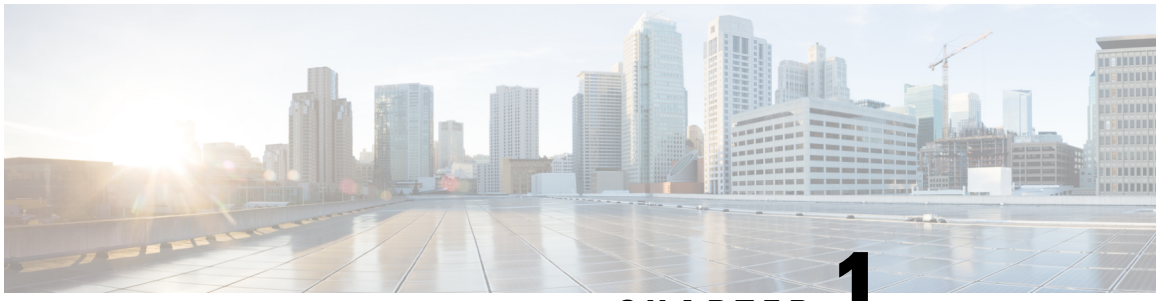


Cisco Catalyst SD-WAN Network-Wide Path Insight User Guide, Releases 26.x and Later

First Published: 2026-04-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Network-Wide Path Insight

Table 1: Feature History

Feature Name	Release Information	Description
Network-Wide Path Insight in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature lets you view network-wide path tracing information using Cisco SD-WAN Manager.
Network-Wide Path Insight in Cisco SD-WAN Manager Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature provides enhancements to network-wide path insight tracing to include additional filters and options for traces, DNS domain discovery, and new displays for application flows, trace views, and app trends.
Network-Wide Path Insight in Cisco SD-WAN Manager Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature provides enhancements to the Network-Wide Path Insight feature to include the collection and display of insight information, trace-level insight information, path insight information, and detailed application trace information.
Network-Wide Path Insight in Cisco SD-WAN Manager Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature provides enhancements to the Network-Wide Path Insight feature to include support for multiple VPNs for traces, the ability to generate synthetic traffic for traces, options for grouping trace information, support for auto-on tasks, new information on insight displays, and expanded insight summaries.

Feature Name	Release Information	Description
Network-Wide Path Insight Integration with Cisco Identity Services Engine	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	When you integrate the Cisco Identity Service Engine with Cisco Catalyst SD-WAN, this feature enables traces to provide the identity of users who send traffic to and receive traffic from applications.
Network-Wide Path Insight Integration with Cisco ThousandEyes	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	With this feature, network-wide path insight presents test results from a Cisco ThousandEyes Enterprise Agent and includes this information in flow results for your review and analysis. This information supplements data that the Cisco ThousandEyes Dashboard provides.
Insight into IPsec Failures	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature provides granular visibility into the IPsec drops.
Synthetic Traffic Packet Capture Replay	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	With this feature, you can simulate traffic of a trace by replaying a PCAP file.
SD-WAN Analytics integration and automation	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	NWPI provides scheduled automation, new event triggers, deeper policy and IPsec visibility, and cloud integration for advanced network troubleshooting and data management.

- Network-Wide Path Insight, on page 3
- Information About Network-Wide Path Insight, on page 4
- Supported Devices for Network-Wide Path Insight, on page 4
- Prerequisites for Network-Wide Path Insight, on page 5
- Restrictions for Network-Wide Path Insight, on page 5
- Use Cases for Network-Wide Path Insight, on page 8
- Configure Cisco ThousandEyes Username and OAuth Bearer Token, on page 8

Network-Wide Path Insight

Table 2: Feature History

Feature Name	Release Information	Description
Network-Wide Path Insight in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature lets you view network-wide path tracing information using Cisco SD-WAN Manager.
Network-Wide Path Insight in Cisco SD-WAN Manager Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature provides enhancements to network-wide path insight tracing to include additional filters and options for traces, DNS domain discovery, and new displays for application flows, trace views, and app trends.
Network-Wide Path Insight in Cisco SD-WAN Manager Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature provides enhancements to the Network-Wide Path Insight feature to include the collection and display of insight information, trace-level insight information, path insight information, and detailed application trace information.
Network-Wide Path Insight in Cisco SD-WAN Manager Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature provides enhancements to the Network-Wide Path Insight feature to include support for multiple VPNs for traces, the ability to generate synthetic traffic for traces, options for grouping trace information, support for auto-on tasks, new information on insight displays, and expanded insight summaries.
Network-Wide Path Insight Integration with Cisco Identity Services Engine	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	When you integrate the Cisco Identity Service Engine with Cisco Catalyst SD-WAN, this feature enables traces to provide the identity of users who send traffic to and receive traffic from applications.

Feature Name	Release Information	Description
Network-Wide Path Insight Integration with Cisco ThousandEyes	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	With this feature, network-wide path insight presents test results from a Cisco ThousandEyes Enterprise Agent and includes this information in flow results for your review and analysis. This information supplements data that the Cisco ThousandEyes Dashboard provides.
Insight into IPsec Failures	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature provides granular visibility into the IPsec drops.
Synthetic Traffic Packet Capture Replay	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	With this feature, you can simulate traffic of a trace by replaying a PCAP file.
SD-WAN Analytics integration and automation	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	NWPI provides scheduled automation, new event triggers, deeper policy and IPsec visibility, and cloud integration for advanced network troubleshooting and data management.

Information About Network-Wide Path Insight

Network-wide path insight provides end-to-end application-tracing serviceability in a Cisco Catalyst SD-WAN network. This feature lets you initiate application tracing and displays the trace results collected from multiple devices in a consolidated view. You also can view detailed information at the packet level, application level, domain level, flow level, and network level. Information from traces provides comprehensive insights into the operations of your network and can assist with performance analysis, planning, and troubleshooting.

For a brief video overview of network-wide path insight, see *Cisco Catalyst SD-WAN Network-Wide Path Insight How to Demo*.

Supported Devices for Network-Wide Path Insight

This feature is supported on Cisco IOS XE Catalyst SD-WAN devices.

Prerequisites for Network-Wide Path Insight

- Ensure that the **Data Stream** option is enabled in Cisco SD-WAN Manager. To enable this option, perform the following steps.

Note

- In a Cisco Catalyst multitenant deployment, you must have the provider role to enable this option. For more information, see User Roles in Multitenant Environment.
- If you try to set up a trace path when **Data Stream** is not enabled, you are prompted to enable it.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. For the **Data Stream** option, click **View**.
3. Click **Edit** and choose **Enable**.
4. Click **Save**.

- From Cisco Catalyst SD-WAN Manager Release 20.13.1, integrating Cisco Identity Services Engine (ISE) with Cisco Catalyst SD-WAN enables network-wide path insight traces to identify the specific users who are associated with traffic flows.

  For integration information, see Configure Cisco ISE in Cisco SD-WAN Manager.

  - Ensure that the users are registered with Cisco ISE.

- From Cisco Catalyst SD-WAN Manager Release 20.14.1, if you want traces to collect information about Cisco ThousandEyes Enterprise Agent tests, ensure that Cisco ThousandEyes is monitoring your network, and ensure that you know your Cisco ThousandEyes account username and OAuth bearer token. In addition, ensure that a Cisco ThousandEyes Enterprise Agent is deployed on a Cisco IOS XE Catalyst SD-WAN device in a service VPN other than VPN0 or 512, or on another host that is connected to a service VPN.

Restrictions for Network-Wide Path Insight

- Support for this feature on Cisco vEdge devices is limited to interoperation with Cisco IOS XE Catalyst SD-WAN devices.
- Only UDP and TCP can be traced using the Network-Wide Path Insight feature.
- This feature is not supported on VPN 0 or the transport VPN.
- This feature is not supported when extranet VPNs or service chain policies are configured in your Cisco Catalyst SD-WAN deployment.
- Not all packet traces are captured per flow. The system takes samples for the most typical packets automatically.

- Flow records do not display the complete history of flow path and hop information for releases before Cisco vManage Release 20.6.1.
- Mixed application and default policies are not supported for releases before Cisco vManage Release 20.6.1.
- You can monitor a maximum of two traces per device, and 10 concurrent active traces per Cisco SD-WAN Manager tenant.
- The following table shows the number of active flows that can be monitored, and the supported number of completed flows. Tracing stops when the monitoring limit is reached.

Release	Number of Supported Active Flows	Number of Supported Number of Completed
Releases before Cisco vManage Release 20.6.1	50 to 100 per device, depending on the Cisco IOS XE Catalyst SD-WAN device	1,000
Cisco vManage Release 20.6.1 through Cisco vManage Release 20.8.x	50 to 100 per device, depending on the Cisco IOS XE Catalyst SD-WAN device	10,000
Cisco vManage Release 20.9.1 and later releases	50 to 100 per device, depending on the Cisco IOS XE Catalyst SD-WAN device	60,000

- In releases before Cisco vManage Release 20.6.1, flow trace does not show the complete network path if the following optimizations are enabled:
  - UTD
  - TCP
  - SSL
  - DRE
- In the **Application Stats** graphs that are available in the **Insight Summary** > **Overview** tab, you cannot choose a WAN color for Cisco ASR 1000 Series Routers and Cisco Catalyst 8500 Series Edge Platforms.
- Traces that identify specific users who send and receive traffic provide information for IPv4 traffic only. This feature is available from Cisco Catalyst SD-WAN Manager Release 20.13.1.
- The site at which the trace starts by default has 100 peering sites with concurrent site-to-site traffic and can be extended to 250 peers in **Administration Setting** of Network Wide Path Insight. If the peering site is more than the configured value, the trace doesn't start from that site.
- For Cisco Catalyst SD-WAN Manager Release 20.14.1 and earlier releases, you can monitor traffic on flows that are initiated before you start a trace.

  For Cisco Catalyst SD-WAN Manager Release 20.15.1 and later releases, TCP/UDP flows that are initatied before you start a trace have lower chances of being monitored when compared with the newly initatied flows. You can use specific filters to monitor traffic on these flows.

Restrictions for Synthetic Traffic Packet Capture Replay

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

PCAP File Requirements

- Only PCAP files with Ethernet packets are supported.
- You can replay only one PCAP file at a time with up to 50 flows in a trace.
- PCAP file size only upto 5 MB is supported
- The total size of all PCAP files should not exceed 100 MB.
- You can upload up to 1000 PCAP files.
- Only TCP or UDP packets can be replayed.
- ICMP, Multicast, Broadcast, or Anycast packets are not supported.
- PCAP files with fragmented packets are not supported in stateful mode.

Packet Type and Size

- Conversion of IPv4 packets to IPv6 packets and vice versa is not supported.
- You cannot use stateless replay packets larger than 1500 bytes.
- For packets larger than 1500 bytes in stateless mode, it is recommended to use stateful mode.

Unsupported Protocols and DIA Scenarios

- You can only replay PCAP files in a single router for Cisco Catalyst SD-WAN DIA scenarios.
- PCAP replay does not support scenarios where one side is a tunnel endpoint while the other side is not the corresponding tunnel's endpoint.
- Application Level Gateway (ALG) is not supported.
- L2VPN is not supported.
- Security Group Tagging (SGT) is not supported.

IP Address Configurations

- PCAP files contain multiple flows and all flows can be replaced with IP addresses configured by you.
- You can configure only one source IP address and one destination IP address.
- You cannot use different IP addresses for different flows.

Use Cases for Network-Wide Path Insight

- Verification of network and policy design when deploying a new site, VPN, or application
- Daily monitoring of network, application, and policy operations
- Collection of information for diagnosing operational issues

For more information, see Use Cases, on page 55.

Configure Cisco ThousandEyes Username and OAuth Bearer Token

From Cisco Catalyst SD-WAN Manager Release 20.14.1, to have a network-wide path insight trace include test results from Cisco ThousandEyes Enterprise Agents, configure your Cisco ThousandEyes account information in Cisco SD-WAN Manager. This information includes your Cisco ThousandEyes username and OAuth bearer token. An OAuth bearer token is one of the two user API token types that Cisco ThousandEyes tokens.

This information is required so that Cisco SD-WAN Manager can obtain from Cisco ThousandEyes information that you are authorized to receive.

You can configure your account information in one of the following ways:

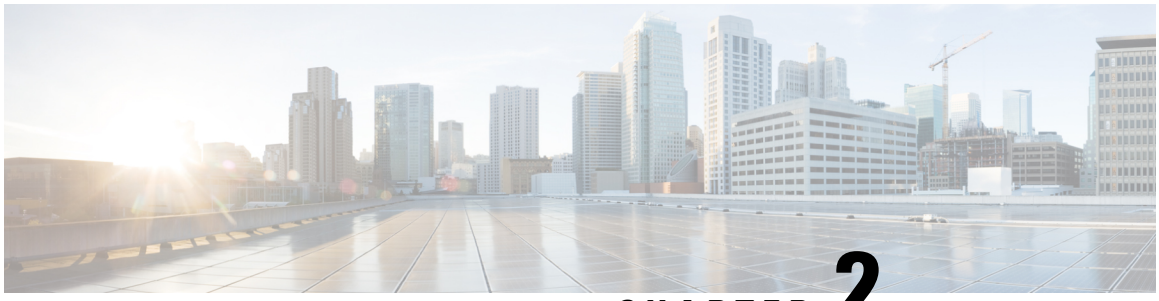
- Configure the **Administration** > **Settings** > **ThousandEyes User API Tokens** options, as described in this section.
- Configure options in the **Add ThousandEyes User API Tokens** dialog box that appears when you start a trace and enable **ThousandEyes Insight**. See Perform Network-Wide Path Insight Tracing for Cisco vManage Release 20.6.1 and Later Releases.



