPN interface cellular, ethernet, GRE, PPP and so on.

In the CLI, you apply the access list as follows:

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

Applying the policy in the inbound direction (**in**) affects prefixes being received on the interface. Applying it in the outbound direction (**out**) affects prefixes being transmitted on the interface.

For an access list that applies QoS classification, apply any DSCP rewrite rules to the same interface to which you apply the access list:

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

Note that you can also 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:

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

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)

Logging Parameters

If you configure a logging action in a data policy, by default, the Cisco vEdge devices log all data packet headers to a syslog file. You can log only a sample of the data packet headers.

In Cisco vManage, you configure how often to log packet headers from:

Configuration > **Policies** > **Localized Policy** > **Add Policy** > **Policy Overview** > **Log Frequency field**

In the CLI, you configure this as follows:

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

number specifies how often to to log packet headers. The default value is 1000. *number* can be an integer, and the software rounds the value down to the nearest power of 2. So for example, with the default value of 1000, the logging frequency is rounded down to 512, so every 512th packet is logged.

You can log the headers of all packets that are dropped because they do not match a service configured with an Allow Service configuration or an **allow-service** command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

In Cisco vManage, you configure this logging from:

Configuration > **Policies** > **Localized Policy** > **Add Policy** > **Policy Overview** > **Implicit ACL Logging field**

In the CLI, you do this as follows:

```
vEdge(config)# policy implicit-acl-logging
```

When you enable implicit ACL logging, by default, the headers of all dropped packets are logged. It is recommended that you configure a limit to the number of packets logged in the Log Frequency field or with the **log-frequency** command.

Configure Localized Policy Using Cisco vManage

To configure localized policies, use the Cisco vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens to configure and modify the following localized policy components:

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

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

Start the Policy Configuration Wizard

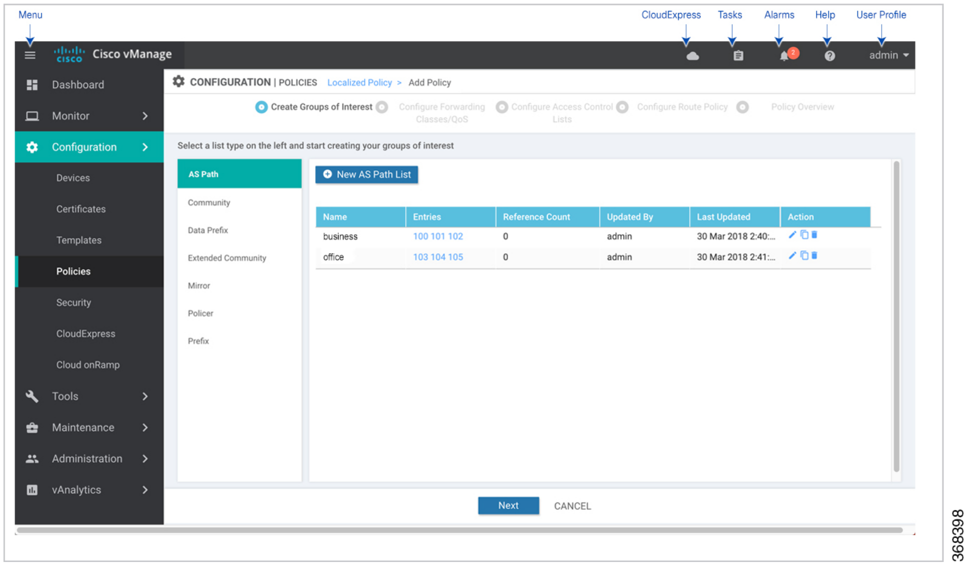
To start the policy configuration wizard:

1. In Cisco vManage, select the **Configuration** > **Policies** screen.
2. Select the **Localized Policy** tab.
3. Click **Add Policy**.

The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

Configure Groups of Interest

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



Select a list type on the left and start creating your groups of interest

Name	Entries	Reference Count	Updated By	Last Updated	Action
business	100 101 102	0	admin	30 Mar 2018 2:40:...	
office	103 104 105	0	admin	30 Mar 2018 2:41:...	

1. Create new lists, as described in the following table:

Table 2:

List Type	Procedure
AS Path	1. In the left bar, 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**.
Community	1. In the left bar, click **Community**. 2. Click **New Community List**. 3. Enter a name for the list. 4. Enter the BGP community in the format *aa*:*nn* or as the string **internet**, **local-as**, **no-advertise**, or **no-export**, separating multiple items with a comma. For *aa*, enter a 2-byte AS number, and for *nn*, enter a 2-byte network number. 5. Click **Add**.
Data Prefix	1. In the left bar, 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**.

List Type	Procedure
Extended Community	1. In the left bar, click **Extended Community**. 2. Click **New Extended Community List**. 3. Enter a name for the list. 4. Enter the BGP extended community as **rt** (*aa*:*nn* | *ip-address*), for a route target community, or **soo** (*aa*:*nn* | *ip-address*), for a route origin community, separating multiple items with a comma. For *aa,* enter a 2-byte AS number, and for *nn* enter a 2-byte network number. 5. Click **Add**.
Class Map	1. In the left bar, 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**.
Mirror	1. In the left bar, 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 to 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**.
Policer	1. In the left bar, 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 0 through 2^{64} bps 7. Click **Add**.

