



Application Priority and SLA

- [Feature history for policy groups, on page 1](#)
- [Application Priority and SLA, on page 1](#)
- [Create an application priority and SLA policy, on page 2](#)
- [Configure traffic policy, on page 4](#)
- [Advanced layout, on page 5](#)
- [Policy sequence generation for match and action rules, on page 7](#)
- [Monitor traffic flow, on page 16](#)

Feature history for policy groups

Table 1: Feature history

Feature Name	Release Information	Description
Configure Traffic and Flow Visibility for Application Priority and SLA Policy	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can configure settings to enable traffic and flow visibility for the application priority and SLA policy in Cisco Catalyst SD-WAN. This feature allows you to monitor application and traffic flow over IPv4, IPv6, or both networks at the global hierarchy level in Cisco SD-WAN Manager.
Preferred Remote Color in AAR Policy	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	You can set a remote preferred color in the AAR policy to control traffic routing based on the SLA criteria.

Application Priority and SLA

An application priority and SLA policy is a traffic policy group that

- configures app route policy, data policy, and QoS Map policies,

- routes and prioritizes traffic for best performance, and
- manages and customizes bandwidth allocations while prioritizing applications based on their relevance to your business.

Create an application priority and SLA policy

Follow these steps to create or edit an application priority and sLA policy.

Procedure

Step 1 Click + **Application priority & SLA policy**.

Step 2 To edit an existing policy, click the ellipsis icon next to the policy under **Action**, and then click **Edit**.

Step 3 Choose one of these business relevance categories:

- **Gold** (Business-relevant): Likely to be important for business operations, for example, WebEx software.
- **Silver** (Default): No determination of relevance to business operations.
- **Bronze** (Business-irrelevant): Unlikely to be important for business operations, for example, gaming software.

Within each business relevance category, the workflow groups applications into application lists, such as broadcast video, multimedia conferencing, and VoIP telephony.

Note

When you upgrade Cisco SD-WAN Manager, built-in protocol pack gets updated. This might affect the existing policy groups which are using the Application priority and SLA policy in the non-advanced layout. You need to redeploy the policies when there is an upgrade. If policy is in the advanced layout, the upgrade will not affect the policy group.

Table 2: Fabric traffic policy

Field	Description
Preferred Path	To configure a preferred path, choose one or more colors of the data plane tunnel or tunnels from the drop-down list. Traffic is load-balanced across all the tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. The preferences apply in order of priority to determine the path or color for forwarding traffic.
When SLA not met	Choose Strict/Drop to perform strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Choose Fallback to best path to configure the best available tunnel to avoid a packet drop. This is the default. Backup Path : Path for traffic to use if the primary path fails.

Field	Description
Backup Path	To configure an alternate path for traffic flow, choose a path from the drop-down list.
Traffic Filtering	Click Edit to view and update app classification based on the business relevance. Choose a service provider class option and drag and drop the applications into different classes such as Gold or Bronze and click Save to update the configuration.
SLA	Add the SLA class in the traffic policy. Click Edit to configure the SLA class by adjusting the values for Loss (%), Latency (ms), or Jitter (ms) for the traffic policy.
QoS Queues	Click Add QoS Policy to add a QoS queue. Click Edit to configure the QoS Queues. Choose one of the following values for the QoS queuing model: • 4 Queues • 5 Queues • 6 Queues • 8 Queues

Table 3: Internet Offload Traffic

Field	Description
Secure Internet Gateway	Choose an application or application family list to tunnel traffic through a Secure Internet Gateway. Enable Fallback to routing for traffic to undergo normal routing if the SIG tunnels are down. Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, you can choose a Cloud OnRamp for SaaS-capable application (Cloud OnRamp for SaaS applications with common user defined endpoints) from the Secure Internet Gateway dropdown.
Direct Internet Access	Select an application or application family list to allow direct internet access. Enable Fallback to routing for traffic to undergo normal routing if Direct Internet Access (DIA) is not available. Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, you can choose a Cloud OnRamp for SaaS-capable application (Cloud OnRamp for SaaS applications with common user defined endpoints) from the Direct Internet Access dropdown.