Note To determine your OAuth bearer token from the Cisco ThousandEyes application, choose **Account Settings** > **Profile** > **User API Tokens**.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **ThousandEyes User API Tokens**.
3. In the **Username** field, enter your Cisco ThousandEyes username.
4. In the **Bearer Token** field, enter your Cisco ThousandEyes OAuth bearer token.
5. (Optional) To configure information for another Cisco ThousandEyes account, Click **+ Add ThousandEyes User API token** and enter the username and OAuth bearer token.

   You can configure up to five Cisco ThousandEyes accounts for each Cisco SD-WAN Manager user.
6. Click **OK**.



CHAPTER 2

Perform Network-Wide Path Insight Tracing

- Perform Network-Wide Path Insight Tracing, on page 9
- Perform Network-Wide Path Insight Tracing for Releases before Cisco vManage Release 20.6.1, on page 9
- Perform Network-Wide Path Insight Tracing for Cisco vManage Release 20.6.1 and Later Releases, on page 10
- Create Auto-On Tasks, on page 20

Perform Network-Wide Path Insight Tracing

Table 3: Feature History

Feature Name	Release Information	Description
Automatic Security Alert, WAN Loss and IPSec Anti-Relay Drop as auto-on tracing options	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Three new options have been added to the auto-on trigger feature for improved network-wide path insight tracing

Perform Network-Wide Path Insight Tracing for Releases before Cisco vManage Release 20.6.1

This section describes how to perform network-wide path insight tracing in releases before Cisco vManage Release 20.6.1. To start a trace, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network Wide Path Insight**.
2. In the **Policy** area, choose **Site ID(*)** from the drop-down list. Ensure that you only choose a site that you have access to.
3. In the **VPN(*)** field, choose a VPN ID from the drop-down list. Only VPNs associated with the chosen site are listed.
4. (Optional) Enter the **Source/ Destination IP Addresses**.

5. (Optional) Choose the **Application** from the drop-down list.
6. (Optional) Specify the required **Trace Duration** in minutes. The default trace duration is 60 minutes and the maximum duration supported is 1440 minutes.
7. (Optional) Choose **Device** and **Source Interface** from the drop-down list.
8. (Optional) Choose **Protocol** from the drop-down list. **TCP** and **UDP** protocols are supported. The **All** option indicates both UDP and TCP protocols.
9. (Optional) Choose **DSCP** from the drop-down list.
10. Click **Start** to initiate a path trace. A dialog box displays the Trace ID, Start time of the trace, and all the details such as their IP addresses and trace status of the started devices.

Note To stop an ongoing trace before the timer expires, click **Stop**. You can also stop a trace from the **Trace** section.

Perform Network-Wide Path Insight Tracing for Cisco vManage Release 20.6.1 and Later Releases

This section describes how to perform network-wide path insight tracing from Cisco vManage Release 20.6.1.

Tracing provides detailed information about application issues and can discover domains and applications that run in domains. You can configure various options to specify the tracing that you need and view detailed information about trace flows.

To start a trace, follow these steps:

	Cisco vManage Release 20.6.x and earlier releases	Cisco Catalyst SD-WAN Manager Release 20.12.1	Cisco vManage Release 20.6.x and later releases
1.	**Network Wide Path Insight** is part of the **Monitor** menu.	You can also start a trace by choosing **Create a Trace** from the **Monitor** > **Overview** > **Global Network View** page.	From the Cisco SD-WAN Manager menu, choose **Tools** > **Network Wide Path Insight**.

2. Perform one of the following actions:

From Cisco vManage Release 20.6.1 through Cisco vManage 20.11.x	From Cisco Catalyst SD-WAN Manager Release 20.12.1
(Optional) In the **Trace** area, check the **Enable DNS Domain Discovery** check box to enable DNS domain discovery for network-wide path insight.	Click **New Trace**.
Click **New Trace**.	(Optional) In the **Trace** area, check the **Enable DNS Domain Discovery** check box to enable DNS domain discovery for network-wide path insight, or continue to Step 3.

Note When you enable DNS domain discovery, to discover DNS domains and the applications that are running in the discovered domains, Cisco SD-WAN Manager uses DNS snooping. You can then monitor the domains under the **Application** option to obtain information about health, trends, and metrics. When you disable this option, the trace monitors the application flows based on the criteria and filters that you specify.

Enabling this option provides deep insight information for DNS domains, especially in Cisco Catalyst SD-WAN Cloud OnRamp for SaaS and Direct Internet Access (DIA) deployments. Check the discovered domains for information about DNS domain queries before you start a trace to probe the traffic in these domains.

Field	Description
3. (Optional) **Trace Name**	Enter a name for the trace. If you don't enter a name, the system assigns the name trace_*ID*, where *ID* is the system-generated identifier of the trace.
Trace Duration	Enter the number of minutes for which the trace lasts. The minimum value is 1. The maximum value is 1440 (24 hours). The default value is 60.

4. In the **Filters** area, perform these actions:

Note All the fields in both **Filters** and **Advanced Filters** use the logical AND Operator. Cisco SD-WAN Manager monitors only those flows that match all the configured conditions.

Field	Description
Select Site	From the drop-down list, select the Cisco Catalyst SD-WAN network site in which you want to perform the trace.
VPN	choose the service VPN for the trace to monitor. From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can choose up to 64 VPNs.
(Optional: This option is applicable only if DNS domain discovery is disabled.) **Source Address/Prefix**	Enter the source IPv4 or IPv6 IP address and the prefix of flows for the trace to monitor. If you leave this field blank, the trace monitors flows with any source address or prefix.
(Optional: This option is applicable only if DNS domain discovery is disabled.) **Destination Address/Prefix**	Enter the destination IPv4 or IPv6 IP address and prefix of flows for the trace to monitor. If you leave this field blank, the trace monitors flows with any destination address or prefix.

Field	Description
(Optional: This option is applicable only if you enable DNS domain discovery.) **Client Address/Prefix**	Enter the source IPv4 or IPv6 IP address or prefix of flows for the trace to monitor. If you leave this field blank, the trace monitors flows with any source address or prefix.
(Optional: This option is applicable only if DNS domain discovery is disabled.) **Application**	Choose this option to designate specific applications for the trace to monitor. If you don't choose an option, the trace monitors all the applications. To remove an application from this field, click **X** next to the corresponding application name.
Application Group	Choose this option to designate specific application groups for the trace to monitor. The trace then monitors all the applications that an application group includes. Use the check boxes that appear to choose the application groups for the trace to monitor. For example, if you choose the application group ms-cloud-group, Cisco SD-WAN Manager monitors all the applications included in this group. These applications are ms-office-365, ms-services, ms-teams, and more. If you don’t choose an option, the trace monitors all the applications. To remove an application group from this field, click **X** next to the corresponding application group name.

5. (Optional) If you enable DNS domain discovery, expand the **Advanced Filters** area and configure parameters for the trace to monitor.

Note All the fields in both **Filters** and **Advanced Filters** use the logical AND Operator. Cisco SD-WAN Manager monitors only those flows that match all the configured conditions.

Field	Description
Device	Choose one or more devices for the trace to monitor by checking the check box for each device. If you don’t choose a device, the trace monitors all devices for the site that you specified in Step 4, on page 11.

Field	Description
Source Interface	Choose the source interface of traffic for the trace to monitor. If you don't choose a source interface, the trace monitors traffic from all source interfaces in the VPN that you specified in Step 4, on page 11.
Source Port	Enter the source port number of traffic that the trace should monitor. The trace monitors traffic that flows from this port number. If you don't choose a source port, the trace monitors traffic for all source ports.
Destination Port	Enter the destination port number of traffic for the trace to monitor. The trace monitors traffic that flows to this port number. If you don't choose a destination port, the trace monitors traffic for all destination ports.
Protocol	Choose the traffic protocol type for the trace to monitor. If you don't choose a protocol, the trace monitors traffic for all supported protocols.
DSCP	choose the DSCP type for the trace to monitor. The **DEFAULT** selection indicates **DSCP0**. If you don't choose a DSCP type, the trace monitors traffic for all DSCP types.
(Optional) **ISE Users**	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) check the check box, then click the **ISE Users** field and check the check box for each user whose traffic the trace should monitor. The trace monitors bidirectional traffic between this user and applications in your network. If you don't choose a user, the trace monitors traffic for all users. **Note** **ISE Users** option is available only if you integrate Cisco ISE with Cisco Catalyst SD-WAN.

Field	Description
(Optional) **ThousandEyes Agent**	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) To designate a Cisco ThousandEyes agent whose tests the trace should monitor, check the check box. Check the check box for the Cisco ThousandEyes Enterprise Agent that you want. You must choose an agent that served as a source agent in the monitored Cisco ThousandEyes test.

If you click the **ThousandEyes Insight** option as described later in this procedure, the trace collects data as described in the following table:

ThousandEyes Agent Option Enabled and Enterprise Agent Designated	Cisco ThousandEyes Enterprise Agent Installation Location	Result
No	Router from which you started the trace	The trace collects complete data from the Enterprise Agent on the router. If your network has other Enterprise Agents, the system also monitors tests from them, but it might not collect some or all of their test data.
No	Any device	If your network has other Enterprise Agents, the system also monitors tests from them, but it might not collect some or all of their test data.
Yes	Any device	The trace collects complete data from the designated Enterprise Agent only.

Note We recommend that you designate a Cisco ThousandEyes agent to ensure maximum trace outcome in any condition. To monitor other traffic while monitoring a Cisco ThousandEyes agent, create another trace and disable the **ThousandEyes Insight** option on the same site.

6. (Optional) Expand the **Monitor Settings** area and configure the following parameters:

Field	Description
QoS Insight	(Minimum supported release: Cisco vManage Release 20.9.1) Includes application, VPN, interface, and queue-level throughput and drop-rate metrics for all traffic in the trace. This option is enabled by default.
ART Visibility	Includes the application response time (ART) metrics for TCP traffic in the trace. These metrics include client network delay (CND) and server network delay (SND) information. This option is enabled by default.
App Visibility	Uses the SD-WAN Application Intelligence Engine (SAIE) flow to discover applications and application groups in the trace. **Note** In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow. If you chose applications or application groups in Step 4, on page 11, this option is enabled automatically. If DPI isn't enabled, we recommend that you enable **App Visibility** to map the flows to the correct applications. Enabling this option authorizes Network-Wide Path Insight to enable DPI in the first hop router of the trace during the trace.
DIA Visibility	Enable the viewing of downstream information from direct internet access flows, beginning with the first flow. Enabling DNS domain discovery automatically enables this option by default. This option doesn't affect the applications transported over a Cisco Catalyst SD-WAN tunnel. If you don't enable this option, the device discovers direct internet access traffic automatically, but it can take some time for this discovery to begin.

Field	Description
WAN Visibility From Cisco Catalyst SD-WAN Manager Release 20.12.1, **Hub WAN Visibility** is called **WAN Visibility**.	When starting a trace, include flows initiated in the WAN to LAN direction. By default, a trace monitors flows initiated in the LAN to WAN direction. For releases before Cisco Catalyst SD-WAN Manager Release 20.12.1, enabling DNS domain discovery automatically enables this option by default, and it can't be disabled. For releases from Cisco Catalyst SD-WAN Manager Release 20.12.1, this option is disabled by default in all cases and you can enable it as needed. **Note** Because traffic typically flows from a spoke to a hub, we recommend that you start a trace from a spoke site.
ThousandEyes Insight	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) To have the trace capture test results from Cisco ThousandEyes Enterprise Agents. If you have entered your Cisco ThousandEyes username and OAuth bearer token in **Administration** > **Settings** > **ThousandEyes User API Tokens**, this option is selected automatically. (See Configure Cisco Thousand Eyes Username and OAuth Bearer Token.) If your username and OAuth bearer token aren't configured, the **Add ThousandEyes User API Tokens** dialog box appears. Enter your username in the **Username** field and OAuth bearer token in the **Bearer Token** field, and click **OK**. The information that you enter here is configured in **Administration** > **Settings** > **ThousandEyes User API Tokens** automatically.
Sampling	To enable sampling when tracing, which causes the trace to capture flows at the specified interval.

Field	Description
Sampling Interval	Enter the time interval, in seconds, between samples. For example, if you enter 100, one flow is traced every 100 seconds even if there are multiple other flows. The minimum sampling interval value is 1 second. The maximum value is 86400 seconds (24 hours). The default value is 60. The sampling options can extend the trace monitoring period by increasing the time it takes to reach the maximum number of flows.
Local Drop Rate Threshold(%)	Set the maximum acceptable packet loss rate for this device.
Wan Loss Rate Threshold(%)	Set the maximum acceptable packet loss rate for the WAN connection.

7. (Optional) From Cisco Catalyst SD-WAN Manager Release 20.12.1, click the **Expand** icon to expand the **Grouping Fields** area and configure the following options.

   By default, the **App Performance Insight** tab on the **Insight Summary** groups information by application. Additional options area let you group information into smaller groups so that you can refine the display of information to meet your needs.

Field	Description
Client Prefix	Enable client prefix aggregation.
Server Prefix	Enable server prefix aggregation.
Source SGT	Enable source security group tag (SGT) aggregation.
User Identity	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Enable Cisco ISE user identities. **Note** This **ISE User Identity** option applies only if you integrate Cisco ISE with Cisco Catalyst SD-WAN.

