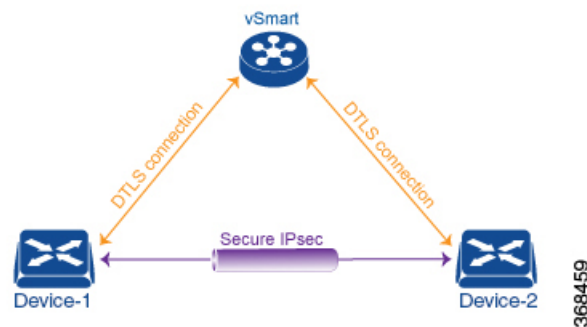




## Data Policies

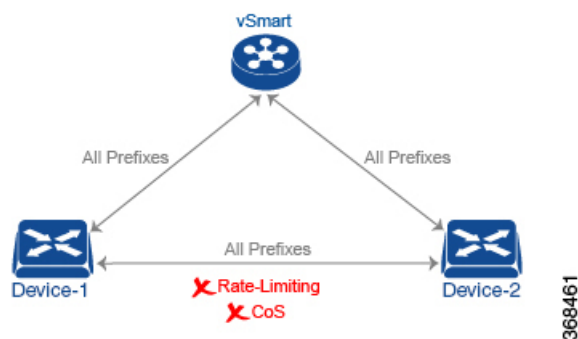
Data policy influences the flow of data traffic traversing the network based either on fields in the IP header of packets or the router interface on which the traffic is being transmitted or received. Data traffic travels over the IPsec connections between Cisco IOS XE SD-WAN devices, shown in purple in the adjacent figure.



The Cisco IOS XE SD-WAN architecture implements two types of data policy:

- Centralized data policy controls the flow of data traffic based on the source and destination addresses and ports and DSCP fields in the packet's IP header (referred to as a 5-tuple), and based on network segmentation and VPN membership. These types of data policy are provisioned centrally, on the Cisco vSmart controller, and they affect traffic flow across the entire network.
- Localized data policy controls the flow of data traffic into and out of interfaces and interface queues on a Cisco IOS XE SD-WAN device. This type of data policy is provisioned locally using access lists. It allows you to classify traffic and map different classes to different queues. It also allows you to mirror traffic and to police the rate at which data traffic is transmitted and received.

By default, no centralized data policy is provisioned. The result is that all prefixes within a VPN are reachable from anywhere in the VPN. Provisioning centralized data policy allows you to apply a 6-tuple filter that controls access between sources and destinations.



As with centralized control policy, you provision centralized data policy on the Cisco vSmart controller, and that configuration remains on the Cisco vSmart controller. The effects of data policy are reflected in how the Cisco IOS XE SD-WAN devices direct data traffic to its destination. Unlike control policy, however, centralized data policies are pushed to the devices in a read-only fashion. They are not added to the router's configuration file, but you can view them from the CLI on the router.

With no access lists provisioned on a Cisco IOS XE SD-WAN device, all data traffic is transmitted at line rate and with equal importance, using one of the interface's queues. Using access lists, you can provision class of service, 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. You can provision policing.

- [Centralized Data Policy, on page 2](#)
- [Localized Data Policy, on page 36](#)

## Centralized Data Policy

Centralized data policy is policy that is configured on a Cisco vSmart Controller (hence, it is centralized) and that affects data traffic being transmitted between the routers on the Cisco SD-WAN overlay network.

### Centralized Data Policy Overview

Data policy operates on the data plane in the Cisco IOS XE SD-WAN overlay network and affects how data traffic is sent among Cisco IOS XE SD-WAN devices in the network. The Cisco IOS XE 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 the devices.

Centralized data policy is applied to packets that originate from a specific sender, or source address, for instance, from a workstation in a local site that is sending voice, data, or other traffic, and it controls which destinations within a VPN the traffic can reach. Data policy is applied to data traffic based on a 6-tuple of fields in the packet's IP header: source IP address, source port, destination IP address, destination port, DSCP, and protocol.

As with control policy, data policy is provisioned centrally on a Cisco vSmart Controller and is applied only on the Cisco vSmart Controller controller. The data policy itself is never pushed to the devices in the network. What is pushed to the Cisco IOS XE SD-WAN devices, via OMP and based on the site ID, are the results of the data policy; hence, the effects of the policy are reflected on the devices. Normally, the data policy on a Cisco IOS XE SD-WAN device acts as the data policy for the entire site that sits behind the device. Data policy that comes from the Cisco vSmart Controller is always implicitly applied in the inbound direction.

Data policy can be applied to data traffic based on the packet header fields, such as the prefix, port, protocol, and DSCP value, and they can also be applied based on the VPN in the overlay network to which the traffic flows.

### Data Policy Based on Packet Header Fields

Policy decisions affecting data traffic can be based on the packet header fields, specifically, on the source and destination IP prefixes, the source and destination IP ports, the protocol, and the DSCP.

This type of policy is often used to modify traffic flow in the network. Here are some examples of the types of control that can be effected with centralized data policy:

- Which set of sources are allowed to send traffic to any destination outside the local site. For example, local sources that are rejected by such a data policy can communicate only with hosts on the local network.
- Which set of sources are allowed to send traffic to a specific set of destinations outside the local site. For example, local sources that match this type of data policy can send voice traffic over one path and data traffic over another.
- Which source addresses and source ports are allowed to send traffic to any destination outside the local site or to a specific port at a specific destination.

### Deep Packet Inspection

In addition to examining the network- and transport-layer headers in data packets, centralized data policy can be used to examine the application information in the data packets' payload. This deep packet inspection offers control over how data packets from specific applications or application families are forwarded across the network, allowing you to assign the traffic to be carried by specific tunnels. To control the traffic flow of specific application traffic based on the traffic loss or latency properties on a tunnel, use application-aware routing.

To base policy decisions on source and destination prefixes and on the headers in the IP data packets, you use centralized data policy, which you configure with the **policy data-policy** command. The Cisco vSmart Controller pushes this type of data policy to the Cisco IOS XE SD-WAN devices. In domains with multiple Cisco vSmart Controllers, all the controllers must have the same centralized data policy configuration to ensure that traffic flow within the overlay network remains synchronized.

To base policy decisions on the application information in the packet payload, you use centralized data policy to perform deep packet inspection. You configure this by creating lists of applications with the **policy lists app-list** command and then calling these lists in a **policy data-policy** command.

To configure the VPNs that Cisco IOS XE SD-WAN devices are allowed to receive routes from, you use centralized data policy, which you configure with the **policy vpn-membership** command. VPN membership policy affects which routes the Cisco vSmart Controller sends to the devices. The policy itself remains on the Cisco vSmart Controller and is not pushed to the devices.

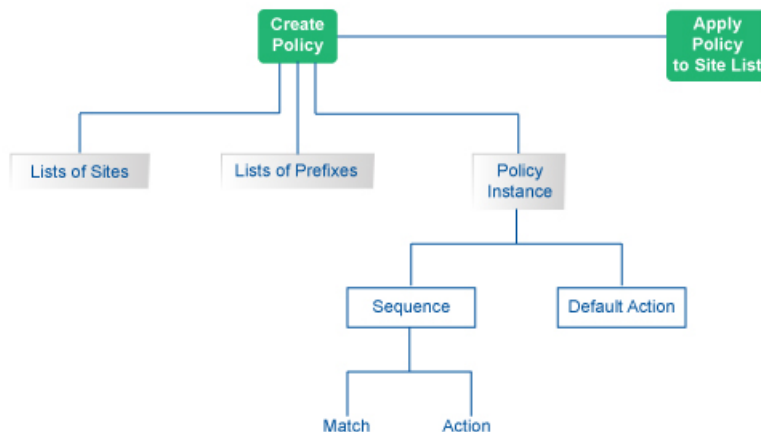
## Configure Centralized Data Policy Based on Prefixes and IP Headers

A centralized data policy based on source and destination prefixes and on headers in IP packets consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is dropped and discarded by default.

### Configuration Components

The following figure illustrates the configuration components for centralized data policy:



To configure centralized data policies, use the Cisco vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

- **Create Groups of Interest**—Create lists that group together related items and that you call in the match or action components of a policy.
- **Configure Traffic Rules**—Create the match and action conditions of a policy.
- **Apply Policies to Sites and VPNs**—Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network.

For a centralized data policy to take effect, you must activate the policy.

This section provides general procedures for configuring centralized data policy on Cisco vSmart Controllers. Centralized data policy can be used for different purposes, which are described in the sections that follow.

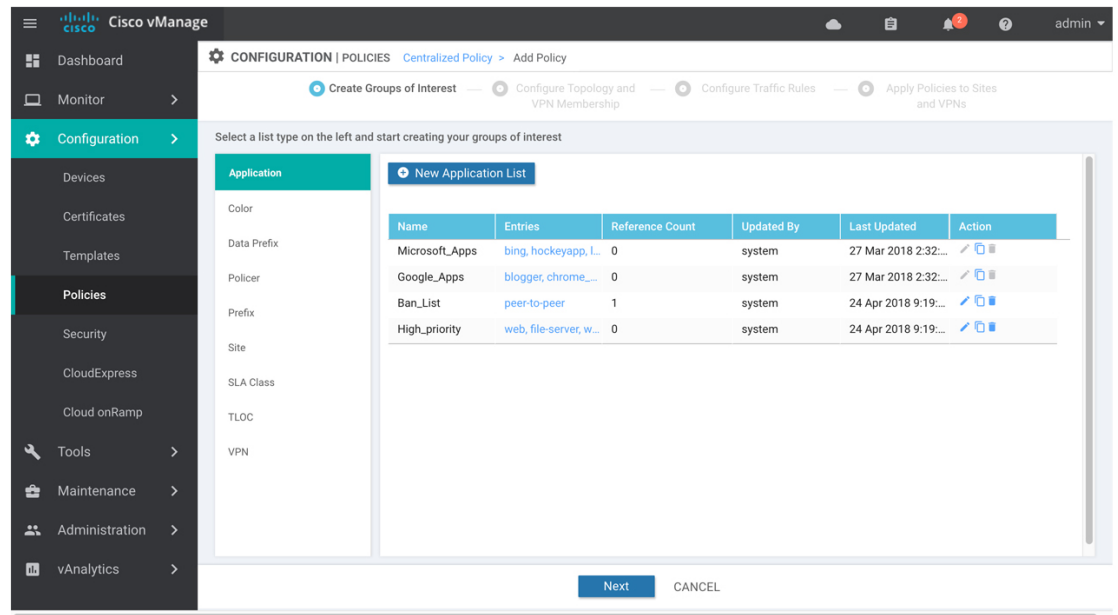
## Start the Policy Configuration Wizard

To start the policy configuration wizard:

- 
- Step 1** In the Cisco vManage NMS, select the **Configure > Policies** screen.
  - Step 2** Select the **Centralized Policy** tab.
  - Step 3** Click **Add Policy**. The policy configuration wizard opens, and the Create Groups of Interest screen displays.
- 

### Step 1: Create Policy Lists

You can create lists of groups to use in centralized policy.