Table 4: Apply Policy

Field	Description
Target	Configure the following parameters: • Direction : Choose the direction for applying the policy: • All : Bidirection traffic flow • Service : Incoming traffic from service. • Tunnel : Incoming traffic from the tunnel. • VPN : Choose a target VPN from the drop-down list. • Interface : Specify a value or a variable for the Ethernet interface or DSL PPPoE interface type for applying the QoS policy.

Configure traffic policy

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > Application priority and SLA**.
- Step 2** Click + **Application priority & SLA policy** to create a policy or edit an existing policy by clicking the ellipsis icon.
- Step 3** Click the **Advanced** button on the top-right corner of the window to switch to the advanced view.

Note

If you make changes to the application priority and SLA policies and switch to the advanced layout, the changes are retained. You cannot switch back to the default view.

- Step 4** Click + **Add Traffic Policy** to configure the traffic policy.

Table 5: Add Traffic Policy

Field	Description
Policy Name	Specify a name for the traffic-rule sequence. From Cisco IOS XE Catalyst SD-WAN Release 26.2.1, the maximum length of the policy name is 128 characters. Cisco SD-WAN Manager UI and API validation reject values longer than 128 characters.
VPN	Choose a VPN from the drop-down list.

Field	Description
Direction	- Choose the direction for applying the policy: All : Bidirectional traffic flow Service : Incoming traffic from service Tunnel : Incoming traffic from tunnel

Step 5 Click + **Add rules** to configure rules.

Table 6: Add Rules

Field	Description
Sequence	The sequence number of the rule.
Name	Specify a name for the rule.
Protocol	Choose a protocol from the drop-down list: IPv4 IPv6 Both
Match	Choose a value for the match condition from the available options. Refer to Match conditions, on page 8 table.
Action	Choose a value for the action to take if the policy matches, from the available options. Refer to Action conditions, on page 10 table.
Base Action	Choose one of the following base actions for the packets based on the rules: Accept Drop

To rearrange match–action pairs in the route policy, drag them to the desired position and click **Save Match and Actions**.

Advanced layout

The advanced view provides further options to configure the traffic policy along with rules, service level agreement (SLA) class, and QoS Map.



Note If you make changes to the application priority and SLA policies and switch to the advanced layout, the changes are retained. You cannot switch back to the default view.

Based on the values you configure in the workflow, a policy profile and the relevant policy objects are created in the back-end when the workflow is completed. Similarly, you can configure traffic filtering and rules by creating the match and action conditions of a policy. You can also configure the app route policy SLA class and create customized QoS queues.

The VPNs that you intend to use in policy group must be present in service or transport profile of configuration group.

You can identify the VPNs when you configure VPNs using configuration groups as VPNs are identified with VPN name. Where as, when you configure VPNs from CLI template, VPNs are identified by VPN IDs. Hence, you cannot read the VPNs in policy groups when they are configured in CLI.

Configure SLA class

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > Application Priority & SLA**.
- Step 2** Create or edit an existing application priority and SLA policy and select **Advanced Mode**.
- Step 3** Create a traffic policy to add your first SLA class in traffic policy.
- Select the base action as **Accept**. Click **Add action** and select **SLA class**. Refer to [Action conditions, on page 10](#).

Table 7: SLA Class Components

Parameter	Description
jitter <i>milliseconds</i>	The maximum jitter on the connection Range: 1–1000 milliseconds
latency <i>milliseconds</i>	The maximum packet latency on the connection Range: 1–1000 milliseconds
loss <i>percentage</i>	The maximum packet loss on the connection Range: 1–100 percent

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a , the SLA class loss, latency, and jitter values are as follows:

- Default values: Loss 5%, latency 500 ms, jitter 500 ms
- Business relevant values: Loss 2%, latency 300 ms, jitter 60 ms
- Business irrelevant values: Loss 10%, latency 600 ms, jitter 600 ms
- Bulk data values: Loss 5%, latency 500 ms, jitter 500 ms

Step 4 Click **Save match and actions**.