8. (Optional) From Cisco Catalyst SD-WAN Manager Release 20.12.1, click the **Expand** icon and perform the following actions in the **Synthetic Traffic** area to enable synthetic traffic.

   Synthetic traffic helps verify network design. When you onboard a new site or change an existing site configuration, it's important to validate whether applications work as designed and intended. Enable synthetic traffic to generate sample user traffic and check if applications are working as expected using network-wide path insight features.

Synthetic traffic starts when the trace starts and stops when the trace stops. After the trace stops, you can view synthetic traffic flows in the **Completed Flows** tab and filter the information to see only synthetic traffic details.

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.16.1) You can use HTTP or HTTPS client and packet capture replay for synthetic traffic.

Table 4: Http(s) Client

URL	Enter the URL to which a router should send synthetic traffic, for example, https://www.cisco.com.
VPN	Choose a service VPN on which to start synthetic traffic. The VPNs that are available are based on the VPNs that you chose in the **Filters** area.
DNS Server	Enter the IP address of the DNS server for translating the URL. Enter your organization's DNS server IP address to ensure synthetic traffic flows to the same destination as actual user traffic.
DSCP	Choose the DSCP to use for the synthetic traffic.
Interval	Specify how often, in minutes, to send the synthetic traffic to the URL during the trace. For example, if you enter an interval of **2**, synthetic traffic is sent every 2 minutes. The minimum value is **1**.
ISE User/User Group	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) choose one of the following options from the drop-down list: • Choose **N/A** to generate synthetic traffic that doesn't relate to a user or Cisco ISE user group. • Choose **User** to generate synthetic traffic from a specific user, then choose the user from the drop-down list to the right. • Choose **User Group** to generate synthetic traffic from a test user in a specific Cisco ISE user group, then select the user group from the drop-down list. **Note** This **ISE User/User Group** option applies only if you integrate Cisco ISE with Cisco Catalyst SD-WAN.

(Optional) Click the plus sign icon and repeat these steps to add another synthetic traffic instance.

Click **Save**.

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.16.1

If you want to replay PCAP in the trace, perform the following actions:

Table 5: PCAP Replay

Field	Description
PCAP File Name	Select the PCAP file from the drop-down menu. Cisco SD-WAN Manager provides many built-in PCAP files that you can use. You can view the description of each PCAP file and internal files on the PCAP Replay page, or download the PCAP file and view them. If you want to use your own PCAP files, you can upload them. To upload a PCAP file: **a.** Click **Administration Setting**. **b.** Click **PCAP Replay**. **c.** Click **Upload PCAP File** and upload the PCAP file. Only the Administrator can provide the PCAP file. The PCAP file size must not exceed 5 MB.
Replay Mode	Choose one of the following PCAP replay modes: • Stateless • Stateful
VPN	Select a service VPN for replaying the PCAP. The VPNs are based on the VPNs that you chose in the Filters area.
Interval (minutes)	Specify the time interval in minutes for replaying the PCAP. For example, if you input 3, the PCAP file is replayed every 3 minutes.
Source IP	Enter the source IP address. The IP address should be an IP address of the selected service VPN.
Target IP	Enter the destination IP address. The IP address could be a NAT DIA address from the service VPN for Cisco Catalyst SD-WAN Manager Release 20.16.1.

Click **Save**.

9. Click **Start** to initiate the trace.

The **Start Trace** window shows the trace ID, start time, IP addresses, and status of the devices.

10. Close the **Start Trace** window.

    The trace is displayed in the list of traces in the **Tools** > **Network Wide Path Insight** window.

Note In Cisco vManage Release 20.6.x and earlier releases, the list of traces is available in the **Monitor** > **Network Wide Path Insight** page.

Create Auto-On Tasks

Note The auto-on task feature is available from Cisco Catalyst SD-WAN Manager Release 20.12.1.

An auto-on task monitors your network for events that you choose and automatically runs a trace if two consecutive events of the same type are detected.

QoS congestion event is generated after continuous congestion for 5 seconds, and only one event is generated in one minute. The auto-on task requires two occurrences in a row to trigger the monitoring.

SLA violation event is generated when one packet does not meet SLA requirements, and only one event is generated in one minute. The auto-on task requires two occurrences in a row to trigger the monitoring.

You can choose applications as SLA violation trigger conditions.

The number of consecutive events can be configured.

Security Alert event triggers a trace automatically when a security alert is detected by the Unified Threat Defense (UTD), such as IPS alerts or file reputation alerts, and also if firewall drops are seen unexpectly.

An auto-on task monitors the network for a period that you specify. Each trace that a task runs lasts for 5 minutes. To avoid congestion from multiple traces running simultaneously, for each site that is monitored, there is a ½ hour interval after a trace starts before the next one begins.

Options for traces that an auto-on task generates are preconfigured and cannot be changed.

An auto-on task is useful if you have identified or suspect a potential or intermittent issue in your network. For example, if you have identified intermittent SLA violations, instead of manually monitoring the network and manually starting a trace when you see an SLA violation, you can create a task that automatically starts traces when SLA violations are detected.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Network Wide Path Insight**.
2. Click **New Auto-on Task**.
3. In the **Task Name** field, enter a name for the task.
4. From the **Select Event** drop-down list, choose the following event(s) that, when detected, start a trace:
   - **QoS Congestion**: Congestion on the non default QoS queue of an interface.

- **SLA Violation**: Traffic outside of the parameters that are defined by a service level agreement (SLA), for example, traffic latency exceeding predefined criteria.



Note In Cisco Catalyst SD-WAN Manager Release 20.18.1, for QOS congestion and SLA violation events, by default, two consecutive events of each type are required to trigger a NWPI trace, and the number of consecutive events is configurable.



Note The **Security Alert**, **WAN Loss** and **IPSec Anti Replay Drop** event types are available from Cisco Catalyst SD-WAN Manager Release 20.18.1

- **Security Alert**: Automatically initiate a trace when security alerts are detected by UTD, such as IPS alerts or file reputation alerts.
- **WAN Loss**: You can configure WAN Loss as an auto-on trace trigger. By setting a loss percentage criterion, Cisco SD-WAN Manager triggers an NWPI trace when the loss percentage is higher than the configured value.
- **IPSec Anti Replay Drop**: You can set a criterion on the drop percentage, to help Cisco SD-WAN Manager trigger an auto-on NWPI trace when the drop is percentage higher than the configured value.

  When abnormal IPsec Anti-replay drops are detected, the device will send a **netconf** notification to Cisco SD-WAN Manager, and NWPI triggers an auto-on trace based on the received notification.



Note In Cisco Catalyst SD-WAN Manager Release 20.18.1, for Security Alert, WAN loss, and IPSec anti-replay drop events, a single event of each type is sufficient to trigger a trace.

5. (Optional) From the **Select Site** drop-down list, choose the name of one or more Cisco Catalyst SD-WAN network sites in which to perform the trace.



Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, you must select one or more Cisco Catalyst SD-WAN network sites.

Up to 50 sites can be supported.

If you do not choose a network site, the task monitors all the sites.

6. In the **Select Duration** field, enter the number of hours the task lasts for.

   The task monitors your network for the selected events during this duration.

   Enter a number from **1** through **168**.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, you can enter a number from **1** through **720** hours or **1** through **30** days.

7. (Optional) Expand the **Advanced Configuration** area and configure the following parameters:

Table 6: QoS Congestion

Field	Description
Application	From Cisco Catalyst SD-WAN Manager Release 20.18.1, the enhanced auto-on configuration allows selection of up to 32 applications. Only QoS Congestion events associated with these specified applications will trigger an auto-on trace.
Number of consecutive events	This setting determines how many consecutive QoS Congestion events from the same Cisco IOS XE Catalyst SD-WAN device are required to trigger an auto-on trace. By default, this is set to 2. This means that if two QoS Congestion events occur in succession, a trace will automatically be initiated to monitor and diagnose the congestion issue.
Congestion burst interval (second)	For continuous QoS congestion, the device generates one QoS congestion event per reporting interval. The configurable reporting interval ranges from 1 to 60 seconds.
Trace only the selected or impacted applications	Click this check box to ensure only the flows with applications matching those reported in the QoS Congestion event are traced. By default, it is not selected. All the applications will be traced in the trace triggered by the auto-on task.

Table 7: SLA Violation

Field	Description
Application	From Cisco Catalyst SD-WAN Manager Release 20.18.1, the enhanced auto-on configuration allows selection of up to 32 applications. Only SLA Violation events associated with these specified applications will trigger an auto-on trace.

Field	Description
Number of consecutive events	This setting determines how many consecutive SLA Violation events from the same Cisco IOS XE Catalyst SD-WAN device are needed to trigger an auto-on trace. The default is 2. This means that a trace will be initiated automatically if two SLA Violation events occur consecutively.
Trace only the selected or impacted applications	Click this check box to ensure only the flows with applications matching those reported in the SLA Violation event are traced. By default, it is not selected. All the applications will be traced in the trace triggered by the auto-on task.

Table 8: Security Alert

Field	Description
UTD IPS Alert	Check this check box to automatically create a trace when Cisco IOS XE Catalyst SD-WAN device identifies and blocks suspicious activity using Intrusion Prevention System (IPS). You can specify a particular Security Identifier (SID) to create a trace only when that specific signature is identified.
UTD File Reputation Alert	Check this check box to create a trace when a malicious file is identified and blocked by the Advanced Malware Protection (AMP). You can specify a particular SHA hash value to create a trace only when that specific file is identified.
UTD File Reputation Retrospective Alert	Check this check box to trigger a trace based on a retrospective analysis of files that have passed through the network.
Firewall Drop	Application flows dropped by a firewall policy are usually as per configuration/design. However, you suspect unexpected drops due to a misconfigured firewall policy, select this checkbox to enable firewall policy drop rate monitoring in auto-on task.
Trace only the traffic with the same source IP as the alert event	Click this check box to ensure that when an auto-on trace is created, it only traces the flows with the source IP reported in the security alert.
Trace only the traffic with the same destination IP as the alert event	Click this check box to ensure that when an auto-on trace is created, it only traces the flows with the destination IP reported in the security alert.

Table 9: WAN Loss

Field	Description
WAN Loss Rate Threshild (%)	Set a loss percentage criterion to help Cisco SD-WAN Manager trigger an auto-on NWPI trace when the loss percentage is higher than the configured value.

Table 10: IPSec Anti Replay Drop

Field	Description
Drop Rate Threshold (%)	Set a criterion on the drop percentage, to help Cisco SD-WAN Manager trigger an auto-on NWPI trace when the drop is percentage higher than the configured value.

8. Click **Start**.

   The task appears in the table of auto-on tasks. This table provides the following information and options for each task and each trace that the task starts:

   - **Task name**: Task trace name. This field also includes the **Insight Summary** link, which lets you see more information about the traces that the task started. See Insight Summary, on page 43.
   - **Task ID**: System-generated identifier of the task or trace.
   - **Event(s)**: The event or events that you configured to start a trace, or the events that triggered a trace.
   - **Site(s)**: The name of each site that the task monitors, or the name of the site in which a trace ran.
   - **State**: **Active** means that the task is live or a trace is running. **Finished** means that the task or trace has completed.
   - **Start Time**: Date and time at which you started the task or that a trace started.
   - **Duration**: Number of hours that a task or trace is live or ran.
   - **Stop Time**: Date and time at which the task or trace ended.
   - **Actions**:
     - Click **Delete** to remove a task or trace from the table.
     - Click **Stop** to stop an active task. Note that a stopped task cannot be restarted.

Start a trace using a time schedule-based auto-on task

From Cisco Catalyst SD-WAN Manager Release 20.18.1, you can schedule traces to start at specific times.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Network Wide Path Insight**.
2. Click **New Auto-on Task** > **Time Scheduled Trace**.
3. In the **Task Name** field, enter a name for the task.

4. In the **Duration** field, select the number of days (maximum 30).
5. In the **Recurrence Setting** pane, enter the **Trace Start Time (s)** and **Duration(s).**

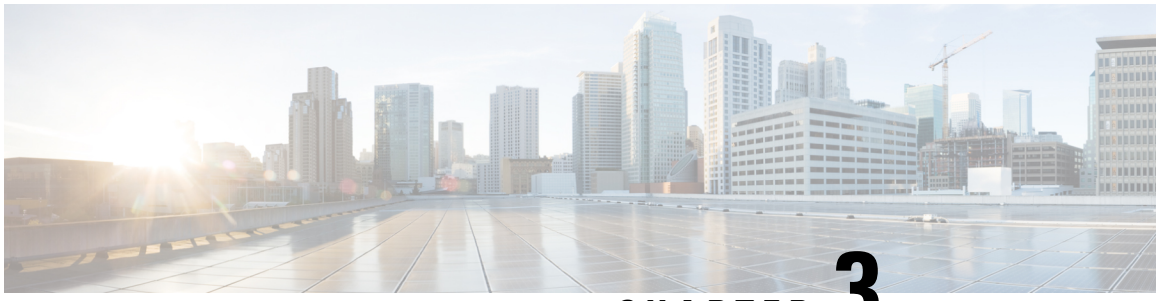


Note A maximum of 8 Trace Start Times is supported, the combined duration of all traces is 1,440 minutes (24 hours). A minimum gap of 10 minutes is required between traces.

Monitor events using a a time schedule-based auto-on task

From Cisco Catalyst SD-WAN Manager Release 20.18.1, you schedule the monitoring of events within specific timeframes.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Network Wide Path Insight**.
2. Click **New Auto-on Task** > **Event Triggered Trace**.
3. In the optional **Recurrence Setting** pane, specify the days to monitor only at critical moments. If unspecified, the auto-on task will monitor events throughout the entire timeline by default.