368879

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

List Type	Procedure
Application	<ol style="list-style-type: none"> <li>In the left bar, click <b>Application</b>.</li> <li>Click <b>New Application List</b>.</li> <li>Enter a name for the list.</li> <li>Click either the <b>Application</b> or <b>Application Family</b> button.</li> <li>From the Select drop-down, select the desired applications or application families.</li> <li>Click <b>Add</b>.</li> </ol> <p>Two application lists are preconfigured. You cannot edit or delete these lists.</p> <ul style="list-style-type: none"> <li><b>Google_Apps</b>—Includes Google applications, such as gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the Entries column.</li> <li><b>Microsoft_Apps</b>—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the Entries column.</li> </ul>

List Type	Procedure
Data Prefix	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>Data Prefix</b>.</li> <li>b. Click <b>New Data Prefix List</b>.</li> <li>c. Enter a name for the list.</li> <li>d. Select either <b>IPv4</b> or <b>IPv6</b>.</li> <li>e. In the Add Data Prefix field, enter one or more data prefixes separated by commas.</li> <li>f. Click <b>Add</b>.</li> </ol>
Policer	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>Policer</b>.</li> <li>b. Click <b>New Policer List</b>.</li> <li>c. Enter a name for the list.</li> <li>d. Define the policing parameters: <ol style="list-style-type: none"> <li>1. In the Burst field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.</li> <li>2. In the Exceed field, select the action to take when the burst size or traffic rate is exceeded. It can be drop, which sets the packet loss priority (PLP) to low.</li> <li>3. In the Rate field, enter the maximum traffic rate, a value from 0 through <math>2^{64} - 1</math> bits per second (bps).</li> </ol> </li> <li>e. Click <b>Add</b>.</li> </ol>
Prefix	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>Prefix</b>.</li> <li>b. Click <b>New Prefix List</b>.</li> <li>c. Enter a name for the list.</li> <li>d. In the Add Prefix field, enter one or more data prefixes separated by commas.</li> <li>e. Click <b>Add</b>.</li> </ol>
Site	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>Site</b>.</li> <li>b. Click <b>New Site List</b>.</li> <li>c. Enter a name for the list.</li> <li>d. In the Add Site field, enter one or more site IDs separated by commas.</li> <li>e. Click <b>Add</b>.</li> </ol>

List Type	Procedure
SLA Class	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>SLA Class</b>.</li> <li>b. Click <b>New SLA Class List</b>.</li> <li>c. Enter a name for the list.</li> <li>d. Define the SLA class parameters:               <ol style="list-style-type: none"> <li>1. In the Loss field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.</li> <li>2. In the Latency field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds.</li> <li>3. In the Jitter field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.</li> </ol> </li> <li>e. Click <b>Add</b>.</li> </ol>
TLOC	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>TLOC</b>.</li> <li>b. Click <b>New TLOC List</b>. The TLOC List popup displays.</li> <li>c. Enter a name for the list.</li> <li>d. In the TLOC IP field, enter the system IP address for the TLOC.</li> <li>e. In the Color field, select the TLOC's color.</li> <li>f. In the Encap field, select the encapsulation type.</li> <li>g. In the Preference field, optionally select a preference to associate with the TLOC.</li> <li>h. Click <b>Add TLOC</b> to add another TLOC to the list.</li> <li>i. Click <b>Save</b>.</li> </ol>
VPN	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>VPN</b>.</li> <li>b. Click <b>New VPN List</b>.</li> <li>c. Enter a name for the list.</li> <li>d. In the <b>Add VPN</b> field, enter one or more VPN IDs separated by commas.</li> <li>e. Click <b>Add</b>.</li> </ol>

**Step 2** Click **Next** to move to Configure Topology and VPN Membership in the wizard.

## Step 2: Configure Traffic Rules

When you first open the Traffic Rules screen, the Application-Aware Routing tab is selected by default. To configure traffic rules for deep packet inspection, see [Deep Packet Inspection, on page 25](#).

To configure traffic rules for centralized data policy:

- Step 1** Click the **Traffic Data** tab.
- Step 2** Click the **Add Policy** drop-down.
- Step 3** Click **Create New**. The Add Data Policy screen displays.
- Step 4** Enter a name and description for the data policy.
- Step 5** In the right pane, click **Sequence Type**. The Add Data Policy popup opens.
- Step 6** Select the type of data policy you want to create. Choices are: **Application Firewall**, **QoS**, **Traffic Engineering**, and **Custom**.
- Step 7** A policy sequence containing the text string **Application Firewall**, **QoS**, **Traffic Engineering**, or **Custom** is added in the left pane
- Step 8** Double-click the text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.
- Step 9** In the right pane, click **Sequence Rule**. The Match/Action box opens, and Match is selected by default. The available policy match conditions are listed below the box.
- Step 10** For QoS and Traffic Engineering data policies: From the **Protocol** drop-down list, select **IPv4** to apply the policy only to IPv4 address families, **IPv6** to apply the policy only to IPv6 address families, or **Both** to apply the policy IPv4 and IPv6 address families.
- Step 11** To select one or more Match conditions, click its box and set the values as described in the following table. Note that not all match conditions are available for all policy sequence types.

Match Condition	Procedure	IPv4 Fields	IPv6 Fields
None (match all packets)	Do not specify any match conditions.		
<b>Applications /Application Family List</b>	<ol style="list-style-type: none"> <li>a. In the Match conditions, click <b>Applications/Application Family List</b>.</li> <li>b. In the drop-down, select the application family.</li> <li>c. To create an application list: <ol style="list-style-type: none"> <li>1. Click <b>New Application List</b>.</li> <li>2. Enter a name for the list.</li> <li>3. Click <b>Application</b> to create a list of individual applications. Click <b>Application Family</b> to create a list of related applications.</li> <li>4. In the <b>Select Application</b> drop-down, select the desired applications or application families.</li> <li>5. Click <b>Save</b>.</li> </ol> </li> </ol>	app-list	



Match Condition	Procedure	IPv4 Fields	IPv6 Fields
<b>Destination Data Prefix</b>	<p>a. In the Match conditions, click <b>Destination Data Prefix</b>.</p> <p>b. To match a list of destination prefixes, select the list from the drop-down.</p> <p>c. To match an individual destination prefix, enter the prefix in the <b>Destination: IP Prefix</b> field.</p>	source/ destination-data-prefix-list	source/ destination-data-prefix-list
<b>Destination Port</b>	<p>a. In the Match conditions, click <b>Destination Port</b>.</p> <p>b. In the <b>Destination: Port</b> field, enter the port number. 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 [-]).</p>	src/dst ip	src/dst ip
<b>DNS Application List</b>	<p>Add an application list to enable split DNS.</p> <p>a. In the Match conditions, click <b>DNS Application List</b>.</p> <p>b. In the drop-down, select the application family.</p>	dns-app-list	
<b>DNS</b>	<p>Add an application list to process split DNS.</p> <p>a. In the Match conditions, click <b>DNS</b>.</p> <p>b. In the drop-down, select <b>Request</b> to process DNS requests for the DNS applications, and select <b>Response</b> to process DNS responses for the applications.</p>	dns-request dns-response	
<b>DSCP</b>	<p>a. In the Match conditions, click <b>DSCP</b>.</p> <p>b. In the <b>DSCP</b> field, type the DSCP value, a number from 0 through 63.</p>	dscp	dscp
<b>Packet Length</b>	<p>a. In the Match conditions, click <b>Packet Length</b>.</p> <p>b. In the Packet Length field, type the length, a value from 0 through 65535.</p>	packet-len	packet-len
<b>PLP</b>	<p>a. In the Match conditions, click <b>PLP</b> to set the Packet Loss Priority.</p> <p>b. In the PLP drop-down, select <b>Low</b> or <b>High</b>. To set the PLP to high, apply a policer that includes the <b>exceed remark</b> option.</p>		
<b>Protocol</b>	<p>a. In the Match conditions, click <b>Protocol</b>.</p> <p>b. In the Protocol field, type the Internet Protocol number, a number from 0 through 255.</p>	protocol	protocol/next header

Match Condition	Procedure	IPv4 Fields	IPv6 Fields
<b>Source Data Prefix</b>	<p><b>a.</b> In the Match conditions, click <b>Source Data Prefix</b>.</p> <p><b>b.</b> To match a list of source prefixes, select the list from the drop-down.</p> <p><b>c.</b> To match an individual source prefix, enter the prefix in the <b>Source</b> field.</p>	source/ destination-data-prefix-list	source /destination-data-prefix-list
<b>Source Port</b>	<p><b>a.</b> In the Match conditions, click <b>Source Port</b>.</p> <p><b>b.</b> In the Source field, enter the port number. 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 [-]).</p>	ports	ports
<b>TCP</b>	<p><b>a.</b> In the Match conditions, click <b>TCP</b>.</p> <p><b>b.</b> In the TCP field, <b>syn</b> is the only option available.</p>	tcp flag	

**Step 12** To select actions to take on matching data traffic, click the **Actions** box.

**Step 13** To drop matching traffic, click **Drop**. The available policy actions are listed to the right of the button.

**Step 14** To accept matching traffic, click **Accept**. The available policy actions are listed to the right of the button.

**Step 15** Set the policy action as described in the following table. Note that not all actions are available for all match conditions

Match Condition	Description	Procedure
<b>Counter</b>	Count matching data packets.	<p><b>a.</b> In the Action conditions, click <b>Counter</b>.</p> <p><b>b.</b> In the <b>Counter Name</b> field, enter the name of the file in which to store packet counters.</p>
<b>DSCP</b>	Assign a DSCP value to matching data packets.	<p><b>a.</b> In the Action conditions, click <b>DSCP</b>.</p> <p><b>b.</b> In the <b>DSCP</b> field, type the DSCP value, a number from 0 through 63.</p>
<b>Forwarding Class</b>	Assign a forwarding class to matching data packets.	<p><b>a.</b> In the Match conditions, click <b>Forwarding Class</b>.</p> <p><b>b.</b> In the <b>Forwarding Class</b> field, type the class value, which can be up to 32 characters long.</p>

Match Condition	Description	Procedure
<b>Policer</b>	Apply a policer to matching data packets.	<p>a. In the Match conditions, click <b>Policer</b>.</p> <p>b. In the Policer drop-down field, select the name of a policer.</p>
<b>Loss Correction</b>	<p>Apply loss correction to matching data packets.</p> <p>Forward Error Correction (FEC) recovers lost packets on a link by sending redundant data, enabling the receiver to correct errors without the need to request retransmission of data.</p> <p>FEC is supported only for IPSEC tunnels, it is not supported for GRE tunnels.</p> <ul style="list-style-type: none"> <li>• <b>FEC Adaptive</b> – Corresponding packets are subjected to FEC only if the tunnels that they go through have been deemed unreliable based on measured loss. Adaptive FEC starts to work at 2% packet loss; this value is hard-coded and is not configurable.</li> <li>• <b>FEC Always</b> – Corresponding packets are always subjected to FEC.</li> <li>• <b>Packet Duplication</b> – Sends duplicate packets over a single tunnel. If more than one tunnel is available, duplicated packets will be sent over the tunnel with the best parameters.</li> </ul>	<p>a. In the Match conditions, click <b>Loss Correction</b>.</p> <p>b. In the <b>Loss Correction</b> field, select <b>FEC Adaptive</b>, <b>FEC Always</b>, or <b>Packet Duplication</b>.</p>
Click <b>Save Match and Actions</b> .		

- Step 16** Create additional sequence rules as desired. Drag and drop to re-arrange them.
- Step 17** Click **Save Data Policy**.
- Step 18** Click **Next** to move to Apply Policies to Sites and VPNs in the wizard.

## Step 3: Apply Policies to Sites and VPNs

In Apply Policies to Sites and VPNs, apply a policy to overlay network sites and VPNs.

- Step 1** In the **Policy Name** field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (\_). It cannot contain spaces or any other characters.
- Step 2** In the **Policy Description** field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.
- Step 3** From the Topology bar, select the tab that corresponds to the type of policy block—**Topology**, **Application-Aware Routing**, **Traffic Data**, or **Cflowd**. The table then lists policies that you have created for that type of policy block.
- Step 4** Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:

## Step 4: Activate a Centralized Data Policy

- a) For a **Topology** policy block, click **Add New Site List and VPN List** or **Add New Site**. Some topology blocks might have no **Add** buttons. Select one or more site lists, and select one or more VPN lists. Click **Add**.
- b) For an **Application-Aware Routing** policy block, click **Add New Site List and VPN list**. Select one or more site lists, and select one or more VPN lists. Click **Add**.
- c) For a **Traffic Data** policy block, click **Add New Site List and VPN List**. Select the direction for applying the policy (**From Tunnel**, **From Service**, or **All**), select one or more site lists, and select one or more VPN lists. Click **Add**.
- d) For a **cflowd** policy block, click **Add New Site List**. Select one or more site lists, Click **Add**.