Configure QoS policy

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > Application Priority & SLA**.
- Step 2** Create or edit an existing application priority and SLA policy and select **Advanced Mode**.
- Step 3** From the left pane, click **QoS queue**, and then click **Add QoS policy**.

Table 8: QoS Queue

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

Step 4 Click **Save**.

Policy sequence generation for match and action rules

The workflow generates data policy and app-route policy sequences based on the match and action conditions configured in a traffic rule. The following rules apply:

- A data policy sequence is generated when the rule includes a data match condition, a data action, or both. If no match condition is configured but a data action is configured, the workflow also generates a data policy sequence.

- An app-route policy sequence is generated when the rule includes an app-route match condition, an app-route action, or both. The workflow also generates an app-route policy sequence for a common-only sequence if a data policy sequence is not already generated for that sequence.
- If the rule includes only the Cloud Monitoring action, the workflow drops the sequence. If the Cloud Monitoring action is configured with other actions, the workflow evaluates the sequence according to the data policy and app-route policy sequence generation rules.
- If both the match and action conditions are empty, the workflow generates an empty data policy sequence.
- For the Cloud OnRamp for SaaS excluded data prefix use case, if the rule includes an application list and either a destination data prefix list or destination IP address with the count action, the workflow also generates an app-route policy sequence.

Match conditions

Table 9: Match parameters - data policy and app-route policy

Match Condition	Description
Omit	Match all packets.
(Applicable only to app-route policy) Cloud Saas Application List	Cisco SD-WAN Manager provides a list of several cloud applications that Cisco Catalyst SD-WAN Cloud OnRamp for SaaS can use to determine the best path selection for each SaaS application. For more information on Cisco Catalyst SD-WAN Cloud OnRamp for SaaS, see the <i>Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x</i>. Note Cloud Saas Application List displays as a match condition if you specify IPv4 as the Protocol option. In the drop-down list, choose a SaaS application from the drop-down list.
(Applicable only to data policy) Packet length	Specifies the packet length. The range is 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 [-]).
(Applicable only to data policy) TCP Flag	Specifies the TCP flag, syn.
Applications/Application Family List	Applications or application families. This match condition is available for IPv6 traffic from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1.
Destination Data Prefix	Group of destination prefixes, IP prefix and prefix length. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
Destination Port	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 [-]).

Match Condition	Description
Destination Region	Choose one of the following: • Primary: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using a multi-hop path, through the core region. • Secondary: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions. • Other: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination. Note Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a
DNS	Specify the direction in which to process DNS packets. To process DNS requests sent by the applications (for outbound DNS queries), specify dns request . To process DNS responses returned from DNS servers to the applications, specify dns response .
DNS Application List	Enables split DNS, to resolve and process DNS requests and responses on an application-by-application basis. Name of an app-list list. This list specifies the applications whose DNS requests are processed. This match condition is available for IPv6 traffic from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1.
DSCP	Specifies the DSCP value.
ICMP Message	For Protocol IPv4 when you enter a Protocol value as 1, the ICMP Message field displays where you can select an ICMP message to apply to the data policy. Likewise, the ICMP Message field displays for Protocol IPv6 when you enter a Protocol value as 58. When you select Protocol as Both, the ICMP Message or ICMPv6 Message field displays. Note This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.
Packet Loss Priority (PLP)	Specifies the packet loss priority. By default, packets have a PLP value of low . To set the PLP value to high , apply a policer that includes the exceed remark option.
Protocol	Specifies Internet protocol number. The range is 0 through 255.
Source Data Prefix	Specifies the group of source prefixes or an individual source prefix.
Source Port	Specifies the source port number. The range is 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 [-]).