CHAPTER 3

Traces

- Feature history of traces, on page 27
- Exporting traces, on page 27
- SD-WAN Analytics triggered NWPI Trace, on page 29
- View Trace Instances, on page 29
- View and Manage Trace Information, on page 29
- Flow Path and Metrics, on page 30
- Insight, on page 31

Feature history of traces

Table 11: Feature History

Feature Name	Release Information	Feature Description
Export and import traces	Cisco Catalyst SD-WAN Control Components Release 20.18.1	If you perform a trace and find a network issue, you can export the trace information to analyze externally. For example, the information may be useful for troubleshooting as part of a Cisco Technical Assistance Center (TAC) case. You can import a saved trace to view the details in Cisco SD-WAN Manager.

Exporting traces

If you perform a trace and find a network issue, you can export the trace information to analyze externally. For example, you can send the exported information to the Cisco Technical Assistance Center (TAC) for analysis. Similarly, you can save trace information for internal use.

File format

Exporting a trace creates a .tar.gz archive containing a set of JSON files. While you can view these in any desired tool, it is most useful to import a saved trace into Cisco SD-WAN Manager to view the trace details.

Export a trace

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Tools** > **Network-wide Path Insights**.

Step 2 In the table of traces, adjacent to a trace, click **…**.

Step 3 Choose any one action:

- **Download**: SD-WAN Manager downloads the trace as a .tar.gz file containing a set of JSON files.
- **Attach to TAC Case**: Upload the trace to open a Cisco service case for troubleshooting, using the SR number of the case.

Import a trace

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Tools** > **Network-wide Path Insights**.

Step 2 Click **Imported Traces** to view a list of imported traces.

Step 3 Click **Import Trace**.

Step 4 Follow the instructions to upload a trace file.

The uploaded trace file appears in the table on the **Imported Traces** page.

View an imported trace

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Tools** > **Network-wide Path Insights**.

Step 2 Click **Imported Traces** to view a list of imported traces.

Step 3 Choose an action available in the table.

- **Insight Summary**: View a summary of the trace.
- **View Insights**: View the details of the trace.
- Delete a trace from the table.

SD-WAN Analytics triggered NWPI Trace

From Cisco Catalyst SD-WAN Manager Release 20.18.1, NWPI Traces can be automatically triggered using SD-WAN Analytics.

Prerequisites to enable SD-WAN Analytics triggered NWPI Trace

1. In Cisco SD-WAN Manager, go to **Settings** > **Data Collection & Statistics** and enable **Cloud Services**.
2. In Cisco SD-WAN Manager, go to **Monitor** > **Network-Wide Path Insight** > **Administration Settings** and click **Allow Analytics to create traces and tasks via API.**

SD-WAN Analytics-triggered traces are typically named in a `[trigger reason] Auto Triage - [timestamp]` format.



Note Enable **Upload Traces and Tasks to the Cloud** to upload the NWPI trace to the SD-WAN Analytics cloud.

You can see the trace's storage location in the trace table. The location can be local stored, cloud stored, or both local and cloud stored.

View Trace Instances

The path trace instances appear with unique trace IDs in the **Trace History** area (in releases before Cisco vManage Release 20.6.1) or in the **Trace** area (in Cisco vManage Release 20.6.1 and later releases). Information about each instance is also displayed, including its state and the actions that you can perform.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, the **Trace** area includes the following tabs:

- **All Trace**: Provides information about the traces that you start manually.
- **Auto-On Task**: Provides information about the traces that are generated by an auto-on task.

View and Manage Trace Information

You can perform the following actions in the **Trace History** area or **Trace** area:

- In releases before Cisco vManage Release 20.6.1:
  - To stop an active trace, click **Stop**. If you have specified the trace duration, the trace stops automatically when the timer expires.
  - To navigate to the **Flow Path and Metrics** section, click **Detail**.
- From Cisco vManage Release 20.6.1:

Action	Procedure	Tab (from Cisco Catalyst SD-WAN Manager Release 20.12.1)
Stop a trace that is in progress.	Click **Stop** in the **Action** column for the trace, and then click **Confirm** in the **Stop Trace** dialog box.	**All Trace** and **Auto-On Task**
Delete a trace that is completed.	Click **Delete** in the **Action** column for the trace, and then click **Confirm** in the **Delete Trace** dialog box.	**All Trace** and **Auto-On Task**
Display trace-level insight summary information (from Cisco vManage Release 20.9.1).	See Insight Summary, on page 43.	**All Trace** and **Auto-On Task**
Display detailed information about the flows in a trace in the **Insight** area.	Click **Insight Summary** for the trace in the **Trace Name** column.	**All Trace**
View the filters and settings for a trace.	Click the name of the trace in the **Trace Name** column.	**All Trace**
View information about the source of a trace.	Click the corresponding value in the **Src Site** column.	**All Trace**
View information about the applications or application groups that a trace monitors.	Click the corresponding value in the **Application/App Group** column.	**All Trace**
View the status of a trace and error messages, if any, that have been generated.	Click the corresponding value in the **Trace State** column.	**All Trace**
View statistics for a task (from Cisco Catalyst SD-WAN Manager Release 20.12.1).	Click the name of the corresponding task.	**Auto-On Task**
View the filters and settings for a trace in a task (from Cisco Catalyst SD-WAN Manager Release 20.12.1).	Expand the task that you want, and then click the name of the trace in the **Trace Name** column.	**Auto-On Task**

Flow Path and Metrics

This section applies to releases before Cisco vManage Release 20.6.1.

In the **Flow Path and Metrics** section, view bidirectional flow path table with hop-by-hop metrics. You can expand any trace instance in the log to view the following details:

Column	Description
Last Update Time	The flow path instances in running state are refreshed every 10 seconds and the time of the update is displayed.
Flow ID	Flow IDs differentiate two identical flow path instances occurring at different times.
State	This state helps you visualize potential issues with the flow. Only SLA state of the flow is supported.
Direction	Directions could be upstream or downstream. The direction in which the first packet flow is identified is considered as upstream.
Local Color, Remote Color	Local edge (source) and the remote edge (destination) colors indicate different WAN interfaces.
Local Drop(%)	Packet drop on hop's local edge routers.
Remote Drop(%)	Packet drop on hop's remote edge routers (WAN underlay drop on remote edge router excluded)
WAN Drop(%)	Packet loss on WAN from hop's local edge router to remote edge router (includes WAN underlay drop on remote edge router, eg.IPSec Anti-Replay drop.)
Jitter(ms), Latency(ms)	Jitter and latency metrics of the flow. These metrics help with evaluating the application performance in real time.
Total Packets, Total Bytes	For each direction of the flow, total number of packets and total byte count are displayed.

Insight

This section applies to Cisco vManage Release 20.6.1 and later.



Note From SD-WAN Manager 26.1.x, to capture all the relevant policy details you must enable **WAN Visibility** while enabling the traces. Refer to Perform Network-Wide Path Insight Tracing section.

Click **View Insight** in the **Actions** column in the list of traces to display detailed information about the flows in the corresponding trace. This detailed information appears in the **Insight** area. The following information is displayed in this area:

- The **DNS Domains** tab is available only when DNS domain discovery is enabled and displays information about each domain that the trace discovers. You can expand any row in the list to display detailed information about the application.

From Cisco vManage Release 20.9.1, click **Discovered Domains** to display information for every domain that the trace discovered but that are not yet traced. Click **Monitored Domains** to display information only for domains that the trace monitored.

Note In Cisco vManage Release 20.6.1 through Cisco vManage Release 20.8.x, the **DNS Domains** tab is called the **Applications** tab.

- (From Cisco vManage Release 20.9.1) The **Applications** tab displays information about applications that were traced. You can expand any row in this list to display bidirectional path information with hop-by-hop metrics for each application.
- The **Active Flows** tab displays information about the flows that are in the Running state. You can expand a flow instance to display bidirectional flow path information with hop-by-hop metrics.
- The **Completed Flows** tab shows information about the flows that are in the Stopped state. You can expand a flow instance to display bidirectional flow path information with hop-by-hop metrics.
- In the **DNS Domains** tab, start or stop flow monitoring of the applications in the selected domain for an active trace. Starting flow monitoring also deploys an HTTP probe (through Cisco vManage Release 20.8.x) or an HTTPS probe (from Cisco vManage Release 20.9.1) for the domain on the WAN. A dialog box indicates that monitoring has started. Monitoring information is displayed in the **Active Flows** and **Completed Flows** tabs.
  - In Cisco vManage Release 20.6.1 through Cisco vManage Release 20.8.x, click **Start Flow Monitor** and **Stop Flow Monitor**, as needed, to start or stop monitoring for the selected domains.
  - From Cisco vManage Release 20.9.1, to start flow monitoring, click **Discovered Domains**, check the corresponding check box for one or more domains to start monitoring, and click **Start Flow Monitor**. In the confirmation dialog box that appears, click **Confirm**. You can change the domain selections in this dialog box before you click **Confirm**.

    From Cisco vManage Release 20.9.1, to stop flow monitoring, click **Monitored Domains**, check the check box for each domain for which you want to stop monitoring, and click **Stop Flow Monitor**. In the confirmation dialog box that appears, click **Confirm**.
- Use the **Search** option to find specific flow instances.

  From Cisco vManage Release 20.6.1, you also can cut and paste the following keywords to search for flows that include corresponding the events:

  - **Local Drop**
  - **WAN Loss**
  - **TCP Reset**
  - **NAT Translation**
  - **DPI First Packet Unclassified**
  - **SLA Violation**
  - **QoS Congestion**
  - **WAN Color Inconsistency**

- **Flow Asymmetry**
- **Policy Bypass**
- **Server No Response**
- **AppQoE Diverted**
- **UTD Diverted**

- For completed flows, use the **Filter** option to display only flow instances that meet specified criteria.
- For completed flows, you can limit the display to flows that occurred within a specified period.

  In releases through Cisco vManage Release 20.8.x, you can choose a period of 1, 10, or 30 minutes, or 1, 2, or 5 hours. You also can click **Custom** and enter a date and time range.

  From Cisco vManage Release 20.9.1, you can drag the ends of the time bar to designate the start and end dates and times for a certain period.

The following sections describe the information that appears for each application and each instance in a flow, and, if DNS domain discovery is enabled, for each domain:

- DNS Domains Tab, on page 33
- Applications Tab, on page 34
- Active Flows and Completed Flows Tabs, on page 36
- Expanded DNS Domains Information, on page 40
- Expanded Application Information, on page 41
- Expanded Flow Instance Information, on page 41



Note The **DNS domains** tab (called **Applications** tab in Cisco vManage Release 20.6.1 through Cisco Manage 20.8.x) is available only when DNS Domain Discovery is enabled for a trace.

DNS Domains Tab

Table 12: DNS Domains Tab (Called Applications Tab in Cisco vManage Release 20.6.1 Through Cisco Manage 20.8.x)

Column	Description
Check box	Check the check box for the domains for which you want monitoring to be enabled or disabled and click **Start Flow Monitor** or **Stop Flow Monitor**.
Domain	Name of the domain that the trace discovered.
Update Time	Date and time at which the information was last refreshed. Instances are refreshed every 30 seconds by default.

Column	Description
Application	Name of the application that the trace discovered in the domain.
Insights	From Cisco Catalyst SD-WAN Manager Release 20.18.1, you can click on**View** in this column to get details about this domain in a side frame.
Application Group or **App Group**	Name of the application group that the trace discovered in the domain.
VPN Id	Available from Cisco Catalyst SD-WAN Manager Release 20.12.1. Identifier of the VPN in which the application flow was traced.
DNS Server	Destination of DNS packets sent from clients.
DNS Redirect	DNS resolver to which a device redirects DNS traffic if a resolver is configured by a centralized policy or by Cisco Umbrella.
Resolved IP	DNS-resolved IP address for the application.
DNS Transport	Transport type used by the domain.
DNS Egress	Egress interface and type used by the domain.
TTL (sec)	DNS time to live, in seconds.
Request	Number of DNS packets sent.
Monitor State	Status of flow monitoring for the domain.

Applications Tab

Table 13: Applications Tabs (Available from Cisco vManage Release 20.9.1)

Column	Description
Columns Displayed in Cisco vManage Release 20.9.1 through Cisco vManage Release 20.11.x	
Last Update Time	Date and time at which the information was last refreshed. Instances are refreshed every 10 seconds by default.
App Name	Name of the application.
App Group	Application group to which the application belongs.
Upstream Flow Count	Number of upstream flows that were counted for the application.

Column	Description
Downstream Flow Count	Number of downstream flows that were counted for the application.
Upstream Bytes (K)	Number of KBs in the upstream traffic of this application.
Downstream Bytes (K)	Number of KBs in the downstream traffic of this application.
Columns Displayed From Cisco Catalyst SD-WAN Manager Release 20.12.1	
Last Update Time	Date and time at which the information was last refreshed. Instances are refreshed every 10 seconds by default.
App Name	Name of the application.
App Group	Application group to which the application belongs.
VPN Id	Identifier of the VPN in which the application flow was traced.
Total Bytes (K)	Number of KBs in the upstream and downstream flows of this application.
Total packets	Number of packets in the upstream and downstream flows of this application.
KBPS	Number of KBs per second in the upstream and downstream flows of this application during the past minute.
PPS	Number of packets per second in the upstream and downstream flows of this application during the past minute.
Total Flows	Number of flows that were counted for the application.
Active Flows	Flows that had activity during the past 1 minute.
Flow Setup Rate	Average number of new flows per second during the past 1 minute.
Flow Live Time (ms) Max/Min/Avg	Maximum, minimum, and average number of milliseconds of detectable flow activity during the duration of the trace.
Sampled Flows	Number of flows that were sampled in the upstream or downstream traffic of this application. Click the up arrow icon next to the column name to display information for upstream traffic. Click the down arrow icon to display information for downstream traffic.