**Step 5** Click **Preview** to view the configured policy. The policy is displayed in CLI format.

**Step 6** Click **Save Policy**. The **Configuration > Policies** screen appears, and the policies table includes the newly created policy.

## Step 4: Activate a Centralized Data Policy

Activating a centralized data policy sends that policy to all connected Cisco vSmart Controllers. To activate a centralized policy:

**Step 1** In the Cisco vManage NMS, select the **Configure > Policies** screen.

**Step 2** Select a policy from the policy table.

**Step 3** Click the **More Actions** icon to the right of the row, and click **Activate**. The Activate Policy popup opens. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy is to be applied.

**Step 4** Click **Activate**.

## Configure Centralized Data Policy Using CLI

Following are the high-level steps for configuring a VPN membership data policy:

1. Create a list of overlay network sites to which the VPN membership policy is to be applied (in the **apply-policy** command):

```
vSmart(config)# policy
vSmart (config-policy)# lists site-list list-name
vSmart (config-lists-list-name)# site-id site-id
```

The list can contain as many site IDs as necessary. Include one **site-id** command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (-). Create additional site lists, as needed.

2. Create lists of IP prefixes and VPNs, as needed:

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

```
vSmart (config)# policy lists
vSmart (config-lists)# vpn-list list-name
vSmart (config-lists-list-name)# vpn vpn-id
```

```
vsmart (config)# policy lists data-ipv6-prefix-list dest_ip_prefix_list
vsmart (config-data-ipv6-prefix-list-dest_ip_prefix_list)# ipv6-prefix 2001:DB8:19::1
vsmart (config-data-ipv6-prefix-list-dest_ip_prefix_list)# commit
Commit complete.
```

```

vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match destination-data-ipv6-prefix-list dest_ip_prefix_list
vsmart (config-match)# commit
vsmart(config-match)# exit
vsmart(config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vm9(config-match)# commit
Commit complete.
vm9(config-match)# end

vsmart(config)# policy
vsmart(config-policy)# data-policy data_policy_1
vsmart(config-data-policy-data_policy_1)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8:19::1
vsmart(config-match)# exit
vsmart(config-sequence-101)# match destination-ipv6 2001:DB8:19::1
vsmart(config-match)#

```

3. Create lists of TLOCs, as needed.

```

vSmart(config)# policy
vSmart(config-policy)# lists tloc-list list-name
vSmart(config-lists-list-name)# tloc ip-address color color encap encapsulation
[preference number]

```

4. Define policing parameters, as needed:

```

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

```

5. Create a data policy instance and associate it with a list of VPNs:

```

vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy-policy-name)# vpn-list list-name

```

6. Create a series of match–pair sequences:

```

vSmart(config-vpn-list)# sequence number
vSmart(config-sequence-number)#

```

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).

7. Define match parameters for packets:

```

vSmart(config-sequence-number)# matchparameters

```

8. Define actions to take when a match occurs:

```

vSmart(config-sequence-number)# action (accept | drop) [count counter-name] [log]
[tcp-optimization]
vSmart(config-sequence-number)# action accept nat [pool number] [use-vpn 0]
vSmart(config-sequence-number)# action accept redirect-dns (host | ip-address)
vSmart(config-sequence-number)# action accept set parameters

vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
vsmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8:19::1
vsmart(config-set)#

```

9. Create additional numbered sequences of match–action pairs within the data policy, as needed.

10. If a route does not match any of the conditions in one of the sequences, it is rejected by default. To accept nonmatching prefixed, configure the default action for the policy:

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

11. Apply the policy to one or more sites in the overlay network:

```
vSmart(config) # apply-policy site-list list-name data-policy policy-name (all
| from-service | from-tunnel)
```

## Structural Components of Policy Configuration for Centralized Data Policy

The following commands are the structural components required to configure VPN membership policy. Each one is explained in more detail in the sections that follow.

```
policy
  lists
    app-list list-name
      (app applications | app-family application-families)
    data-prefix-list list-name
      ip-prefix prefix
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc ip-address color color encaps encapsulation [preference value]
    vpn-list list-name
      vpn vpn-id
  policer policer-name
    burst bytes
    exceed action
    rate bandwidth
  data-policy policy-name
    vpn-list list-name
      sequence number
      match
        app-list list-name
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port port-numbers
        dscp number
        dns-app-list list-name
        dns (request | response)
        packet-length number
        protocol number
        source-data-prefix-list list-name
        source-ip prefix/length
        source-port port-numbers
        tcp flag
      action
        cflowd (not available for deep packet inspection)
        count counter-name
        drop
        log
        redirect-dns (dns-ip-address | host)
        tcp-optimization
        accept
          nat [pool number] [use-vpn 0]
          set
            dscp number
            forwarding-class class
            local-tloc color color [encap encapsulation] [restrict]
            next-hop ip-address
            policer policer-name

          tloc ip-address color color [encap encapsulation]
```

```

tloc-list list-name
  vpn vpn-id
  default-action
    (accept | drop)
apply-policy site-list list-name
  data-policy policy-name (all | from-service | from-tunnel)

```

## Lists

Centralized data policy for deep packet inspection uses the following types of lists to group related items. In the CLI, you configure lists under the **policy lists** command hierarchy on Cisco vSmart Controllers.

- **Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest**
- **Configuration > Policies > Custom Options > Lists.**

In the CLI, you configure lists under the **policy lists** command hierarchy on Cisco vSmart Controllers.

List Type	Description	vManage / CLI Command
Applications and application families	<p>List of one or more applications or application families running on the subnets connected to the device.</p> <ul style="list-style-type: none"> <li>• <i>application-names</i> can be the names of one or more applications. The Cisco IOS XE SD-WAN devices supports about 2300 different applications. To list the supported applications, use the ? in the CLI.</li> <li>• <i>application-families</i> can be one or more of the following: <b>antivirus</b>, <b>application-service</b>, <b>audio_video</b>, <b>authentication</b>, <b>behavioral</b>, <b>compression</b>, <b>database</b>, <b>encrypted</b>, <b>erp</b>, <b>file-server</b>, <b>file-transfer</b>, <b>forum</b>, <b>game</b>, <b>instant-messaging</b>, <b>mail</b>, <b>microsoft-office</b>, <b>middleware</b>, <b>network-management</b>, <b>network-service</b>, <b>peer-to-peer</b>, <b>printer</b>, <b>routing</b>, <b>security-service</b>, <b>standard</b>, <b>telephony</b>, <b>terminal</b>, <b>thin-client</b>, <b>tunneling</b>, <b>wap</b>, <b>web</b>, and <b>webmail</b>.</li> </ul>	<p><b>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Application</b></p> <p>or</p> <p><b>Configuration &gt; Policies &gt; Centralized Policy &gt; Lists &gt; Application</b></p> <p><b>app-list list-name</b></p> <p>(<b>app applications</b>   <b>app-family application-families</b>)</p>

List Type	Description	vManage / CLI Command
Prefixes	List of one or more IP prefixes.	<b>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Prefix</b> or <b>Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Prefix</b> <b>prefix-list</b> <i>list-name</i> <b>ip-prefix</b> <i>prefix/length</i>
Sites	List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as <b>site-id 1</b> ) or a range of site identifiers (such as <b>site-id 1-10</b> ).	<b>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Site</b> or <b>Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Site</b> <b>site-list</b> <i>list-name</i> <b>site-id</b> <i>site-id</i>
TLOCs	<p>List of one or more TLOCs in the overlay network.</p> <p>For each TLOC, specify its address, color, and encapsulation. <i>address</i> is the system IP address. <i>color</i> can be one of <b>3g</b>, <b>biz-internet</b>, <b>blue</b>, <b>bronze</b>, <b>custom1</b>, <b>custom2</b>, <b>custom3</b>, <b>default</b>, <b>gold</b>, <b>green</b>, <b>lte</b>, <b>metro-ethernet</b>, <b>mpls</b>, <b>mpls-restricted</b>, <b>private1</b> through <b>private6</b>, <b>public-internet</b>, <b>red</b>, and <b>silver</b>. <i>encapsulation</i> can be <b>gre</b> or <b>ipsec</b>.</p> <p>Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an <b>action accept</b> condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion.</p>	<b>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; TLOC</b> or <b>Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Site</b> <b>tloc-list</b> <i>list-name</i> <b>tloc</b> <i>ip-address color color encap encapsulation</i> [ <b>preference number</b> ]



List Type	Description	vManage / CLI Command
VPNs	<p>List of one or more VPNs in the overlay network. For data policy, you can configure any VPNs except for VPN 0 and VPN 512.</p> <p>To configure multiple VPNs in a single list, include multiple <b>vpn</b> options, specifying one VPN number in each option. You can specify a single VPN identifier (such as <b>vpn 1</b>) or a range of VPN identifiers (such as <b>vpn 1-10</b>).</p>	<p><b>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; VPN</b></p> <p>or</p> <p><b>Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; VPN</b></p> <p><b>vpn-list</b> <i>list-name</i></p> <p><b>vpn</b> <i>vpn-id</i></p>

## VPN Lists

Each centralized data policy is associated with a VPN list. You configure VPN lists with the **policy data-policy vpn-list** command. The list you specify must be one that you created with a VPN Group of Interest or List in the Cisco vManage policy configuration wizard or with the **policy lists vpn-list** command.

For centralized data policy, you can include any VPNs except for VPN 0 and VPN 512. VPN 0 is reserved for control traffic, so never carries any data traffic, and VPN 512 is reserved for out-of-band network management, so also never carries any data traffic. Note that while the CLI allows you to include these two VPNs in a data policy configuration, the policy is not applied to these two VPNs.