Match Condition	Description
Traffic To	In a Multi-Region Fabric architecture, match border router traffic flowing to the access region that the border router is serving, the core region, or a service VPN. Note Minimum release: Cisco vManage Release 20.8.1

Action conditions

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

Table 10: Action conditions - data policy and app-route policy

Action Condition	Description
Click Accept	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.
Click Drop	Discards the packet. This is the default action. When you choose this option, then only Counter and Log can be added as additional actions and all other actions are not available to select. From Cisco IOS XE Catalyst SD-WAN Release 26.2.1, IPv6 high-priority traffic follows the same behavior as IPv4 high-priority traffic. High-priority traffic is skipped by policy processing and is not dropped by a policy sequence, even when the default action is set to Drop. This behavior applies only to packets consumed by the local router. If the packets are forwarded to another device, policy processing still applies.
Counter	Counts the accepted or dropped packets. Specifies the name of a counter. Use the show policy access-lists counters command on the Cisco IOS XE Catalyst SD-WAN device.
Log	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1 Click Log to enable logging. When (DP, AAR or ACL) data policy packets are configured with log action, logs generated and logged to syslog. Due to the global log-rate-limit , not all logs are logged. A syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active. For information on policy log-rate-limit CLI, see policy log-rate-limit command in the Cisco Catalyst SD-WAN Qualified Command Reference Guide .
(Applicable only to app-route policy) Cloud SLA	Cloud SLA enables traffic to use the best path selection with Cisco Catalyst SD-WAN Cloud OnRamp for SaaS. Click Cloud SLA .

Action Condition	Description
(Applicable only to app-route policy) SLA Class List	

Action Condition	Description
	Choose from the following options: SLA Class List Set the policy action for an SLA Class List match condition. For the SLA class, all matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The device first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels. Click SLA Class List. In the SLA Class drop-down list, choose one or more SLA classes. Preferred Color In the Preferred Color drop-down list, choose the color of the data plane tunnel or tunnels to prefer. Traffic is load-balanced across all the tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. That is, color preference is a loose matching, not a strict matching. Preferred Color Group When the Preferred Color is not selected, you can choose the preferred color group from the Preferred Color Group drop-down list. Select the preferred color group of the data plane tunnel or tunnels to prefer. You can configure up to three levels of priority based on the color or path preference. This field is available from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1. Restrict to Preferred Color This option is applicable only with Preferred Color Group. Check the Restrict to Preferred Color option to drop traffic if no tunnels match the SLA in the preferred color group. When there is no SLA match you can choose the following options: Strict/Drop Click Strict/Drop to perform strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Fallback to best path Click Fallback to best path to select the best available tunnel to avoid a packet drop. You can select the Fallback to best path action only when the Fallback Best Tunnel option is enabled while defining a SLA class. If the Fallback Best Tunnel option is not enabled, then

Action Condition	Description
	the following error message displays in Cisco SD-WAN Manager: SLA Class selected, does not have Fallback Best Tunnel enabled. Please change the SLA class or change to Strict/Drop. c. Load-balance. Click Load Balance to load balance traffic across all the tunnels. You can now select the Backup SLA Preferred Color. Set the policy action for a Backup SLA Preferred Color match condition. When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel interface is not available, traffic is sent out to another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching condition, not a strict matching condition. 6. Remote Preferred Color Set a Remote Preferred Color in the AAR policy to control traffic routing based on the application list. You can add multiple remote preferred colors in the AAR policy. Use the Restrict to Remote Color to restrict the tunnel to preferred TLOCs. With Restrict to Remote Color option, the traffic drops when the SLA is not met with the preferred remote color.
(Applicable only to data policy) Cflowd	Enables cflowd traffic monitoring.
(Applicable only to data policy) DSCP	DSCP value. The range is 0 through 63.
(Applicable only to data policy) Forwarding Class	Name of the forwarding class.
(Applicable only to data policy) Local TLOC	Enables sending packets to one of the TLOCs that matches the color and encapsulation. The available colors are: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red and silver. The encapsulation options are: ipsec and gre. 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 restrict option. By default, encapsulation is ipsec.