Column	Description
Sampled Bytes (K)	Number of KBs in the upstream or downstream traffic of this application. Click the up arrow icon next to the column name to display information for upstream traffic. Click the down arrow icon to display information for downstream traffic.

Active Flows and Completed Flows Tabs

Table 14: Active Flows and Completed Flows Tabs

Column	Description
Last Update Time or **Start - Update Time**	In releases through Cisco vManage 17.8.x: Date and time at which the information was last refreshed. In releases from Cisco vManage 20.9.1: Date and time at which the flow started, and date and time at which the information was last refreshed. Instances are refreshed every 10 seconds by default.
Flow ID	System-assigned identifier of the flow.

Column	Description
Readout	

Column	Description
	Information that the flow contains (error, warning, or information). Click an icon to display detailed information about the flow in a dialog box (in releases before Cisco vManage Release 20.9.1) or a slide-in pane (in releases from Cisco vManage Release 20.9.1). If the flow identifies an application issue, you can use this information to assist with a root-cause analysis. From Cisco Catalyst SD-WAN Manager Release 20.14.1, a Cisco ThousandEyes icon indicates that the flow comes from a Cisco ThousandEyes test. The dialog box or slide-in pane includes the following information: • **Overview**: Includes details about flow asymmetry, bidirectional WAN color inconsistency, QoS congestion, LAN or WAN packet drops, SLA violation, path change, flow reset, SAIE packet classification status, TCP server response, and so on. **Note** From Cisco Catalyst SD-WAN Manager Release 20.15.1, when the WAN packet drops in a flow, the Cisco SD-WAN Manager displays the percentage of IPsec failures on the hop. • **Path Insight** (available from Cisco vManage Release 20.9.1): Provides information about how a forwarding path was determined for a flow. This information includes the edge router name; destination IP address; IP address lookup and matched route information; route-receiving source protocol, preference, and metrics; flow path-routing candidates; method for deciding the flow path; NAT translation detail; and the flow path used. (You may have to scroll to the bottom of the **Path Insight** tab to access the horizontal scroll bar.) • **Underlay Insight** (available from Cisco Catalyst SD-WAN Manager Release 20.14.1): Provides underlay hop information about each overlay hop in the flow. **Note** In Cisco vManage Release 20.7.x and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.

Column	Description
	At the beginning of a trace in a network using Multi-Region Fabric, some Path Insight or Routing Insight information might be missing in the second or subsequent hops for the first few flows.
VPN Id	From Cisco Catalyst SD-WAN Manager Release 20.12.1, identifier of the VPN in which the application flow was traced.
Source IP	Source IP address of the traffic that the trace monitors.
Source Port or **Src Port**	Source port of the traffic that the trace monitors.
Destination IP	Destination IP address of the traffic that the trace monitors.
Destination Port or **Dest Port**	Destination port of the traffic that the trace monitors.
Protocol	Protocol of the traffic that the trace monitors.
DSCP Upstream/Downstream	DSCP type that the trace monitors for upstream traffic and downstream traffic.
Application	Application that the trace monitors.
Application Group	Application group that the trace monitors.
Domain	Domain that the flow belongs to. Click a domain name to display the protocol from which the domain was recognized. **Note** This field shows information only for DNS and HTTPS protocol flows. For other flow types, this field displays **Unknown**.
ART CND (ms)/SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND).
User	From Cisco Catalyst SD-WAN Manager Release 20.13.1, the username of the user who sends or receives traffic that the trace monitors. • A username does not include a domain. For example, if a username is aduser@add.com, the name appears as aduser. • A username appears only if Cisco ISE is integrated with Cisco Catalyst SD-WAN. If Cisco ISE is not integrated, this field displays “Unknown."

Column	Description
User Group	From Cisco Catalyst SD-WAN Manager Release 20.13.1, the name of the Cisco ISE user group to which the user who sends or receives traffic belongs. **Note** A user group name appears only if Cisco ISE is integrated with Cisco Catalyst SD-WAN. If Cisco ISE is not integrated, this field displays “Unknown."
Security Group Tag	From Cisco Catalyst SD-WAN Manager Release 20.12.1, security group tag that is assigned to the flow.

Expanded DNS Domains Information

Table 15: Expanded DNS Domains Information (Called Expanded Application Information in Cisco vManage Release 20.6.1 Through Cisco vManage 20.8.x)

Column	Description
Egress Interface	Egress interface type used by the domain.
Local Edge, Remote Edge	Names of the local edge (source) and the remote edge (destination) of the flow.
Local Color	Color of the local edge (source) of the flow, which indicates the egress WAN interface.
Remote Color	Color of the remote edge (destination) of the flow, which indicates the ingress WAN interface.
App CND (ms)/App SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND).
HTTP Probe Response Time (ms)	Response time, in milliseconds, of an HTTP probe ping from the device to the application server.
HTTP Probe Loss (%)	Packet loss percentage of an HTTP probe ping from the device to the application server.
Path Score	Path score of an HTTP probe ping from the device to the application server.

Expanded Application Information

Table 16: Expanded Application Information (Available from Cisco vManage Release 20.9.1)

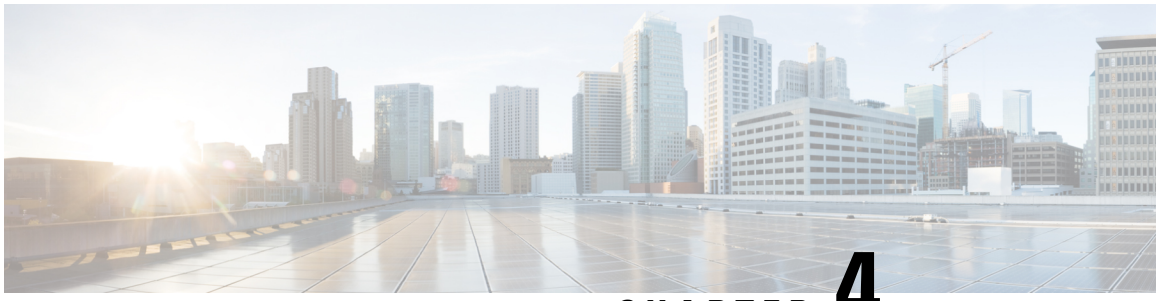
Column	Description
Direction	Direction of the application flow (**upstream** or **downstream**). The first packet that the flow identifies is shown as a flow in the upstream direction.
HopIndex	Hop index number for each direction of the application.
Local Edge	Name of the local edge device (source) of the application.
Remote Edge	Name of the remote edge device (destination) of the application.
Local Color	Color of the local edge device (source) of the application, which indicates the egress WAN interface.
Remote Color	Color of the remote edge device (destination) of the application, which indicates the ingress WAN interface.
Local Drop (%), WAN Drop (%), Remote Drop (%) or **Local Drop (%), WAN Loss (%), Remote Drop (%)**	Packet drop, as measured in the local and remote edge routers. Packet drop is also measured in the complete WAN network.
Jitter (ms), Latency (ms)	Jitter and latency metrics of the application during the past minute. These values help with evaluating the application performance in real time.
ART CND (ms)/SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND) during the past minute.
Total Packets, Total Bytes, or **Sampled Total Packets and Sampled Total Bytes**	For each direction of the application flow, the total number of packets and the total byte count of packets.

Expanded Flow Instance Information

Table 17: Expanded Flow Instance Information

Column	Description
Direction	Direction of the flow (**upstream** or **downstream**). The first packet that the flow identifies is considered to flow in the upstream direction.

Column	Description
HopIndex	Hop index number for each direction of the flow.
Local Edge	Name of the local edge (source) of the flow.
Remote Edge	Name of the remote edge (destination) of the flow.
Local Color	Color of the local edge (source) of the flow, which indicates the egress WAN interface.
Remote Color	Color of the remote edge (destination) of the flow, which indicates the ingress WAN interface.
Local Drop (%), WAN Drop (%), Remote Drop (%) or **Local Drop (%), WAN Loss (%), Remote Drop (%)**	Packet drop, as measured in the local and remote edge routers. The packet drop is also measured in the complete WAN network.
Jitter (ms), Latency (ms)	Jitter and latency metrics of the flow. These values help with evaluating the application performance in real time.
ART CND (ms)/SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND).
Total Packets, Total Bytes	For each direction of the flow, the total number of packets and the total byte count of packets.
Queue Id	Identifier of the QoS queue for the flow.
QDepthLimit/Max/Min/Avg	Limit, maximum, minimum, and average values of the QoS queue depth for the flow.



CHAPTER 4

Insight Summary

Minimum release: Cisco vManage Release 20.9.1.

An insight summary provides trace-level insight information for application traffic and flows. This information appears in a slide-in pane.

- Display Insight Summary Information, on page 43
- Overview Tab, on page 44
- App Performance Insight Tab, on page 45
- Event Insight Tab, on page 46
- QoS Insight Tab, on page 47
- Policy Insight Tab, on page 48
- ThousandEyes Insight Tab, on page 48

Display Insight Summary Information

The following table describes how to display the various insight summaries that are available.

Table 18: Display Insight Summary Information

Insight Summary Information	Procedure
For Manually Generated Traces	
Insight summary for a single manually generated trace	In the **All Trace** tab, click **Insight Summary** in the **Trace Name** column for the trace that you want.
Consolidated insight summary for selected manually generated traces (from Cisco Catalyst SD-WAN Manager Release 20.12.1)	In the **All Trace** tab, check the check box for each trace that you want, and then click **Insight Summary** above the **Trace Name** column.
For Auto-On Task Traces (from Cisco Catalyst SD-WAN Manager Release 20.12.1)	
Insight summary for a single trace generated by an auto-on task	In the **Auto-On Task** tab, expand a task and click **Insight Summary** next to the trace that you want.
Consolidated insight summary for all the traces generated by an auto-on task	In the **Auto-On Task** tab, click **Insight Summary** next to the name of the task.

Overview Tab

The **Overview** tab displays the following information.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, click **Sampled Flow Insight** to see the **Applications** graph, **Events** graph, and **Hotspot Issues**.

The **Users** field appears if you checked the **ISE User Identity** check box in the **Grouping Fields** area when you started the trace. Information for up to 5,000 users that the trace detects is selected by default. You can remove a user by unchecking it in the drop-down list, and add a user by choosing it in the drop-down list.

In the **VPN** field, information for all the VPNs that the trace detects is selected by default. You can remove a VPN by unchecking it in the drop-down list, and add a VPN by choosing it in the drop-down list.

The information in this **Sampled Flow Insight** area is based on sampled data, which comes from a subset of the total number of flows that were monitored. The number of flows that are sampled is determined by an internal algorithm. For example, if the trace monitors 1,000 flows, this tab might show information for only 10 of those flows.

- **Applications** graph: Displays the number of flows that the trace detects in each application in the monitored traffic. Hover your cursor over the data points in the graph to display the percentage of total flows that the corresponding application flow represents.

  From Cisco Catalyst SD-WAN Manager Release 20.12.1, check the **Application** check box to display information for all flows that include application traffic. Check the **DNS** check box to display information for all the flows with DNS resolution.

- **Events** graph: Displays the events that the trace detects in the monitored traffic and the number of application flows that each event affects. Hover your cursor over the data points in the graph to display the percentage of total application flows that the corresponding event affected.

  From Cisco Catalyst SD-WAN Manager Release 20.12.1, check one or more severity check boxes (**Critical**, **Warning**, and **Informational**) to display information for events that have the corresponding severity level.

- **Hotspot Issues**: For each event, provides information about each application flow that was affected, including the traffic path in which the event occurred and the duration of the event.

  This information is displayed for each event that appears in the **Events** field. By default, all the events that the trace detects appear in this field. You can remove an event by clicking **X** next to its name and add an event by choosing the event from the **Events** drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, when viewing the **Overview** tab for a single trace, click **Application Stats** to see the following graphs. These graphs provide information for the top 10 applications with the most flows. Hover your cursor over the data points in a graph to display more detailed information for the corresponding item.

- **Applications (top 10) - Total Flows**: Total number of application flows for the duration of the trace. The selected color is for the egress WAN interface on which flows were initialized.

- **Applications (top 10) - Total Bytes**: Overall application bidirectional bandwidth for the duration of the trace. Upstream and downstream flow bandwidths are counted on the egress WAN on which flows were initialized.

- **Applications (top 10) – Flow Setup Rate**: New incoming flows per second, calculated at 1-minute intervals.

- **Applications (top 10) – Active Flow**: Number of active flows, calculated at 1-minute intervals.
- **Applications (top 10) – Bandwidth**: Number of KB per second, calculated at 1-minute intervals.
- **Applications (top 10) – Flow Live Time**: Overall lifetime of application flows, based on the flows completed within the monitor interval and calculated at 1-minute intervals.

The **Applications (top 10) - Total Flows** and **Applications (top 10) - Total Bytes** graphs provide information for each item that is selected in the **VPN**, **Device**, and **WAN Color** fields. All the items that the trace detects are selected by default.

The other graphs provide information only when one item is selected in the **VPN**, **Device**, and **WAN Color** fields.

You can remove an item from these fields by unchecking it in the corresponding drop-down list, and add an item by choosing the item from the corresponding drop-down list.