## Policer Parameters

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In Cisco vManage NMS, you configure policer parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > Policer**
- **Configuration > Policies > Custom Options > Centralized Policy > Lists > Policer**

In the CLI, you configure policer parameters as follows:

```
vSmart(config)# policy policer policer-name
vSmart(config-policer)# rate bps
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

**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 centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the **match plp** option.

## Sequences

Each VPN list consists of sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy.

In the Cisco vManage NMS, you configure sequences from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type**
- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type**

In the CLI, you configure sequences with the `policy data-policy vpn-list sequence` command.

Each sequence can contain one match condition and one action condition.

## Match Parameters

Centralized data policy can match IP prefixes and fields in the IP headers, as well as applications. You can also enable split DNS.

In Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Match**
- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Match**

Each sequence in a policy can contain one match condition.

For data policy, you can match these parameters:

Description	vManage Configuration/CLI Configuration Command	Value or Range
Match all packets	Omit Match Omit <code>match</code> command	—
Applications or application families	Match Applications/Application Family List <code>app-list list-name</code>	Name of an application list or an <code>app-list</code> list
Group of destination prefixes	Match Destination Data Prefix <code>destination-data-prefix-list list-name</code>	Name of a data prefix list or a <code>data-prefix-list</code> list
Individual destination prefix	Match Destination Data Prefix <code>destination-ip prefix/length</code>	IP prefix and prefix length

Description	vManage Configuration/CLI Configuration Command	Value or Range
Destination port number	Match Destination Port <b>destination-port</b> <i>number</i>	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 [-])
Enable split DNS, to resolve and process DNS requests and responses on an application-by-application basis	Match DNS Application List <b>dns-app-list</b> <i>list-name</i>	Name of an <b>app-list</b> list. This list specifies the applications whose DNS requests are processed.
Specify the direction in which to process DNS packets	Match DNS <b>dns</b> ( <b>request</b>   <b>response</b> )	To process DNS requests sent by the applications (for outbound DNS queries), specify <b>dns request</b> . To process DNS responses returned from DNS servers to the applications, specify <b>dns response</b> .
DSCP value	Match DSCP <b>dscp</b> <i>number</i>	0 through 63
Packet length	Match Packet Length <b>packet-length</b> <i>number</i>	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 loss priority (PLP)	Match PLP <b>plp</b>	<b>(high   low)</b> By default, packets have a PLP value of <b>low</b> . To set the PLP value to <b>high</b> , apply a policer that includes the <b>exceed remark</b> option.
Internet protocol number	Match Protocol <b>protocol</b> <i>number</i>	0 through 255
Group of source prefixes	Match Source Data Prefix <b>source-data-prefix-list</b> <i>list-name</i>	Name of a data prefix or a <b>data-prefix-list</b> list
Individual source prefix	Match Source Data Prefix <b>source-ip</b> <i>prefix/length</i>	IP prefix and prefix length
Source port number	Match Source Port <b>source-port</b> <i>address</i>	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 [-])

Description	vManage Configuration/CLI Configuration Command	Value or Range
TCP flag	<code>tcp flag</code>	<code>syn</code>

## Action Parameters

**Table 1: Feature History**

Feature Name	Release Information	Description
Path Preference Support for Cisco IOS XE SD-WAN Devices	Cisco IOS XE Release Amsterdam 17.2.1r	This feature extends to Cisco IOS XE SD-WAN devices, support for selecting one or more local transport locators (TLOCs) for a policy action.

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped, and it can be counted. Then, you can associate parameters with accepted packets.

In Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action**
- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action.**

In the CLI, you configure the action parameters with the `policy data-policy vpn-list sequence action` command.

Each sequence in a centralized data policy 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	vManage Configuration/CLI Configuration Parameter	Value or Range
Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.	Click <b>Accept</b> . <b>accept</b>	—
Enable cflowd traffic monitoring.	Click <b>Accept</b> , then action <b>Cflowd cflowd</b>	—
Count the accepted or dropped packets.	Action Counter Click <b>Accept</b> , then action <b>Counter</b> <b>count counter-name</b>	Name of a counter. Use the <b>show policy access-lists counters</b> command on the Cisco IOS XE SD-WAN device.
Discard the packet. This is the default action.	Click <b>Drop</b> . <b>drop</b>	—

Description	vManage Configuration/CLI Configuration Parameter	Value or Range
Redirect DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions.	Click <b>Accept</b> , then action <b>Redirect DNS</b> <b>redirect-dns host</b> <b>redirect-dns ip-address</b>	For an inbound policy, <b>redirect-dns host</b> allows the DNS response to be correctly forwarded back to the requesting service VPN.  For an outbound policy, specify the IP address of the DNS server.
Fine-tune TCP to decrease round-trip latency and improve throughput for matching TCP traffic.	Click <b>Accept</b> , then action <b>TCP Optimization</b> <b>tcp-optimization</b>	—



**Note** On Cisco IOS XE routers, all the ongoing optimized flows are dropped when the TCP Optimization is removed.

Then, for a packet that is accepted, the following parameters can be configured:

Description	vManage	CLI Configuration Parameter	Value or Range
Enable cflowd traffic monitoring.	Click <b>Accept</b> , then action <b>Cflowd</b> .	<b>cflowd</b>	—
Direct matching traffic to the NAT functionality so that it can be redirected directly to the Internet or other external destination.	Click <b>Accept</b> , then action <b>NAT Pool</b> or <b>NAT VPN</b> .	<b>nat [pool number]</b> <b>[use-vpn 0]</b>	—
DSCP value.	Click <b>Accept</b> , then action <b>DSCP</b> .	<b>set dscp value</b>	0 through 63
Forwarding class.	Click <b>Accept</b> , then action <b>Forwarding Class</b> .	<b>set forwarding-class value</b>	Name of forwarding class

Description	vManage	CLI Configuration Parameter	Value or Range
<p>Direct matching packets to a TLOC that matches the color and encapsulation</p> <p>By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC.</p>	Click <b>Accept</b> , then action <b>Local TLOC</b> .	<b>set local-tloc color</b> <i>color</i> [ <b>encap</b> <i>encapsulation</i> ]	<p><i>color</i> can be:</p> <p><b>3g, biz-internet, blue, bronze, custom1, custom2,</b></p>
<p>Direct matching packets to one of the TLOCs in the list if the TLOC matches the color and encapsulation</p> <p>By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the <b>restrict</b> option.</p>	Click <b>Accept</b> , then action <b>Local TLOC</b>	<b>set local-tloc-list color</b> <i>color</i> <b>encap</b> <i>encapsulation</i> [ <b>restrict</b> ]	<p><b>custom3, default, gold, green lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver.</b></p> <p>By default, <i>encapsulation</i> is <b>ipsec</b>. It can also be <b>gre</b>.</p>
Set the next hop to which the packet should be forwarded.	Click <b>Accept</b> , then action <b>Next Hop</b> .	<b>set next-hop</b> <i>ip-address</i>	IP address
Apply a policer.	Click <b>Accept</b> , then action <b>Policer</b> .	<b>set policer</b> <i>policer-name</i>	Name of policer configured with a <b>policy policer</b> command.
<p>Specify a service to redirect traffic to before delivering the traffic to its destination.</p> <p>The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them.</p> <p>The VPN identifier is where the service is located.</p> <p>Configure the services themselves on the Cisco IOS XE SD-WAN devices that are collocated with the service devices, using the <b>vpn service</b> command.</p>	Click <b>Accept</b> , then action <b>Service</b> .	<b>set service</b> <i>service-name</i> [ <b>tloc</b> <i>ip-address</i>   <b>tloc-list</b> <i>list-name</i> ] [ <b>vpn</b> <i>vpn-id</i> ]	<p>Standard services: <b>FW, IDS, IDP</b></p> <p>Custom services: <b>netsvc1, netsvc2, netsvc3, netsvc4</b></p> <p>TLOC list is configured with a <b>policy lists tloc-list</b> list.</p>

Description	vManage	CLI Configuration Parameter	Value or Range
Direct traffic to a remote TLOC that matches the IP address, color, and encapsulation.	Click <b>Accept</b> , then action <b>TLOC</b> .	<b>set tloc address color color [encap encapsulation]</b>	TLOC address, color, and encapsulation
Direct traffic to one of the remote TLOCs in the TLOC list if it matches the IP address, color, and encapsulation of one of the TLOCs in the list. If a preference value is configured for the matching TLOC, that value is assigned to the traffic.	Click <b>Accept</b> , then action <b>TLOC</b> .	<b>set tloc-list list-name</b>	Name of a <b>policy lists tloc-list</b> list
Set the VPN that the packet is part of.	Click <b>Accept</b> , then action <b>VPN</b> .	<b>set vpn vpn-id</b>	0 through 65530

The following table describes the IPv4 and IPv6 actions.

IPv4 Actions	IPv6 Actions
drop, dscp, next-hop (from-service only)/vpn, count, forwarding class, policer (only in interface ACL), App-route SLA (only)	
App-route preferred color, app-route sla strict, cflowd, nat, redirect-dns	
	drop, dscp, next-hop/vpn, count, forwarding class, policer (only in interface ACL) App-route SLA (only), App-route preferred color, app-route sla strict
policer (DataPolicy), tcp-optimization, fec-always,	policer (DataPolicy)
tloc, tloc-list (set tloc, set tloc-list)	tloc, tloc-list (set tloc, set tloc-list)
App-Route backup-preferred color, local-tloc, local-tloc-list	App-Route backup-preferred color, local-tloc, local-tloc-list

## Default Action

If a data packet being evaluated does not match any of the match conditions in a data policy, a default action is applied to the packet. By default, the data packet is dropped

In the Cisco vManage NMS, you modify the default action from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Default Action**

- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Default Action.**

In the CLI, you modify the default action with the `policy data-policy vpn-list default-action accept` command.

## Apply Centralized Data Policy

For a centralized data policy to take effect, you apply it to a list of sites in the overlay network.

To apply a centralized policy in the Cisco vManage NMS:

1. In the Cisco vManage NMS, select the **Configure > Policies** screen.
2. Select a policy from the policy table.
3. Click the **More Actions** icon to the right of the row, and click **Activate**. The Activate Policy popup opens. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy is to be applied.
4. Click **Activate**.

To apply a centralized policy in the CLI:

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service
| from-tunnel)
```

By default, data policy applies to all data traffic passing through the device: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. You can explicitly configure this behavior by including the **all** option. To have the data policy apply only to traffic coming from the service site and exiting from the local site through the tunnel interface, include the **from-service** option. To have the policy apply only to traffic entering from the tunnel interface and traveling to the service site, include the **from-tunnel** option. You can apply different data policies in each of the two traffic directions.

For all **data-policy** policies that you apply with **apply-policy** commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists **site-list 1 site-id 1-100** and **site-list 2 site-id 70-130**. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different **data-policy** policies, the attempt to commit the configuration on the Cisco vSmart Controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (**app-route-policy**)
- Centralized control policy (**control-policy**)
- Centralized data policy used for cflowd flow monitoring (**data-policy** that includes a **cflowd** action and **apply-policy** that includes a **cflowd-template** command)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for **control-policy** and **data-policy** policies can have overlapping site IDs. So for the two example site lists above, **site-list 1 site-id 1-100** and **site-list 2 site-id 70-130**, you could apply one to a control policy and the other to a data policy.



As soon as you successfully activate the configuration by issuing a **commit** command, the Cisco vSmart Controller pushes the data policy to the devices located in the specified sites. To view the policy as configured on the Cisco vSmart Controllers, use the **show running-config** command on the Cisco vSmart Controller:

```
vSmart# show running-config policy
vSmart# show running-config apply-policy
```

To view the policy that has been pushed to the Cisco IOS XE SD-WAN device, use the **show sdwan policy from-vsmart** command on the Cisco IOS XE SD-WAN device.

```
Device# show sdwan policy from-vsmart
```

## Deep Packet Inspection

You configure deep packet inspection using a standard centralized data policy. You define the applications of interest in a vManage policy list or with **policy lists app-list** CLI command, and you call these lists in the match portion of the data policy. You can control the path of the application traffic through the network by defining, in the **action** portion of the data policy, the local TLOC or the remote TLOC, or for strict control, you can define both.

### Configure Deep Packet Inspection Using vManage

To configure a centralized data policy for deep packet inspection, use the vManage policy configuration wizard. Use the wizard to create and edit deep packet inspection policy components:

- Configure groups of interest (lists) to group related items to be called in the centralized data policy.
- Configure traffic rules.
- Apply the policy.

#### Step 1: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In vManage NMS, select the Configure > Policies screen.
2. Select the Centralized Policy tab.
3. Click Add Policy.

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

#### Step 2: Create Groups of Interest

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

To configure groups of interest for deep packet inspection:

1. In the left pane, select the type of list. For centralized data policy for deep packet inspection, you can use Application, Site, and VPN lists.
2. To create a new list, click New List.

To modify an existing list, click the More Actions icon to the right of the desired list, and click the pencil icon.

3. In the List Name field, enter a name for the list. 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.
4. In the field below the List Name field, enter the desired values for the list. For some lists you type the desired values, and for others you select from a drop-down.
5. Click Add (for a new list) or Save (for an existing list).
6. Click Next to move to the Configure Topology and VPN Membership screen.
7. Click Next to move the Configure Traffic Rules in the wizard.