Action Condition	Description
(Applicable only to data policy) NAT Pool or NAT VPN	Enables NAT functionality, so that traffic can be redirected directly to the internet or other external destination. You can configure up to 31 (1–31) NAT pools per router.
(Applicable only to data policy) Next Hop	Sets the next hop IP address to which the packet should be forwarded. Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1, the Use Default Route when Next Hop is not available field is available next to the Next Hop action parameter. This option is available only when the sequence type is Traffic Engineering or Custom , and the protocol is either IPv4 or IPv6 , but not both.
(Applicable only to data policy) Policer	Applies a policer. Specifies the name of policer configured with the policy policer command.
(Applicable only to data policy) Redirect DNS	Redirects DNS requests to a particular DNS server or Umbrella. Redirecting requests is optional, but if you do so, you must specify both actions. For an inbound policy, redirect-dns host 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. redirect-dns umbrella is only supported in Direct Internet Interface (DIA) use cases. It is not supported in SIG/SSE or overlay scenarios. When using redirect-dns umbrella , you do not need to explicitly configure nat use-vpn 0 . Note When you upgrade to releases later than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you must configure redirect DNS through nat use-vpn 0 to redirect DNS to Direct Internet Interface (DIA). Note You can set only local TLOC preferences with redirect-dns as actions on the same sequence, but not remote TLOC. Note You cannot configure Redirect DNS and SIG at the same time. NAT DIA fallback and redirect-dns IP actions are supported at the same time in data policy beginning with Cisco IOS XE Catalyst SD-WAN Release 26.1.1.

Action Condition	Description
(Applicable only to data policy) Remote Preferred Color	Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1 You can set a preferred remote color in the AAR policy to control traffic routing based on the application list. Use the Restrict to Remote Color option to drop traffic if the selected remote color does not meet the SLA.
(Applicable only to data policy) Secure Internet Gateway	Redirect application traffic to a SIG. Note Before you apply a data policy for redirecting application traffic to a SIG, you must have configured the SIG tunnels. For more information on configuring Automatic SIG tunnels, see Automatic Tunnels . For more information on configuring Manual SIG tunnels, see Manual Tunnels. Check the Fallback to Routing check box to route internet-bound traffic through the Cisco SD-WAN overlay when all SIG tunnels are down. This option is introduced in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1.
(Applicable only to data policy) Secure Service Edge	Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1 Redirect application traffic to a Secure Service Edge instance. For more information on configuring Automatic tunnels on Cisco Secure Access, see Automatic Tunnels . Check the Fallback to Routing check box to route internet-bound traffic through the Cisco SD-WAN overlay when all Secure Service Edge tunnels are down.
(Applicable only to data policy) Service	Specifies a service to redirect traffic to before delivering the traffic to its 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. Standard services: FW, IDS, IDP Custom services: netsvc1, netsvc2, netsvc3, netsvc4 TLOC list is configured with a policy lists tloc-list list. Configure the services themselves on the Cisco IOS XE Catalyst SD-WAN devices that are collocated with the service devices, using the vpn service command.

Action Condition	Description
(Applicable only to data policy) TLOC	Direct traffic to a remote TLOC that 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.
(Applicable only to data policy) VPN	Set the VPN that the packet is part of. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here .

Monitor traffic flow

To enable traffic flow monitoring while configuring an application priority & SLA policy configure the following values:

This feature provides options to monitor traffic flow on incoming packets in the LAN for application and flow visibility over IPv4, IPv6, or both network addresses.



Note The Cflowd configuration applies to the global level and not the site level.

The additional settings that you configure are applied to the Cisco SD-WAN Controllers while deploying the application priority and SLA policy. For more information about configuring Cflowd, refer to Configure Cflowd section in *Cisco Catalyst SD-WAN Network Hierarchy Configuration Guide*.

Before you begin

- Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a , Cisco Catalyst SD-WAN Manager Release 20.13.1.
- Ensure that you have configured Cflowd collector details in the Cisco SD-WAN Manager menu from **Configuration > Network Hierarchy > Collectors > Cflowd**.

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > Application Priority & SLA**.
- Step 2** Create or edit an existing application priority and SLA policy.
- Step 3** Click **Additional settings**.

Table 11: Additional Settings

Field	Description
Application Visibility	Monitor all the applications running in all VPNs over IPv4, IPv6, or both networks in the LAN.
Flow Visibility	Monitor traffic flow over IPv4, IPv6, or both network addresses in the LAN.

Step 4 Click **Save**.