Note You can view detailed information about an event in the **Event Insight** tab.

App Performance Insight Tab

The **App Performance Insight** tab displays the following performance information for the selected items.



Note This tab is not available for consolidated insight summaries.

From Cisco Catalyst SD-WAN Manager Release 20.12.11, the **Score** graph appears when you expand **Hop Metrics**. The other graphs appear when you expand **Detailed Metrics** under the expanded **Hop Metrics**.

- **Score** graph: Provides an evaluation of application performance.
- **Loss** graph: Provides information about packet loss.
- **Delay** graph: Provides information about delays in the traffic flows.
- **Jitter** graph: Provides information about the inconsistencies in latency in traffic flows.
- **CND/SND** graph: Provides information about client network delay (CND) and server network delay (SND).
- **Applications Path & Performance** Sankey chart: Provides a snapshot of bandwidth used and loss information at a particular time. You can choose the time by clicking a dot on a timeline in a metrics graph.

The graphs display information for each application that appears in the **Application** field and the hop that is displayed in the **Hop** field. From Cisco Catalyst SD-WAN Manager Release 20.12.1, the **Application** field appears when you expand **Group Fields**. The Sankey chart displays information for each application that appears in the **Application** field and for all the hops, regardless of the hop that is displayed in the **Application** field.

The five applications with the most hotspot issues appear in the **Application** field by default. You can remove an application by clicking the **X** next to its name, and add an application by choosing the application from the **Application** drop-down list. You can choose a hop from the **Hop** drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, information for all the VPNs that the trace detects are selected by default. You can remove a VPN by unchecking it in the corresponding drop-down list, and add a VPN by choosing the item from the corresponding drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can arrange the information that displays into groups, according to the items that you choose in the **Group Fields** area. The fields that are displayed depend on the **Grouping Fields** options that you chose when you started the trace. You can remove a grouping item by clicking **X** next to its name, and add an item by choosing it from the corresponding drop-down list.

Click **Upstream** to display information for upstream traffic in the graphs and chart. Click **Downstream** to display information for downstream traffic in the graphs and chart.

Hover your cursor over a data point in a graph to display more detailed information. Click a data point in a graph to update the Sankey chart for that data point. Hover your cursor over a data point in the Sankey chart to display more detailed information.

From Cisco Catalyst SD-WAN Manager Release 20.15.1, when WAN packet drops in a flow, the IPsec input failures are captured in the metrics.

Cisco SD-WAN Hop Metrics

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1

If the Enhanced Application Aware Routing feature is enabled on a Cisco SD-WAN Manager instance, you can view the associated metrics for the hop. From the **Queue** drop-down menu, choose from the available queues to view the **Loss** graph and **Jitter/Delay** graph.

From the **Loss** graph you can view:

- **WAN Loss Rate**
- **Local Drop Rate**
- **IPsec Authentication Failures**
- **IPsec Anti Replay Failures**



Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, there is a dedicated page for IPsec event history to assist in debugging IPsec anti-replay drops.

- **IPsec Other Input Failures**

Event Insight Tab

The **Event Insight** tab displays the following information about application flows that were affected during each minute of the duration of an event. You can use this information to assist with a root-cause analysis.

Note This tab is not available for consolidated insight summaries.

- **Flows** graph: Provides information about the number of flows at a particular time.
- **Applications Path & Event** Sankey chart: Provides detailed information about the effect of designated events at a particular time. Hover your cursor over a data point to see more information.

The graph displays information for each application that appears in the **Application** field and the hop that is displayed in the **Hop** field. From Cisco Catalyst SD-WAN Manager Release 20.12.1, the **Application** field appears when you expand **Group Fields**. The Sankey chart displays information for each application that appears in the **Application** field, for all the hops regardless of the hop that is displayed in the **Hop** field, and for the events that are displayed in the **Events** field.

The five applications with the most hotspot issues appear in the **Application** field by default. You can remove an application by clicking **X** next to its name, and add an application by choosing the application from the **Application** drop-down list. You can choose a hop from the **Hop** drop-down list.

Hotspot events that the trace detects appear in the **Events** field by default. You can remove an event by clicking **X** next to its name and add an event by choosing the event from the **Application** drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, information for all the VPNs that the trace detects is selected by default. You can remove a VPN by unchecking it in the corresponding drop-down list, and add a VPN by choosing the item from the corresponding drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can use the fields in the **Group Fields** area to group the information that displays by the selected items. The fields that are displayed depend on the **Grouping Fields** options that you chose when you started the trace. You can remove a grouping item by clicking **X** next to its name, and add an item by choosing it from a drop-down list.

Click **Upstream** to display information for upstream traffic in the graph and chart. Click **Downstream** to display information for downstream traffic in the graph and chart.

Hover your cursor over a data point to display detailed information about the events that affect the flow at that point. Click a data point to update the Sankey chart for that data point. Hover your cursor over a data point in the Sankey chart to display more detailed information.

QoS Insight Tab

The **QoS Insight** tab displays network-wide information about which application traffic entered which QoS queues on the devices that the trace detects. This information includes all the hops for the traffic.

Note This tab is not available for consolidated insight summaries.

To display information on this tab, enable the **QoS Insight** option when you start the trace.

- **QoS Drop Rate** graph: Provides information about the packet or byte drop rates for the selected devices over the period of the trace.

- **QoS - Applications Distribution** Sankey chart: Provides detailed information about the traffic spectrum and QoS processing at a particular time. The chart illustrates forwarded or dropped traffic that occurs in a flow that goes from an application to a VPN to a physical interface to a queue.

To provide complete information about bandwidth consumers that cause dropped packets, this tab displays information for all the applications on a device, regardless of the applications that you choose by using the **Application** filter when you start a trace. It also displays information for **VPN0** and all the service VPNs, regardless of the service VPNs that you choose by using the **VPN** filter when you start the trace.

The graph and chart display information for each device that appears in the **Devices** field.

The chart displays information for each item that appears in the **Applications**, **VPNs**, **Interfaces**, **Queues**, and **Forward/Drop** fields. All the items that the trace detects are displayed in these fields by default, except items with a packet per second (PPS) rate of less than 0.05. You can remove an item by clicking the **X** next to its name, and add an item by choosing the item from a corresponding drop-down list.

Click **Packet** to display packet drop rate information in the graph and packets per second (PPS) information in the Sankey chart. Click **Byte** to display byte drop rate information in the graph and kilobits per second (Kbps) information in the Sankey chart.

Hover your cursor over a data point in the graph to display more detailed information. Click a data point in the graph to update the Sankey chart for that data point. Hover your cursor over a data point in the Sankey chart to display more detailed information.

Policy Insight Tab

From Cisco Catalyst SD-WAN Manager Release 20.18.1, you can gather insights into how app route policies and data policies are applied to applications. SLA Not Met and multiple underlay DSCPs on same queue stats are highlighted.

ThousandEyes Insight Tab

From Cisco Catalyst SD-WAN Manager Release 20.14.1, the **ThousandEyes Insight** tab displays the following information that the trace collects from tests that Cisco ThousandEyes Enterprise Agents performed. The information in this tab supplements Cisco ThousandEyes overlay path and metrics information with underlay path and metrics information.

Note This tab is not available for consolidated insight summaries.

Cisco ThousandEyes tests discover network paths, and measure end-to-end loss, jitter, and latency from Enterprise Agents to application servers. This data does not include Cisco Catalyst SD-WAN insight information. This information can help you isolate issues with the network.

To display the following information on this tab, enable the **ThousandEyes Insight** option when you start the trace. The graphs and path visualization display information for the test and agent that you choose.

- **ThousandEyes Tests** table: Provides information for the Cisco ThousandEyes tests that the trace monitored.

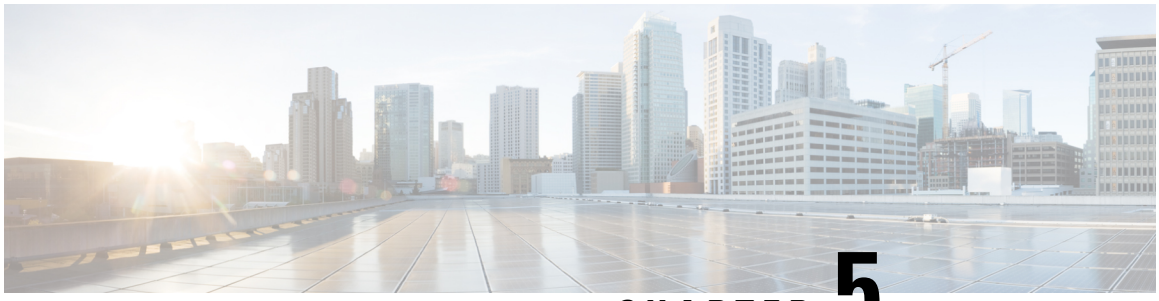
- **Loss** graph: Provides information for the end-to-end loss that Cisco ThousandEyes tests captured, and information about Cisco Catalyst SD-WAN network loss.
- **Jitter/Latency** graph: Provides information for the end-to-end jitter and latency that Cisco ThousandEyes tests captured, and information about Cisco Catalyst SD-WAN network jitter and latency.
- **Path Visualization**: Provides information for the end-to-end network paths that Cisco ThousandEyes tests discovered, supplemented with Cisco Catalyst SD-WAN network segment overlay and underlay paths and metrics that the trace captured.

Hover your cursor over a data point in a graph or the path visualization to display more detailed information.

Click the name of a test in a graph or the path visualization to display detailed information for the test.

Click a data point on a graph and then click **Go to ThousandEyes** to display the **Cisco ThousandEyes Application** page, which provides detailed information for the selected test and agent.

Click a data point on a graph and then click **Go to SD-WAN Insight** to display the **Completed Flows** tab under **NWPI Insight** with detailed flow information for the selected test and agent.



CHAPTER 5

Trace Views

In releases before Cisco vManage Release 20.6.1, you can view the trace flow from three sections: **Geography View**, **Feature View (Upstream)**, and **Feature View (Downstream)**.

From Cisco vManage Release 20.6.1, you can view the trace flow information from these tabs in the **Insight - Advanced Views** area after expanding a flow in the **Insight** area—**Domain Trend**, **Flow Trend**, **Upstream Feature**, **Downstream Feature**, and **Geography**.

Note In Cisco vManage Release 20.6.1 through Cisco vManage 20.8.x, **Domain Trend** is called **App Trend**.

- Domain Trend, on page 51
- Flow Trend, on page 52
- Geography View, on page 52
- Upstream and Downstream Feature Views, on page 52

Domain Trend

The **Domain Trend** tab is available from Cisco vManage Release 20.6.1. It was called **App Trend** in In Cisco vManage Release 20.6.1 through Cisco vManage 20.8.x. This tab appears only when DNS discovery is enabled and displays trends for metrics and events in an application flow. Hover your cursor over the data points in the tab to see detailed information.

The client network delay (CND) and server network delay (SND) information that appears on this tab are measured by the applications' TCP traffic. DNS request frequency shows how often a SaaS application is visited. HTTP probe response time and loss rate are measured by probes that are sent by a router to the SaaS application server to detect a reachable direct internet access (DIA) network path and help evaluate the benefit of deploying a DIA traffic policy.

From the **Chart Metrics** drop-down list, you can choose the metric types for which you want to view information. From the **Devices** drop-down list, you can choose specific devices for which you want to view data. By default, trend information appears for all metric types and all devices.

You can limit the display to trends that occurred within a specified time, or those that occurred within a specified period. You can choose a period of 1, 10, or 30 minutes, or 1, 2, or 5 hours. You also can click **Custom** and enter a date and time range, or click **Real Time** to display information as it is collected.

Flow Trend

The **Flow Trend** tab is available from Cisco vManage Release 20.6.1. This tab displays trends for metrics and events in a trace flow. Hover your cursor over data points to see detailed information.

From the **Chart Metrics** drop-down list, you can choose specific metric types for viewing information. From the **Flow Direction** drop-down list, you can choose the traffic flow direction for viewing data. By default, trend information appears for latency, jitter, WAN loss, and average queue depth, and for all the flow directions.

Use the **Navigate to Event** drop-down list to choose information about a specific event.

You can limit the display to trends that occurred within a specified time, or those that occurred within a specified period. You can choose a period of 1, 10, or 30 minutes, or 1, 2, or 5 hours. You also can click **Custom** and enter a date and time range, or click **Real Time** to display information as it is collected.

Geography View

Supported releases: Cisco Catalyst SD-WAN Manager Release 20.14.1 and earlier

In the **Geography View** section for releases before Cisco vManage Release 20.6.1 or the Geography tab in releases beginning with Cisco vManage Release 20.6.1, you can view the end-to-end trace flow and metrics plotted on the map for a selected trace. The topology graph displays the geographic information about the devices included in the flow.

- The geography view supports "Automatic Network Path Discovery," where you input only the Site and VPN to trace the complete **bidirectional, end-to-end** real-traffic network flow path.
- Each node in the topology is connected with two lines. One line represents upstream direction and the other represents downstream direction.
- Issues (example: SLA violation) detected in the flow metric are shown in different colored lines.

Upstream and Downstream Feature Views

In the **Feature View** section for releases before Cisco vManage Release 20.6.1 or the **Upstream Feature** and **Downstream Feature** tabs in releases beginning with Cisco vManage Release 20.6.1, view the upstream and downstream feature trace with associated policy details.