### Step 3: Configure Traffic Rules

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

To configure traffic rules for deep packet inspection policy:

1. In the Application-Aware Routing bar, click Traffic Data.
2. To create a new centralized data policy, click Add Policy.  
To modify an existing policy, click the More Actions icon to the right of the desired policy, and click the pencil icon.
3. If data traffic does not match any of the conditions in one of the sequences, it is dropped by default. If you want nonmatching routes to be accepted, click the pencil icon in the Default Action, click Accept, and click Save Match And Actions.
4. To create a match–action sequence for data traffic:
  - a. Click Sequence Type.
  - b. To create a match–action rule, click Sequence Rule. The Match button is selected by default.
  - c. Click the desired Match button, and enter the desired values in Match Conditions. For some conditions, you type the desired values, and for others you select from a drop-down.
  - d. Click the Actions button. The default action is Reject. To accept matching packets, click the Accept radio button. Then click the desired action, and enter the desired values for Actions.
  - e. Click Save Match and Actions.
  - f. Create additional Sequence Rules or Sequence Types, as needed.
5. To rename a Sequence Type, double-click its name in the right pane, and type the new name. The name also changes in the right pane.
6. To re-order sequence rules and types, drag and drop them.
7. Click Save.
8. Click Next to move to the Apply Policies to Sites and VPNs in the wizard.

### Step 4: Apply Policies to Sites and VPNs

1. In Apply Policies to Sites and VPNs, apply a policy to overlay network sties and VPNs:

2. In the Policy Name field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (\_). It cannot contain spaces or any other characters.
3. In the Policy Description field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.
4. From the Topology bar, select the Application-Aware Routing tab. The table then lists policies that you have created for that type of policy block.
5. Click Add New Site List and VPN List or Add New Site. Some topology blocks might have no Add buttons. Select one or more site lists, and select one or more VPN lists. Click Add.
6. Click Preview to view the configured policy. The policy is displayed in CLI format.
7. Click Save Policy. The Configuration > Policies screen opens, and the policies table includes the newly created policy.

### Step 5: Activate a Centralized Data Policy

Activating a centralized data policy sends that policy to all connected vSmart controllers. To activate a centralized policy:

1. In vManage NMS, select the Configure > Policies screen.
2. Select a policy from the policy table.
3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable vSmart controllers to which the policy is to be applied.
4. Click Activate.

## Configure Deep Packet Inspection Using CLI

Following are the high-level steps for configuring a centralized data policy to use for deep packet inspection:

1. Create a list of overlay network sites to which the data policy is to be applied in the **apply-policy** command:

```
vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```

The list can contain as many site IDs as necessary. Include one **site-id** command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (-).

Create additional site lists, as needed.

2. Create lists of applications and application families that are to be subject to the data policy. Each list can contain one or more application names, or one or more application families. A single list cannot contain both applications and application families.

```
vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-app-list)# app application-name
```

```
vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-applist)# app-family family-name
```

**3. Create lists of IP prefixes and VPNs, as needed:**

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

```
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id
```

**4. Create lists of TLOCs, as needed:**

```
vSmart(config)# policy
vSmart(config-policy)# lists tloc-list list-name
vSmart(config-lists-list-name)# tloc ip-address color color encap encapsulation
[preference number]
```

**5. Define policing parameters, as needed:**

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

**6. Create a data policy instance and associate it with a list of VPNs:**

```
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy-policy-name)# vpn-list list-name
```

**7. Create a series of match–pair sequences:**

```
vSmart(config-vpn-list)# sequence number
vSmart(config-sequence-number)#
```

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).

**8. Define match parameters based on applications:**

```
vSmart(config-sequence-number)# match app-list list-name
```

**9. Define additional match parameters for data packets:**

```
vSmart(config-sequence-number)# match parameters
```

**10. Define actions to take when a match occurs:**

```
vSmart(config-sequence-number)# action (accept | drop) [count]
```

**11. For packets that are accepted, define the actions to take. To control the tunnel over which the packets travels, define the remote or local TLOC, or for strict control over the tunnel path, set both:**

```
vSmart(config-action)# set tloc ip-address color color encap encapsulation
vSmart(config-action)# set tloc-list list-name
vSmart(config-action)# set local-tloc color color encap encapsulation
vSmart(config-action)# set local-tloc-list color color encap encapsulation [restrict]
```

**12. Define additional actions to take.****13. Create additional numbered sequences of match–action pairs within the data policy, as needed.****14. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching prefixes to be accepted, configure the default action for the policy:**

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

**15. Apply the policy to one or more sites in the overlay network:**

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all |
from-service | from-tunnel)
```

To enable the infrastructure for deep packet inspection on the vEdge routers, include the following command in the configuration on the routers:

```
vEdge(config)# policy app-visibility
```

## Structural Components of Policy Configuration for Deep Packet Inspection

Following are the structural components required to configure centralized data policy for deep packet inspection. Each one is explained in more detail in the sections below.

On the vSmart controller:

```
policy
  lists
    app-list list-name
      (app applications | app-family application-families)
    data-prefix-list list-name
      ip-prefix prefix
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc ip-address color color encap encapsulation [preference value]
    vpn-list list-name
      vpn vpn-id
  policer policer-name
    burst bytes
    exceed action
    rate bps
  data-policy policy-name
    vpn-list list-name
      sequence number
    match
      app-list list-name
      destination-data-prefix-list list-name
      destination-ip ip-addresses
      destination-port port-numbers
      dscp number
      packet-length number
      protocol protocol
      source-data-prefix-list list-name
      source-ip ip-addresses
      source-port port-numbers
      tcp flag
    action
      drop
      count counter-name
      log
      accept
        nat [pool number] [use-vpn 0]
        set
          dscp number
          forwarding-class class
          local-tloc color color [encap encapsulation] [restrict]
          next-hop ip-address
          policer policer-name
          service service-name local [restrict] [vpn vpn-id]
          service service-name (tloc ip-address | tloc-list list-name) [vpn vpn-id]
          tloc ip-address color color encap encapsulation
          tloc-list list-name
          vpn vpn-id
      default-action
```

```
(accept | drop)
apply-policy site-list list-name
  data-policy policy-name (all | from-service | from-tunnel)
```

```
On the vEdge router:
policy
  app-visibility
```

## Action Parameters for Configuring Deep Packet Inspection

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped, and it can be counted. Then, you can associate parameters with accepted packets.

In vManage NMS, you configure match parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action**
- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action.**

In the CLI, you configure the action parameters under the **policy data-policy vpn-list sequence action** command.

Each sequence in a centralized data policy 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	vManage Configuration/CLI Configuration Parameter	Value or Range
Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.	Click <b>Accept</b> . <b>accept</b>	—
Count the accepted or dropped packets.	Action Counter Click <b>Accept</b> , then action <b>Counter</b> <b>count counter-name</b>	Name of a counter. Use the <b>show policy access-lists counters</b> command on the Cisco device.
Discard the packet. This is the default action.	Click <b>Drop</b> . <b>drop</b>	—

To view the packet logs, use the **show app log flows** and **show log** commands.

Then, for a packet that is accepted, the following parameters can be configured. Note that you cannot use DPI with either cflowd or NAT.

Description	vManage	CLI Configuration Parameter	Value or Range
DSCP value.	Click <b>Accept</b> , then action <b>DSCP</b> .	<b>set dscp value</b>	0 through 63

Description	vManage	CLI Configuration Parameter	Value or Range
Forwarding class.	Click <b>Accept</b> , then action <b>Forwarding Class</b> .	<b>set forwarding-class</b> <i>value</i>	Name of forwarding class
Direct matching packets to a TLOC that matches the color and encapsulation  By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC.	Click <b>Accept</b> , then action <b>Local TLOC</b> .	<b>set local-tloc color</b> <i>color</i> [ <b>encap</b> <i>encapsulation</i> ]	<i>color</i> can be: <b>3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold,</b>
Direct matching packets to one of the TLOCs in the list if the TLOC matches the color and encapsulation  By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the <b>restrict</b> option.	Click <b>Accept</b> , then action <b>Local TLOC</b>	<b>set local-tloc-list color</b> <i>color</i> <b>encap</b> <i>encapsulation</i> [ <b>restrict</b> ]	<b>green lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver.</b>  By default, <i>encapsulation</i> is <b>ipsec</b> . It can also be <b>gre</b> .
Set the next hop to which the packet should be forwarded.	Click <b>Accept</b> , then action <b>Next Hop</b> .	<b>set next-hop</b> <i>ip-address</i>	IP address
Apply a policer.	Click <b>Accept</b> , then action <b>Policer</b> .	<b>set policer</b> <i>policer-name</i>	Name of policer configured with a <b>policy policer</b> command.
Direct matching packets to the name service, before delivering the traffic to its ultimate destination.  The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them.  The VPN identifier is where the service is located.  Configure the services themselves on the vEdge routers that are collocated with the service devices, using the <b>vpn service</b> configuration command.	Click <b>Accept</b> , then action <b>Service</b> .	<b>set service</b> <i>service-name</i> [ <b>tloc</b> <i>ip-address</i>   <b>tloc-list</b> <i>list-name</i> ] [ <b>vpn</b> <i>vpn-id</i> ]	Standard services: <b>FW, IDS, IDP</b>  Custom services: <b>netsvc1, netsvc2, netsvc3, netsvc4</b>  TLOC list is configured with a <b>policy lists tloc-list</b> list.

Description	vManage	CLI Configuration Parameter	Value or Range
Direct matching packets to the named service that is reachable via a GRE tunnel whose source is in the transport VPN (VPN 0). If the GRE tunnel used to reach the service is down, packet routing falls back to using standard routing. To drop packets when a GRE tunnel to the service is unreachable, include the restrict option. In the service VPN, you must also advertise the service using the <b>service</b> command. You configure the GRE interface or interfaces in the transport VPN (VPN 0).	Click <b>Accept</b> , then action <b>Service</b> .	<b>set service</b> <i>service-name</i> [ <b>tloc</b> <i>ip-address</i>   <b>tloc-list</b> <i>list-name</i> ] [ <b>vpn</b> <i>vpn-id</i> ]	Standard services: <b>FW, IDS, IDP</b> Custom services: <b>netsvc1, netsvc2, netsvc3, netsvc4</b>
Direct traffic to a remote TLOC. The TLOC is defined by its IP address, color, and encapsulation.	Click <b>Accept</b> , then action <b>TLOC</b> .	<b>set local-tloc color</b> <i>color</i> [ <b>encap</b> <i>encapsulation</i> ]	TLOC address, color, and encapsulation
Direct traffic to one of the remote TLOCs in the TLOC list.	Click <b>Accept</b> , then action <b>TLOC</b> .	<b>set tloc-list</b> <i>list-name</i>	Name of a <b>policy lists tloc-list</b> list
Set the VPN that the packet is part of.	Click <b>Accept</b> , then action <b>VPN</b> .	<b>set vpn</b> <i>vpn-id</i>	0 through 65530

### Default Action

If a data packet being evaluated does not match any of the match conditions in a data policy, a default action is applied to the packet. By default, the data packet is dropped.

In vManage NMS, you modify the default action from Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > Application-Aware Routing > Sequence Type > Sequence Rule > Default Action.

In the CLI, you modify the default action with the **policy data-policy vpn-list default-action accept** command.

## Apply Centralized Data Policy for Deep Packet Inspection

For a deep packet inspection centralized data policy to take effect, you apply it to a list of sites in the overlay network.

To apply a centralized policy in vManage NMS:

1. In vManage NMS, select the Configure > Policies screen.
2. Select a policy from the policy table.
3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable vSmart controllers to which the policy is to be applied.
4. Click Activate.

To apply a centralized policy in the CLI:



```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service  
| from-tunnel)
```

By default, data policy applies to all data traffic passing through the vEdge router: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. You can explicitly configure this behavior by including the **all** option. To have the data policy apply only to policy exiting from the local site, include the **from-service** option. To have the policy apply only to incoming traffic, include the **from-tunnel** option.