List Type	Procedure
Prefix	**1.** In the left bar, click **Prefix**. **2.** Click **New Prefix List**. **3.** Enter a name for the list. **4.** In the Internet Protocol, 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 screen, the **QoS Map** tab is selected by default:

To configure forwarding classes for use by QoS Map:

1. To create a new QoS mapping:
   a. In the QoS tab, click the **Add QoS Map** drop-down.
   b. Select **Create New**.
   c. Enter a name and description for the QoS mapping.
   d. Click **Add Queue**. The Add Queue popup displays.
   e. Select the queue number from the Queue drop-down.
   f. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types.
   g. Enter the **Forwarding Class**.
   h. Click **Save Queue**.

2. To import an existing QoS mapping:
   a. In the QoS tab, click the **Add QoS Map** drop-down.
   b. Select **Import Existing**. The Import Existing Application QoS Map Policy popup displays.
   c. Select a QoS Map policy.
   d. Click **Import**.

3. To view or copy a QoS mapping or to remove the mapping from the localized policy, click the **More Actions** icon to the right of the row, and select the desired action.

4. To configure policy rewrite rules for the QoS mapping:
   a. In the Policy Rewrite tab, click the **Add Rewrite Policy** drop-down.
   b. Select **Create New**.

c. Enter a name and description for the rewrite rule.

d. Click **Add Rewrite Rule**. The Add Rule popup displays.

e. Select a class from the **Class** drop-down.

f. Select the priority (**Low** or **High**) from the Priority drop-down.

g. Enter the DSCP value (0 through 63) in the **DSCP** field.

h. Enter the class of service (CoS) value (0 through 7) in the **Layer 2 Class of Service** field.

i. Click **Save Rule**.

5. To import an existing rewrite rule:

   a. In the QoS tab, click the **Add Rewrite Policy** drop-down..

   b. Select **Import Existing**. The Import Existing Policy Rewrite popup displays.

   c. Select a rewrite rule policy.

   d. Click **Import**.

6. Click **Next** to move to Configure Access Lists in the wizard.

Configure ACLs

1. In the Configure Access Control Lists screen, 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** - to configure IPv4 ACL policy
   - **Add IPv6 ACL Policy** - to configure IPv6 ACL policy
   - **Import Existing** - to import existing ACL policy

3. If you click **Add IPv4 ACL Policy**, the Add IPv4 ACL Policy screen displays.

   or

   If you click **Add IPv6 ACL Policy**, the Add IPv6 ACL Policy screen displays.

4. Enter a name and description for the ACL in the ACL Policy screen.

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. The Match tab 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 **More Options** next to the rule's name and select the desired option.
16. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
    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**.
    e. Click **Save Access Control List Policy**.
17. Click **Next** to move to Configure Route Policy in the wizard.

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

Configure Route Policies

In Configure Route Policies, configure the routing policies:

1. In the **Add Route Policy** tab, select **Create New**.
2. Enter a name and description for the route policy.
3. In the left pane, click **Add Sequence Type**. A Route box is displayed in the left pane.
4. Double-click the **Route** box, and type a name for the route policy.
5. In the right pane, click **Add Sequence Rule** to create a single sequence in the policy. The Match tab 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 an route policy sequence rule, in the left pane, click **More Options** next to the rule's name and select the desired option.
16. If no packets match any of the 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 in the wizard.

Configure Policy Settings

In Policy Overview, configure 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** - to perform traffic flow monitoring on IPv4 traffic.
    - **Netflow IPv6**- to perform traffic flow monitoring on IPv6 traffic.
    - **Application** - to track and monitor IPv4 applications.
    - **Application IPv6**- to track and monitor IPv6 applications.
    - **Cloud QoS**- to enable QoS scheduling.
    - **Cloud QoS Service Side**- to enable QoS scheduling on the service side.
    - **Implicit ACL Logging**- to log the headers of all 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. In Cisco vManage, select the **Configuration** > **Templates** screen.
2. If you are creating a new device template:
    a. In the Device tab, click **Create Template**.

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. In the Device tab, click the **More Actions** icon to the right of the desired template, and click the **Pencil** icon.

   b. Click the **Additional Templates** tab. 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 the **Additional Templates** tab 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. In the title bar, click the **Custom Options** drop-down.

2. In the **Localized Policy** tab, and then select a policy.

3. Click **More Actions** and click **Activate**.

4. In the **Activate Policy** popup, click **Activate** to push the policy to all reachable Cisco vSmart Controllers in the network.

5. Click **OK** to confirm activation of the policy on all Cisco vSmart Controllers.

6. To deactivate the centralized policy, select the = tab, and then select a policy.

7. 6. Click **More Actions** and click **Deactivate**.

8. In the **Deactivate Policy** popup, click **Deactivate** to confirm that you want to remove the policy from all reachable Cisco vSmart Controllers.

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 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
  !
  !
```