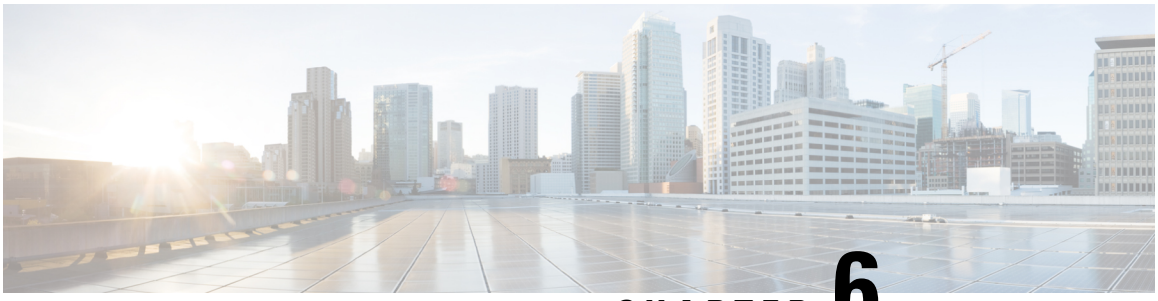
To view the upstream and downstream details of the flow, expand a flow record in the flow path and metrics table.

- The feature view provides a list of ingress and egress features that are applied to the flow, and the execution result of each feature.
    - Typical ingress features include: SD-WAN ACL, NBAR, SD-WAN data policy, SD-WAN app-route policy, SD-WAN forwarding, and so on.
    - Typical egress features include: NBAR, IPsec, SDWAN QoS Output, QoS, Transmit report, and so on.

- For releases before Cisco vManage Release 20.6.1, in the Ingress or Egress view, click a policy to view detailed configuration in a pop-up window and validate policy behavior. For releases beginning with Cisco vManage Release 20.6.1, click **View Policy** to view this information and validate behavior for the corresponding policy. (**View Policy** does not apply to policies that are configured by using a CLI template.)



Note The downstream feature view shows similar information but organized from a downstream direction.



CHAPTER 6

Use Cases

- Use Case 1: Verify a Cisco Cloud OnRamp for SaaS Policy, on page 55
- Use Case 2: Troubleshoot Network Quality on a Website, on page 59

Use Case 1: Verify a Cisco Cloud OnRamp for SaaS Policy

Assume that you have a deployment that includes several branch sites. One of these sites, the SJC branch, with a site ID of 3, has two WAN links: an MPLS link, and a public internet link through which the Microsoft cloud can be accessed directly.

In addition, assume that a Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy, which is a part of an Application-Aware Routing (App-route) policy, has been created and enabled for Microsoft Office 365 applications.

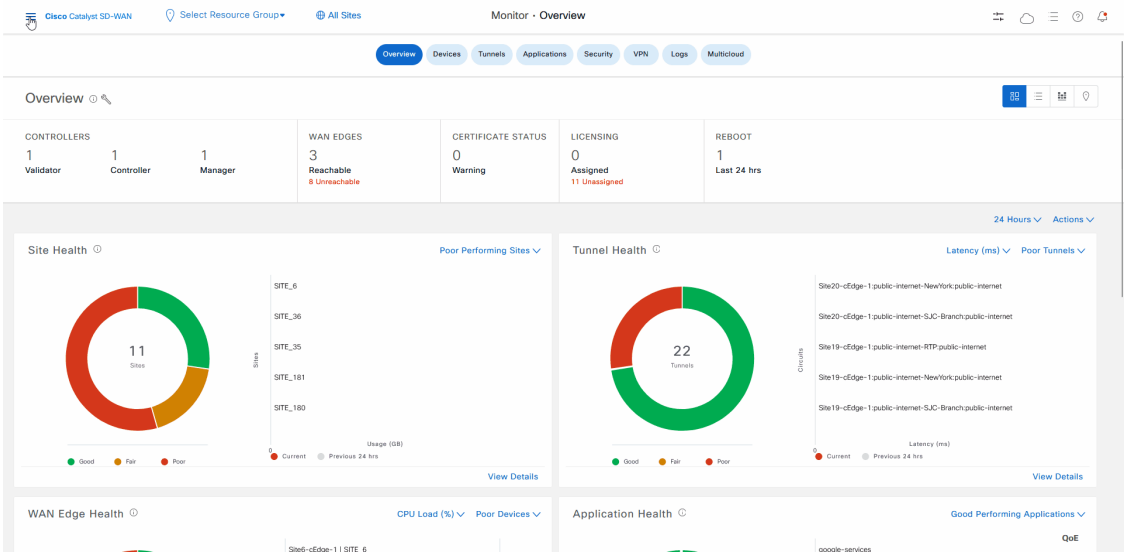
In this use case, let's see how network-wide path insight can be used to determine whether the traffic from Microsoft Office 365 applications is following the expected network path, validate that the policy is programmed correctly and operates as intended, and view the configuration of the policy.

To begin, perform the following actions to start a trace in the SJC branch:

1. From the Cisco Catalyst SD-WAN menu, choose, **Tools** > **Network Wide Path Insight**.
2. Click **New Trace**.
3. In the **Trace Name** field, enter a name for the trace.

   In this use case, we use the name **Verify-Cor-Saas-Policy**.
4. From the **VPN** drop-down list, choose **VPN - 10**.
5. Click **Start**.

Figure 1: Start a Trace



Let the trace run for approximately 5 minutes so that it can collect data, then perform the following actions to see a Sankey diagram that shows the network paths of Microsoft Office 365 applications traffic. This application-level information lets you see whether the traffic is taking the expected network path according to your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy.

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Verify-Cor-Saas-Policy** trace.
2. In the **Insight Summary** slide-in pane, choose the **App Performance Insight** tab and use the filters to see the Sankey chart that shows the network paths of Microsoft applications traffic.

   The Sankey chart shows that this traffic flows directly from the SJC branch to the SaaS cloud-based host.

Figure 2: Display the Upstream Application Path & Performance Sankey Chart

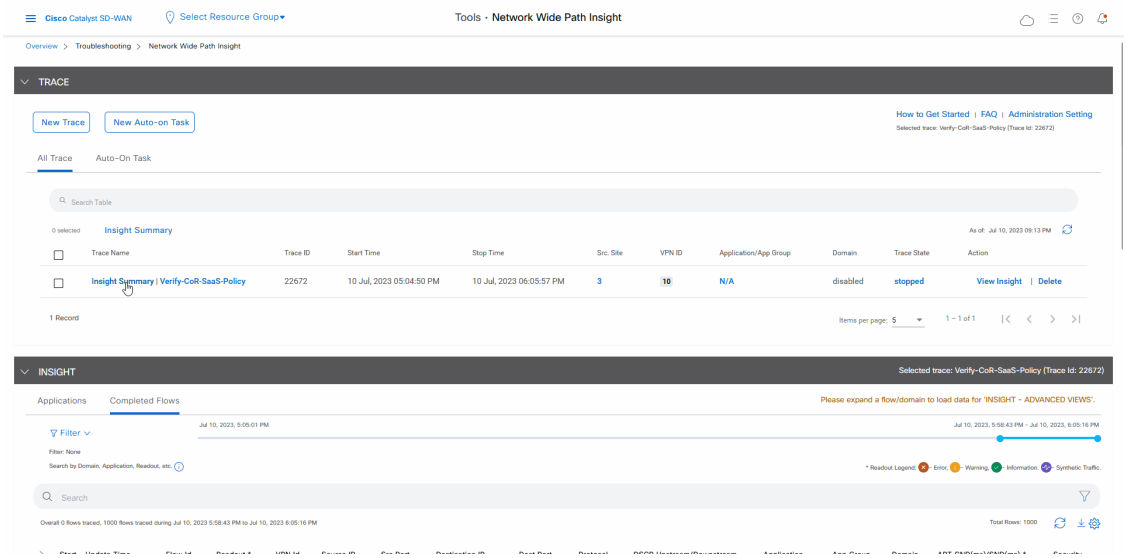
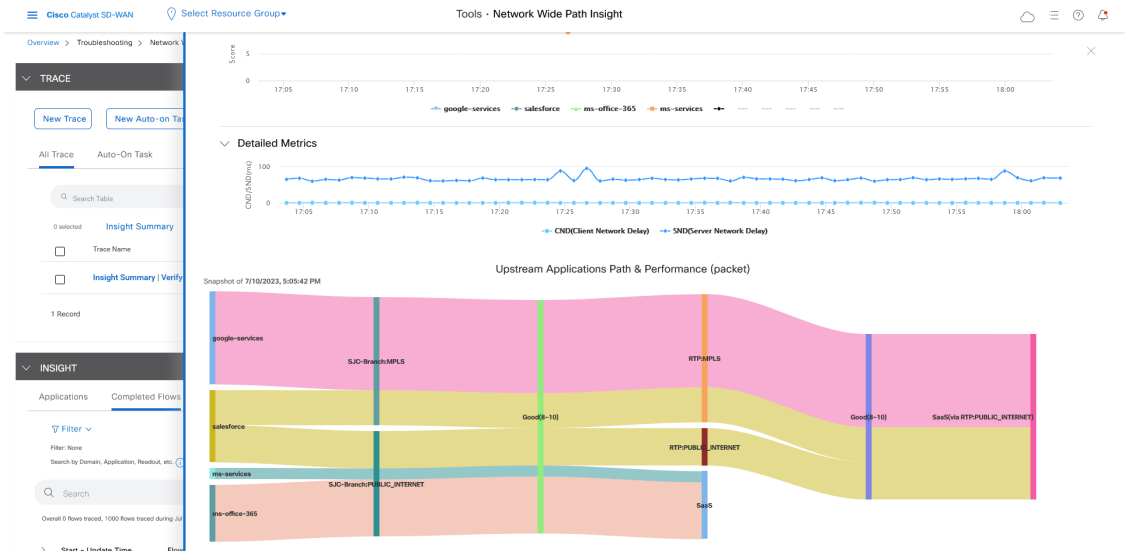


Figure 3: Upstream Application Path & Performance Sankey Chart



After reviewing application-level data, you can check whether your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy took effect for Microsoft Office 365 applications traffic. To do so, look at flow-level information for this traffic:

1. In the **All Trace** tab, go to the **Completed Flows** tab in the **Insight** area.
2. Search for **Office**.
3. For any Microsoft Office 365 flow, click the green check mark in the **Readout** column to display the **Flow Readout** slide-in pane.
4. Click the **Path Insight** tab in the **Flow Readout** pane.

Figure 4: View Flow-Level Information

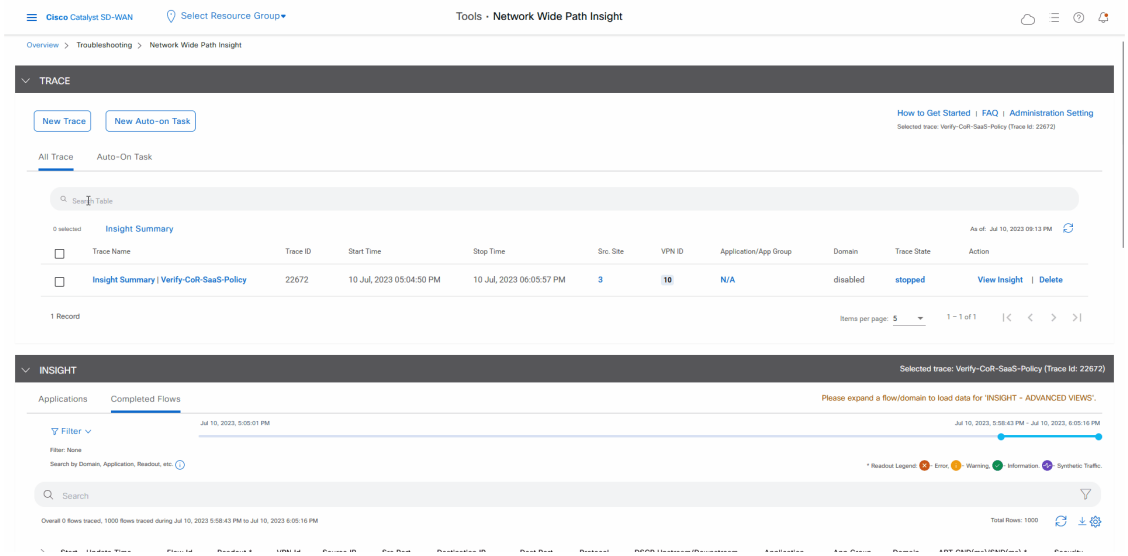
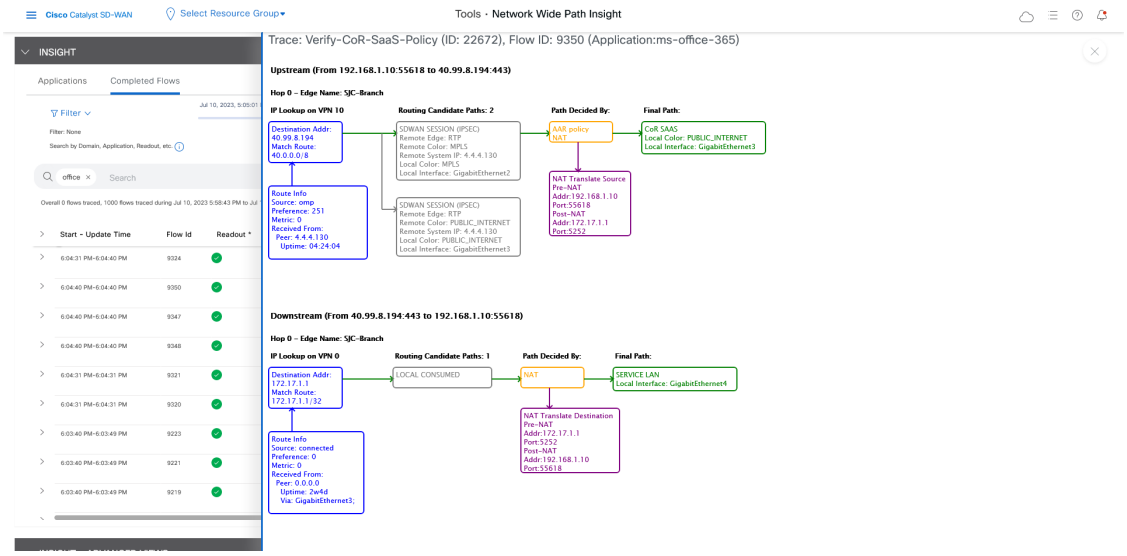


Figure 5: Flow-Level Information



Finally, you can confirm how the App-route policy is programmed. This information lets you validate that Microsoft Office 365 applications traffic flows through the link that is intended according to your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy, which is a part of the App-route policy.