You cannot apply the same type of policy to site lists that contain overlapping site IDs. That is, all data policies cannot have overlapping site lists among themselves. If you accidentally misconfigure overlapping site lists, the attempt to commit the configuration on the vSmart controller fails.

As soon as you successfully activate the configuration by issuing a **commit** command, the vSmart controller pushes the data policy to the vEdge routers located in the specified sites. To view the policy as configured on the vSmart controller, use the **show running-config** command on the vSmart controller:

```
vSmart# show running-config policy  
vSmart# ;show running-config apply-policy
```

To view the policy that has been pushed to the vEdge router, use the **show policy from-vsmart** command on the vEdge router.

```
vEdge# show policy from-vsmart
```

### Monitor Running Applications

To enable the deep packet inspection infrastructure on the vEdge routers, you must enable application visibility on the routers:

```
vEdge(config)# policy app-visibility
```

To display information about the running applications, use the **show app dpi supported-applications**, **show app dpi applications**, and **show app dpi flows** commands on the router.

### View DPI Applications Using vManage

You can view the list of all the application-aware applications supported by the SD-WAN software on the router using the following steps:

1. In the Cisco vManage, select the **Monitor > Network** screen.
2. From the **WAN-Edge** pane, select the **Device** that supports DPI. The vManage Control Connections page displays.
3. In the left pane, select **Real Time** to view the device details.
4. From the **Device Options** drop-down, choose **DPI Applications** to view the list of applications running on the device.
5. From the **Device Options** drop-down, choose **DPI Supported Applications** to view the list of applications that are supported on the device.

## Centralized Data Policy Configuration Examples

This topic provides some examples of configuring centralized data policy to influence traffic flow across the Cisco IOS XE SD-WAN domain and to configure a Cisco IOS XE SD-WAN device to be an Internet exit point.

### General Centralized Data Policy Example

This section shows a general example of a centralized data policy to illustrate that you configure centralized data policy on a Cisco vSmart Controller and that after you commit the configuration, the policy itself is pushed to the required Cisco IOS XE SD-WAN devices.

Here we configure a simple data policy on the Cisco vSmart Controller vm9:

```
vm9# show running-config policy
policy
data-policy test-data-policy
  vpn-list test-vpn-list
  sequence 10
  match
    destination-ip 209.165.201.0/27
  !
  action drop
  count test-counter
  !
  !
  default-action drop
  !
  !
  lists
  vpn-list test-vpn-list
  vpn 1
  !
  site-list test-site-list
  site-id 500
  !
  !
  !
```

Then, apply this policy to the site list named **test-site-list**, which includes site 500:

```
vm9# show sdwan running-config apply-policy
apply-policy
  site-list test-site-list
  data-policy test-data-policy
  !
  !
```

Immediately after you activate the configuration on the Cisco vSmart Controller, it pushes the policy configuration to the Cisco IOS XE SD-WAN devices in site 500. One of these devices is vm5, where you can see that the policy has been received:

```
vm5# show sdwan policy from-vsmart
policy-from-vsmart
data-policy test-data-policy
  vpn-list test-vpn-list
  sequence 10
  match
    destination-ip 209.165.201.0/27
  !
  action drop
  count test-counter
```

```

!
!
default-action drop
!
!
lists
vpn-list test-vpn-list
vpn 1
!
!
!
!

```

### Control Access

This example shows a data policy that limits the type of packets that a source can send to a specific destination. Here, the host at source address 192.0.2.1 in site 100 and VPN 100 can send only TCP traffic to the destination host at 203.0.113.1. This policy also specifies the next hop for the TCP traffic sent by 192.0.2.1, setting it to be TLOC 209.165.200.225, color gold. All other traffic is accepted as a result of the **default-action** statement.

```

policy
lists
site-list north
site-id 100
vpn-list vpn-north
vpn 100
!
data-policy tcp-only
vpn-list vpn-north
sequence 10
match
source-ip 192.0.2.1/32
destination-ip 203.0.113.1/32
protocol tcp
action accept
set tloc 209.165.200.225 gold
!
default-action accept
!
!
apply-policy
site north data-policy tcp-only

```

### Restrict Traffic

This examples illustrates how to disallow certain types of data traffic from being sent from between VPNs. This policy drops data traffic on port 25, which carries SMTP mail traffic, that originates in 209.165.201.0/27. However, the policy accepts all other data traffic, including non-SMTP traffic from 209.165.201.0/27.

```

policy
lists
data-prefix-list north-ones
ip-prefix 209.165.201.0/27
port 25
vpn-list all-vpns
vpn 1
vpn 2
site-list north
site-id 100
!
data-policy no-mail
vpn-list all-vpns
sequence 10

```

```

        match
        source-data-prefix-list north-ones
        action drop
    !
    default-action accept
!
!
apply-policy
site north data-policy no-mail

```

## Localized Data Policy

Data policy operates on the data plane in the Cisco IOS XE SD-WAN overlay network and affects how data traffic is sent among the Cisco IOS XE SD-WAN 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 IOS XE SD-WAN device.

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

For IPv4, you can configure QoS actions.

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

You can apply access lists either in the outbound or inbound direction on the interface. Applying an IPv4 ACL in the outbound direction affects data packets traveling from the local service-side network into the IPsec tunnel toward the remote service-side network. Applying an IPv4 ACL in the inbound direction affects data packets exiting from the IPsec tunnel and being received by the local Cisco IOS XE SD-WAN device. For IPv6, an outbound ACL is applied to traffic being transmitted by the router, and an inbound ACL is applied to received traffic.

### Explicit and Implicit Access Lists

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

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

### Perform QoS Actions

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

## Localized Data Policy for IPv4

This topic provides procedures for configuring IPv4 localized data policy. This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply QoS, and policing to data packets. You can create access lists that act on unicast and multicast traffic.

In Cisco vManage NMS, you configure localized data policy from the **Configuration > Policies** screen, using a policy configuration wizard. In the CLI, you configure these policies on the Cisco IOS XE SD-WAN device.

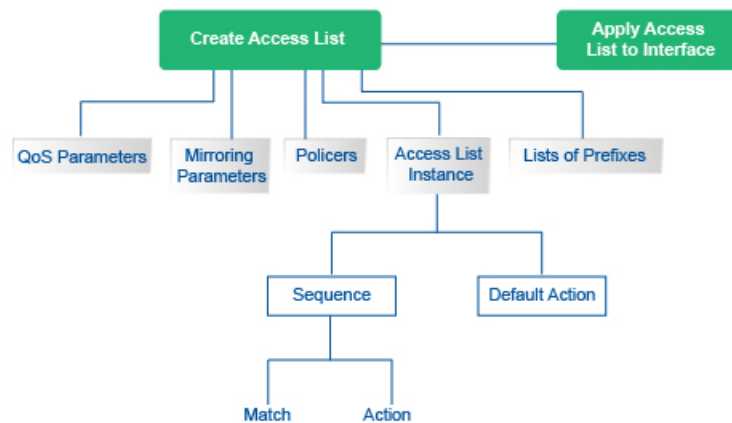
### Configuration Components

An access list consists of a sequence of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packet stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

The following figure illustrates the configuration components for access lists.

**Figure 1: Configuration Components**



## Configure Localized Data Policy for IPv4 Using Cisco vManage

**Table 2: Feature History**

Feature Name	Release Information	Description
Control Traffic Flow Using Class of Service Values	Cisco IOS XE SD-WAN Release 16.12.1b	This feature lets you control the flow of traffic into and out of a Cisco IOS XE SD-WAN device interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule.

To configure IPv4 localized policy, use the Cisco vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens to configure IPv4 localized policy components:

- Groups of Interest, also called lists—Create data prefix lists and policer parameters that group together related items and that you call in the match or action components of a policy.
- Forwarding Classes—Define forwarding classes and rewrite rules to use for QoS.
- Access Control Lists—Define the match and action conditions of ACLs.
- Route Policies—Define the match and action conditions of route policies.
- Policy Settings—Define additional policy settings, including Cloud QoS 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.

### Step 1: Start the Policy Configuration Wizard

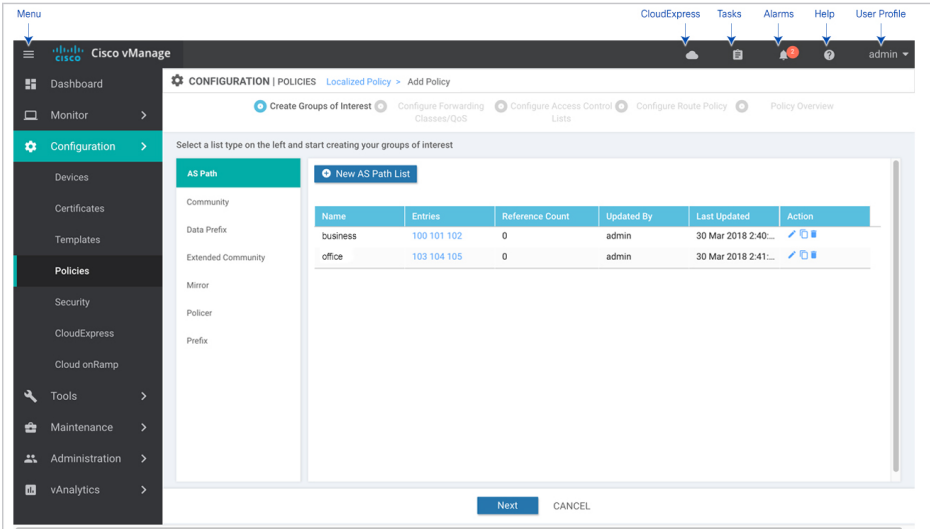
To start the policy configuration wizard:

1. In Cisco vManage NMS, select the **Configure > 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.

### Step 2: Create Groups of Interest

In the Create Groups of interest screen create lists to use in the localized data policy:



The screenshot shows the 'Create Groups of Interest' screen in Cisco vManage. The interface includes a sidebar with navigation options and a main content area with a table of existing lists. The table has the following data:

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

At the bottom of the screen, there are 'Next' and 'CANCEL' buttons.

1. Create news lists of groups, as described in the following table:

Table 3:

List Type	Procedure
Data Prefix	<ol style="list-style-type: none"> <li>1. In the left bar, click <b>Data Prefix</b>.</li> <li>2. Click <b>New Data Prefix List</b>.</li> <li>3. Enter a name for the list.</li> <li>4. Enter one or more IP prefixes.</li> <li>5. Click <b>Add</b>.</li> </ol>
Mirror	<ol style="list-style-type: none"> <li>1. In the left bar, click <b>Mirror</b>.</li> <li>2. Click <b>New Mirror List</b>. The Mirror List popup displays.</li> <li>3. Enter a name for the list.</li> <li>4. In the Remote Destination IP field, enter the IP address of the destination to which to mirror the packets.</li> <li>5. In the Source IP field, enter the IP address of the source of the packets to mirror.</li> <li>6. Click <b>Save</b>.</li> </ol>
Policer	<ol style="list-style-type: none"> <li>1. In the left bar, click <b>Policer</b>.</li> <li>2. Click <b>New Policer List</b>.</li> <li>3. Enter a name for the list.</li> <li>4. In the Burst field, enter maximum traffic burst size. It can be a value from 15000 to 10000000 bytes.</li> <li>5. In the Exceed field, select the action to take when the burst size or traffic rate is exceeded. Select <b>Drop</b> (the default) to set the packet loss priority (PLP) to low. Select <b>Remark</b> to set the PLP to high.</li> <li>6. In the Rate field, enter the maximum traffic rate. It can be value from 0 through <math>2^{64} - 1</math> bps</li> <li>7. Click <b>Add</b>.</li> </ol>

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

### Step 3: Configure Forwarding Classes for QoS

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

To configure forwarding classes for use by QoS:

1. To create a new QoS mapping:
  - a. In the QoS tab, click the **Add QoS** 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. Enter the forwarding class.
  - g. Click **Save**.
2. To import an existing QoS mapping:
  - a. In the QoS tab, click the **Add QoS** drop-down.
  - b. Select **Import Existing**.
  - c. Select a QoS mapping.
  - 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 QoS 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.  
**Low** priority is supported only for Cisco IOS XE SD-WAN devices.
  - 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**.
5. To import an existing rewrite rule:
  - a. In the QoS tab, click the **Add Rewrite Policy** drop-down..
  - b. Select **Import Existing**.
  - c. Select a rewrite rule.
  - d. Click **Import**.
6. Click **Next** to move to Configure Access Lists in the wizard.



#### Step 4: Configure ACLs

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

#### Step 5: Configure Policy Settings

In Policy Overview, configure policy settings:

1. Enter a name and description for the ACL.
2. To enable cflowd visibility so that a Cisco IOS XE SD-WAN device can perform traffic flow monitoring on traffic coming to the router from the LAN, click **Netflow**.

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

### Step 6: Apply a Localized Data Policy in a Device Template

1. In Cisco vManage NMS, 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 IOS XE SD-WAN devices.
  - d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (\_). It cannot contain spaces or any other characters.
  - e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
  - f. Continue with Step 4.
3. If you are editing an existing device template:
  - a. 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).

## Structural Components of Configuration for Access Lists

Following are the structural components required to configure access lists, shown as they appear in the CLI and when you click **Preview** in the Cisco vManage localized policy configuration wizard. Each component is explained in the sections below.

```

policy
  lists
    data-prefix-list list-name
    ip-prefix prefix/length
  class-map
    class class map map
  cloud-qos
  cloud-qos-service-side
  implicit-acl-logging
  log-frequency number
  qos-scheduler scheduler-name
    class class-name
    bandwidth-percent percentage
    buffer-percent percentage
    drops drop-type
    scheduling (llq | wrr)
  qos-map map-name
    qos-scheduler scheduler-name
  rewrite-rule rule-name
    class class-name priority dscp dscp-value layer-2-cos number
  mirror mirror-name
    remote-dest ip-address source ip-address
  policer policer-name
    rate bandwidth
    burst bytes
    exceed action
  access-list list-name
    sequence number
      match
        match-parameters
      action
        drop
          count counter-name
          log
        accept
          class class-name
          count counter-name
          log
          mirror mirror-name
          policer policer-name
          set dscp value
          set next-hop ipv4-address
      default-action
        (accept | drop)
vpn vpn-id
  interface interface-name
    access-list list-name (in | out)
    policer policer-name (in | out)
    rewrite-rule rule-name

```

### Lists

Access lists use prefix lists to group related prefixes.

In the Cisco vManage NMS, you configure prefix lists from:

- **Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest**

- **Configuration > Policies > Custom Options > Localized Policy > Lists > Data Prefix**

In the CLI, you configure lists under the **policy lists** command hierarchy on Cisco IOS XE SD-WAN devices.

**Table 4:**

List Type	Description	vManage Configuration/ CLI Configuration Command
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 <b>ip-prefix</b> options, specifying one prefix in each option.	<b>Configuration &gt; Policies &gt; Localized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Data Prefix &gt; New Data Prefix List</b> <b>Configuration &gt; Policies &gt; Custom Options &gt; Localized Policy &gt; Lists &gt; Data Prefix &gt; New Data Prefix List</b> data-prefix-list <i>list-name</i> ip-prefix <i>prefix/length</i>

## QoS Parameters

In Cisco vManage NMS, you configure QoS parameters:

- **Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest > Class Map, or Configuration > Policies > Custom Options > Localized Policy > Lists > Class Map**
- **Configuration > Policies > Localized Policy > Add Policy > Configuring Forwarding Classes/QoS, or Configuration > Policies > Custom Options > Localized Policy > Configuring Forwarding Classes/QoS**
- **Configuration > Policies > Localized Policy > Add Policy > Policy Overview, or Configuration > Policies > Custom Options > Localized Policy > Policy Overview**

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 NMS:

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

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

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

To enable QoS parameters for traffic that the Cisco IOS XE SD-WAN 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.

## Policer Parameters

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In Cisco vManage NMS, you configure policer parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > Policer**
- **Configuration > Policies > Custom Options > Centralized Policy > Lists > Policer**

In the CLI, you configure policer parameters as follows:

```
vSmart(config)# policy policer policer-name
vSmart(config-policer)# rate bps
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

**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 centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the **match plp** option.

## 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 NMS, 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 NMS, 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:

**Table 5:**

Description	vManage Configuration/ CLI Configuration Command	Value or Range
Classification map	Match Class <b>class</b> <i>class-name</i>	Name of a class defined with a <b>policy class-map</b> command.
Group of destination prefixes	Match Destination Data Prefix <b>destination-data-prefix-list</b> <i>list-name</i>	Name of a <b>data-prefix-list</b> list.
Individual destination prefix	Not available in vManage NMS <b>destination-ip</b> <i>prefix/length</i>	IP prefix and prefix length

Description	vManage Configuration/ CLI Configuration Command	Value or Range
Destination port number	Match Destination Port <b>destination-port</b> <i>number</i>	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 [-])
DSCP value	Match DSCP <b>dscp</b> <i>number</i>	0 through 63
Internet Protocol number	Match Protocol <b>protocol</b> <i>number</i>	0 through 255
Packet length	Match Packet Length <b>packet-length</b> <i>number</i>	Length of the packet. <i>number</i> 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 [-])
Group of source prefixes	Match Source Data Prefix <b>source-data-prefix-list</b> <i>list-name</i>	Name of a <b>data-prefix-list</b> list.
Packet loss priority (PLP)	Match PLP <b>plp</b>	<b>(high   low)</b> By default, packets have a PLP value of <b>low</b> . To set the PLP value to <b>high</b> , apply a policer that includes the <b>exceed remark</b> option.
Individual source prefix	Match Source Data Prefix <b>source-ip</b> <i>prefix/length</i>	IP prefix and prefix length
Source port number	Match Source Port <b>source-port</b> <i>address</i>	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 [-])
TCP flag	Match TCP <b>tcp</b> <i>flag</i>	<b>syn</b>

## 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 the Cisco vManage NMS, 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 actions 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:

**Table 6:**

Description	vManage Configuration/ CLI Configuration Parameter	Value or Range
Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the <b>action</b> portion of the access list.	Click Accept <b>accept</b>	—
Count the accepted or dropped packets.	Action Counter Click Accept, then action Counter <b>count</b> <i>counter-name</i>	Name of a counter. To display counter information, use the <b>show policy access-lists counters</b> command on the Cisco IOS XE SD-WAN device.
Discard the packet. This is the default action.	Click Drop <b>drop</b>	—

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

**Table 7:**

Description	vManage Configuration/ CLI Configuration Parameter	Value or Range
Classify the packet.	Click Accept, then Class <b>class</b> <i>class-name</i>	Name of a QoS class defined with a <b>policy class-map</b> command.
Mirror the packet.	Click Accept, then Mirror List <b>mirror</b> <i>mirror-name</i>	Name of mirror defined with a <b>policy mirror</b> command.
Police the packet.	Click Accept, then Policer <b>policer</b> <i>policer-name</i>	Name of a policer defined with a <b>policy policer</b> command.
Packet's DSCP value.	Click Accept, then DSCP <b>set dscp</b> <i>value</i>	0 through 63.
Next-hop address.	Click Accept, then Next Hop <b>set next-hop</b> <i>ipv4-address</i>	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 the Cisco vManage NMS, 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 the Cisco vManage NMS, you apply the access list in one of these interface feature configuration templates:

- **Configuration > Templates > VPN Interface Bridge**
- **Configuration > Templates > VPN Interface Cellular**
- **Configuration > Templates > VPN Interface Ethernet**
- **Configuration > Templates > VPN Interface GRE**
- **Configuration > Templates > VPN Interface PPP**
- **Configuration > Templates > VPN Interface PPP Ethernet**

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

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

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

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

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

**Table 8:**

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

## Configure Localized Data Policy for IPv4 Using the CLI for Cisco IOS XE SD-WAN Devices

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

1. Create lists of IP prefixes, as needed:

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

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

```
Device(config)# class-map match-any class1
Device(config)# match qos-group 1
class-map match-any class6
match qos-group 6
class-map match-any class7
match qos-group 7
class-map match-any class4
match qos-group 4
class-map match-any class5
match qos-group 5
class-map match-any class2
match qos-group 2
class-map match-any class3
match qos-group 3
class-map match-any class1
match qos-group 1
end
```



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

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

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

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

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

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

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

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

6. Configure a WAN interface without a shaping configuration:

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

7. Configure a WAN interface with a shaping configuration:

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

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

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

### 9. Define policing parameters:

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

### 10. Associate an access list set to policer:

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

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

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

## Localized Data Policy for IPv6

This topic provides procedures for configuring IPv6 localized data policy. This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply policing to data packets.

For IPv6, you can apply access lists only to interfaces in the transport VPN, VPN 0.

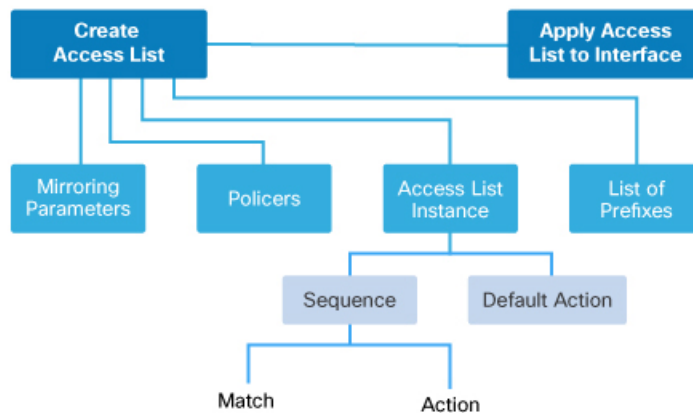
In Cisco vManage NMS, you configure localized data policy from the **Configuration > Policies** screen, using a policy configuration wizard. In the CLI you configure these policies on the Cisco IOS XE SD-WAN device.

### Configuration Components

An access list consists of a sequence of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packet stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

The following figure illustrates the configuration components for IPv6 access lists:



368534

## Configure Localized Data Policy for IPv6 Using vManage

To configure IPv6 localized data policy, use the Cisco vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens, and you use four of them to configure IPv6 localized policy components:

- Groups of Interest, also called *lists*—Create data prefix lists and policer parameters that group together related items and that you call in the match or action components of a policy.
- Access Control Lists—Define the match and action conditions of ACLs.
- Route Policies—Define the match and action conditions of route policies.
- Policy Settings—Define additional 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.

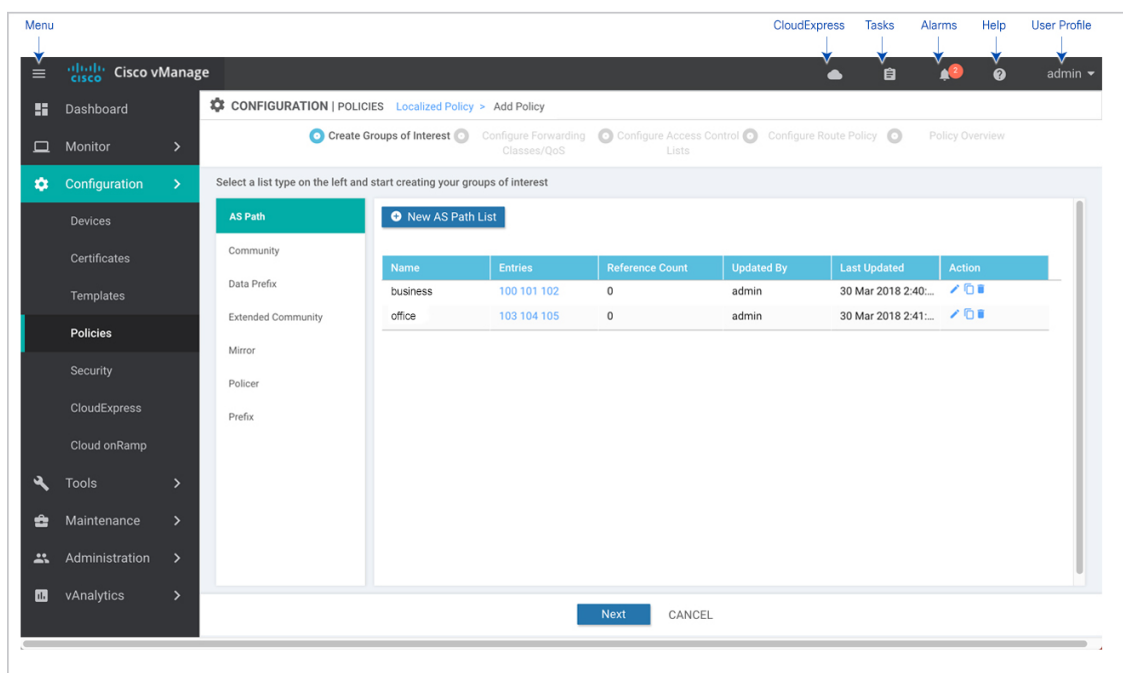
### Step 1: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In Cisco vManage NMS, select the **Configure > Policies** screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Select the **Localized Policy** tab.
3. Click **Add Policy**. The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

### Step 2: Create Groups of Interest

In the Create Groups of interest screen create lists to use in the localized data policy:



368398

1. Create news lists of groups, as described in the following table:

List Type	Procedure
AS Path	<p>Permit or deny prefixes from certain autonomous systems.</p> <ol style="list-style-type: none"> <li>In the left bar, click <b>AS Path</b>.</li> <li>Enter a name for the list. For Cisco IOS XE SD-WAN devices: Enter a number from 1 to 500.</li> <li>Set the preference value for the list in the <b>Add AS Path</b> field.</li> </ol>
Community	<ol style="list-style-type: none"> <li>In the left bar, click <b>Community</b>.</li> <li>Click <b>New Community List</b>.</li> <li>Enter a name for the list.</li> <li>In the <b>Add Community</b> field, enter one or more data prefixes separated by commas.</li> <li>Click <b>Add</b>.</li> </ol>

List Type	Procedure
Data Prefix	<p><b>a.</b> In the left bar, click <b>Data Prefix</b>.</p> <p><b>b.</b> Click <b>New Data Prefix List</b>.</p> <p><b>c.</b> Enter a name for the list.</p> <p><b>d.</b> In the Internet Protocol field, click <b>IPv4</b> or <b>IPv6</b>.</p> <p><b>e.</b> In the <b>Add Data prefix</b> field, enter one or more data prefixes separated by commas.</p> <p><b>f.</b> Click <b>Add</b>.</p>
Extended Community	<p><b>a.</b> In the left bar, click <b>Extended Community</b>.</p> <p><b>b.</b> Click <b>New Extended Community List</b>.</p> <p><b>c.</b> Enter a name for the list.</p> <p><b>d.</b> In the <b>Add Extended Community</b> field, enter one or more data prefixes separated by commas.</p> <p><b>e.</b> Click <b>Add</b>.</p>
Class Map	<p>Map a class name to an interface queue number.</p> <p><b>a.</b> In the left bar, click <b>Class Map</b>.</p> <p><b>b.</b> Click <b>New Class List</b>. The Class List popup displays.</p> <p><b>c.</b> Enter a name for the list. The class name can be a text string from 1 to 32 characters long.</p> <p><b>d.</b> Select a queue number between 0 and 7 from the <b>Queue</b> drop-down menu.</p> <p><b>e.</b> Click <b>Save</b>.</p>
Mirror	<p>Define the remote destination for mirrored packets, and define the source of the packets.</p> <p><b>a.</b> In the left bar, click <b>Mirror</b>.</p> <p><b>b.</b> Click <b>New Mirror List</b>.</p> <p><b>c.</b> Enter a name for the list.</p> <p><b>d.</b> Enter the <b>Remote Destination IP</b> address in the left field, where the mirrored traffic should be routed.</p> <p><b>e.</b> Enter the <b>Source IP</b> address of the mirrored traffic in the right field.</p> <p><b>f.</b> Click <b>Add</b>.</p>

List Type	Procedure
Policer	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>Policer</b>.</li> <li>b. Click <b>New Policer List</b>.</li> <li>c. Enter a name for the list.</li> <li>d. Define the policing parameters: <ol style="list-style-type: none"> <li>1. In the <b>Burst</b> field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.</li> <li>2. In the <b>Exceed</b> field, select the action to take when the burst size or traffic rate is exceeded. It can be <b>drop</b>, which sets the packet loss priority (PLP) to low, or <b>remark</b>, which sets the PLP to high.</li> <li>3. In the <b>Rate</b> field, enter the maximum traffic rate, a value from 0 through 264 – 1 bits per second (bps).</li> </ol> </li> <li>e. Click <b>Add</b>.</li> </ol>
Prefix	<ol style="list-style-type: none"> <li>a. In the left bar, click <b>Prefix</b>.</li> <li>b. Click <b>New Prefix List</b>.</li> <li>c. Enter a name for the list.</li> <li>d. Click either <b>IPv4</b> or <b>IPv6</b>.</li> <li>e. Under <b>Add Prefix</b>, enter the prefix for the list. (An example is displayed.) Optionally, click the green <b>Import</b> link on the right-hand side to import a prefix list.</li> <li>f. Click <b>Add</b>.</li> </ol>

2. Click **Next** to move to Configure Forwarding Classes/QoS in the wizard. For IPv6 localized data policy, you cannot configure QoS.
3. Click **Next** to move to Configure Access Lists in the wizard.

### Step 3: Configure ACLs

1. In the Configure Access Control Lists screen, click **Add Access Control List Policy**, and choose **Add IPv6 ACL Policy** from the drop-down.
2. Enter a name and description for the ACL.
3. From the left column, click **Add ACL Sequence**.
4. Click **Sequence Rule** to open the ACL match/action sequence menu.
5. Click a match condition. See [Match Parameters](#) for a full description of these options.
6. On the left side, enter the values for the match condition.



7. On the right side, enter the action or actions to take if the policy matches. See [Action Parameters](#) for a full description of these options.
8. Repeat Steps 3 through 7 to add match–action pairs to the ACL.
9. To rearrange match–action pairs in the ACL, drag them to the desired position in the right pane.
10. To remove a match–action pair from the ACL, click the X in the upper right of the condition.
11. Click **Save Match and Actions** to save a sequence rule.
12. To copy, delete, or rename an ACL sequence rule, in the left pane, click the **More Options** menu (three dots) next to the rule's name and select the desired option.
13. 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**.
14. Click **Next** to move to Configure Route Policy in the wizard.
15. Click **Next** to move to the Policy Overview screen.

#### Step 4: Configure Policy Settings

In Policy Overview, configure policy settings:

1. Enter a name and description for the ACL.
2. Under **Policy Settings**, select one of the following policy options:

Policy Settings Options	Description
Netflow	
Application	
Cloud QoS	
Cloud QoS Service side	
Implicit ACL Logging	Log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface.

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

### Step 5: Apply a Localized Data Policy in a Device Template

1. In Cisco vManage NMS, 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 a Cisco IOS XE SD-WAN device.
  - 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).

## Structural Components of Configuration for Access Lists

Following are the structural components required to configure access lists. Each one is explained in more detail in the sections below.

```

policy
  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
      count 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)

```

## Policer Parameters

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In the Cisco vManage NMS, you configure policer parameters from:

- **Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest > Policer > New Policer List**
- **Configuration > Policies > Custom Options > Localized Policy > Lists > Policer > New Policer List**

In the CLI, you configure policer parameters as follows:

```

Device(config)# policy policer policer-name
Device(config-policer)# rate bps
Device(config-policer)# burst bytes
Device(config-policer)# exceed action

```

- **rate** is the maximum traffic rate. It can be a value from 0 through  $2^{64} - 1$  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 centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the **match plp** option.

## Sequences

### 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 the Cisco vManage NMS, 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 ipv6 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 NMS, 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 ipv6 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	vManage Match Tab / CLI Command	Value or Range
Enter a Destination port number.	Destination Port <b>destination-port</b> <i>number</i>	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 [-])
Select the Next Header protocol.	Protocol <b>next-header</b> <i>number</i>	0 through 255, corresponding to an <a href="#">Internet Protocol number</a>
Specify the packet length	Packet Length <b>packet-length</b> <i>number</i>	Length of the packet. <i>number</i> 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 [-])
Specify the packet loss priority (PLP)	PLP <b>plp</b>	<b>(high   low)</b> By default, packets have a PLP value of <b>low</b> . To set the PLP value to <b>high</b> , apply a <a href="#">policer</a> that includes the <b>exceed remark</b> option.
Select a Source data prefix list		
Enter a Source port number	Source Port <b>source-port</b> <i>address</i>	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 [-])
Enter a Destination Data Prefix		
TCP	TCP <b>tcp</b> <i>flag</i>	<b>syn</b>
Set the packet's DSCP value	Class <b>set class</b> <i>value</i>	0 through 63
Traffic class	Traffic Class <b>traffic-class</b> <i>value</i>	0 through 63

## 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 NMS, 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 actions parameters with the **policy ipv6 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:

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

Description	vManage Action Tab / CLI Command	Value or Range
Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the <b>action</b> portion of the access list.	Click <b>Accept</b> . <b>accept</b>	—
Count the accepted or dropped packets.	<b>Counter Name</b> <b>count</b> <i>counter-name</i>	Name of a counter. To display counter information, use the <b>show ipv6 policy access-lists counters</b> command on the Cisco IOS XE SD-WAN device.
Designate the next hop router.	<b>Next Hop</b>	
Traffic Class	<b>set traffic-class</b> <i>value</i>	0-63
Mirror the packet.	Mirror List <b>mirror</b> <i>mirror-name</i>	Name of mirror defined with a <b>policy mirror</b> command.
Set the packet's DSCP value.	Class	0 through 63
Police the packet.	Policer <b>policer</b> <i>policer-name</i>	Name of a policer defined with a <b>policy policer</b> command.
Discard the packet. This is the default action.	Click <b>Drop</b> . <b>drop</b>	—

## 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 the Cisco vManage NMS, 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 ipv6 default-action accept` command.

## Apply Access Lists

For an access list to take effect, you must apply it to a tunnel interface in VPN 0.

In the Cisco vManage NMS, you apply the access list in one of the interface feature configuration templates.

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

```
vEdge(config)# vpn 0 interface interface-name
vEdge(config-interface)# ipv6 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.

## 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 router.

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

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

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

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

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

- Whether the implicit ACL is configured as allow (`allow-service allow-service`) 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 for an implicit and an explicit ACL is handled:

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 Localized Data Policy for IPv6 Using the CLI

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

1. Define policing parameters:

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

2. Create an access list instance:

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

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

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

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

4. Define match parameters for packets:

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

5. Define actions to take when a match occurs:

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

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

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

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

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

## Localized Data Policy Configuration Examples

This topic provides some straightforward examples of configuring localized data policy to help you get an idea of how to use policy to influence traffic flow across the Cisco 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.