1. In the **All Trace** tab, go to the **Completed Flows** tab in the **Insight** area.
2. Expand any Microsoft Office 365 flow by clicking the right-arrow icon at the beginning of the row.
3. Scroll down to the **Insight – Advanced Views** area.
4. In the **Upstream Feature** tab:
   a. Choose an event from the **Event List** drop-down list.
   b. Click **Expand All Features** to see detailed ingress and egress information about the features that are executed for the flow, then click **Collapse All Features**.
   c. In the **Ingress Feature** area, expand **SDWAN App Route Policy** to see policy information.
   d. Click **View Policy** next to **SDWAN App Route Policy** to see the policy programming.

Figure 6: Confirm the Programming of the App-Route Policy

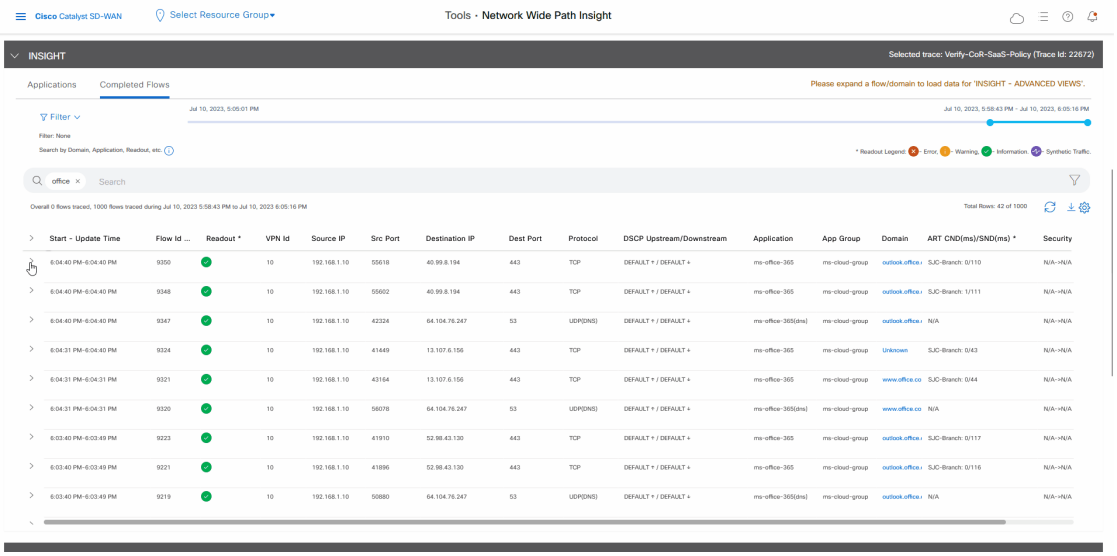
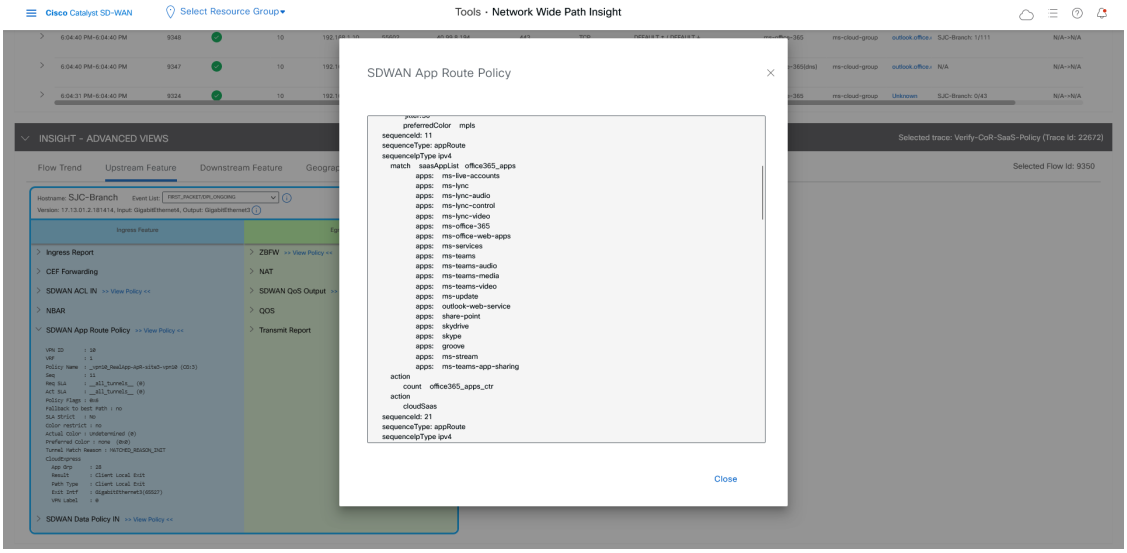


Figure 7: Detailed Information about the App-Route Policy



Use Case 2: Troubleshoot Network Quality on a Website

Assume that your users have trouble accessing the Google website and experience slowness after they are able to access.

In this use case, you'll see how to use network-wide path insight to determine the root cause of these issues.

To begin, perform the following actions to start a trace in the SJC branch:

1. From the Cisco Catalyst SD-WAN menu, choose, **Tools** > **Network Wide Path Insight**.
2. Click **New Trace**.

3. In the **Trace Name** field, enter a name for the trace.

   In this use case, we use the name **Troubleshooting-Google**.

4. Click **Start**.

Let the trace run for approximately 5 minutes so that it can collect data, then follow these steps to determine the root cause of the issue:

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Troubleshooting-Google** trace.

   A slide-in pane with detailed insight information appears. The **Overview** tab shows that 243 google-services flows are affected by local drop events and provides related detailed information for these flows.

2. In the **Events** area, click the link under "impacted 243 google-services flows" to display the **Completed Flows** tab in the **Insight** area on the **All Trace** tab.

   Based on the link that you clicked, the table on the **Completed Flows** tab displays only information for google-services application flows that have a local drop event.

3. To see additional information for a particular flow, click the red X in the **Readout** column for the flow to display the **Flow Readout** slide-in pane.

   The **Overview** tab on the **Flow Readout** slide-in pane shows that the flow is affected by a local drop event and provides related detailed information.

Figure 8: View Insight and Readout Information for Flows

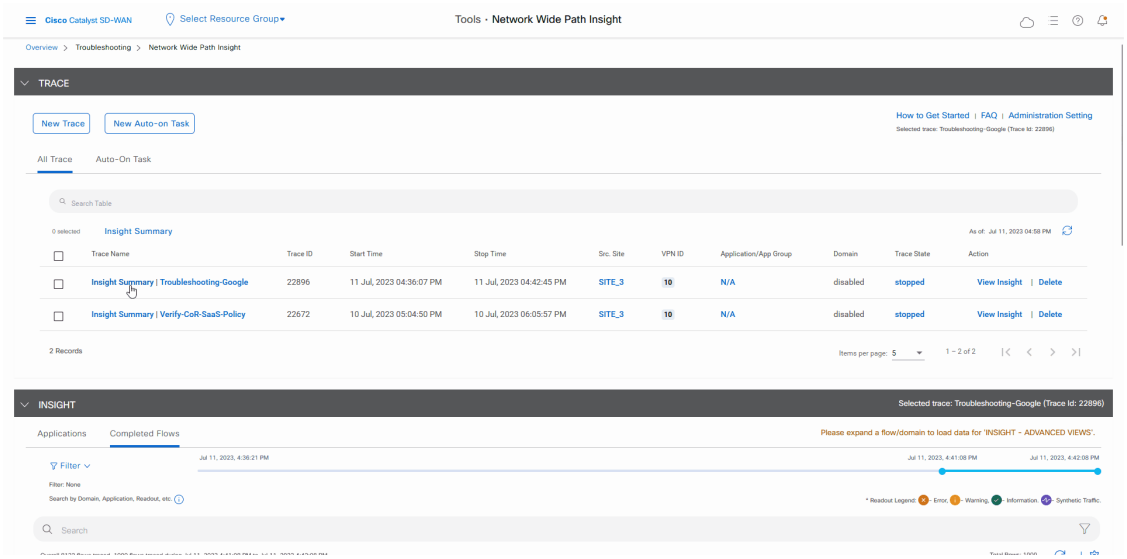


Figure 9: Flow Insight Information

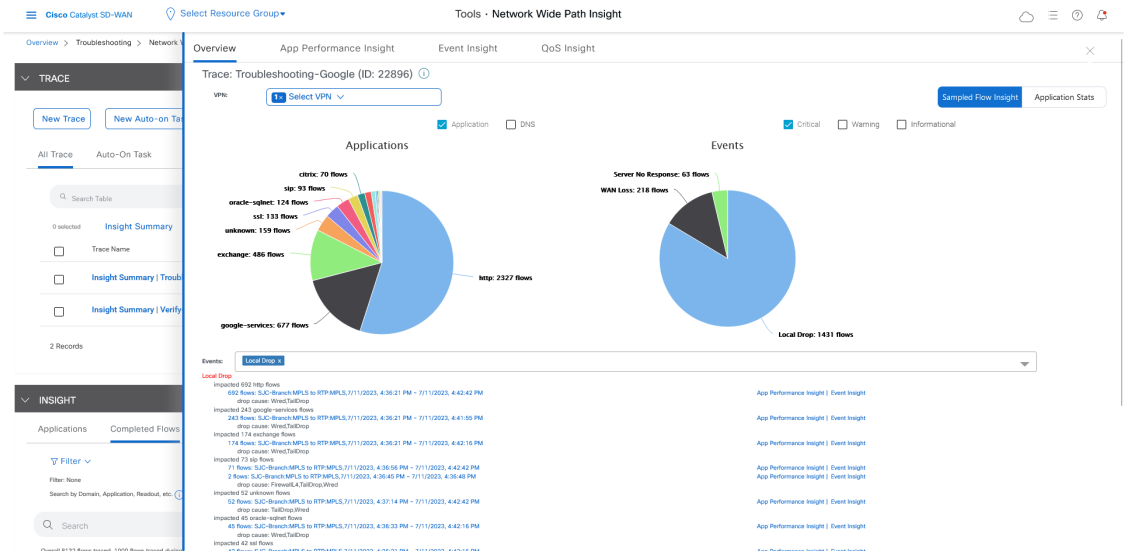
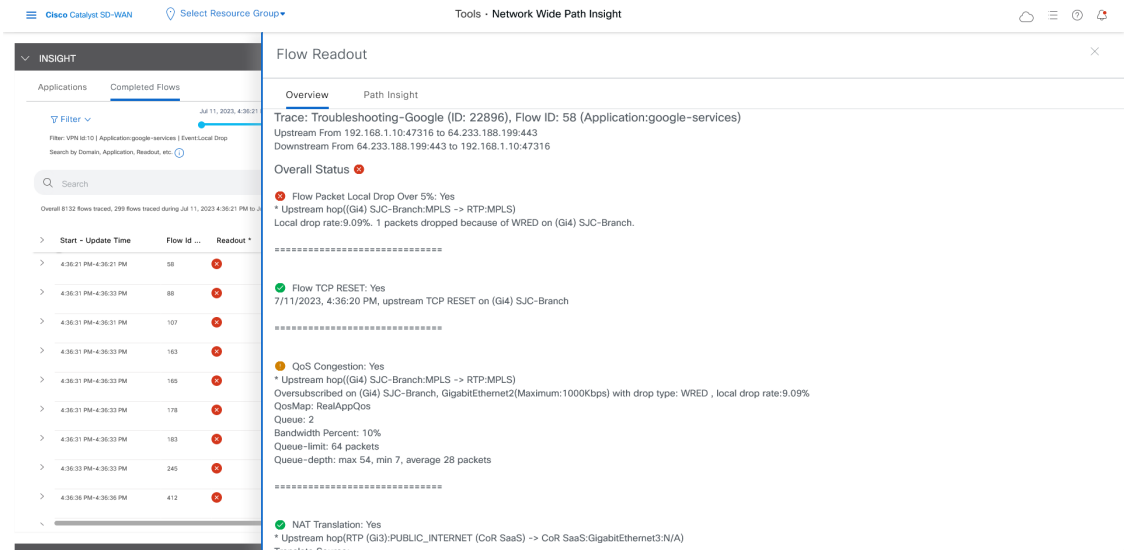


Figure 10: Flow Readout Information



You've now determined that the issue is related to local drop events. These events occur due to packets that are dropped because of network congestion, and they affect the quality of traffic flows on your network. Next, you can use network-wide path insight to answer the following questions that relate to QoS:

- Which queue is google-services traffic sent to?
- What applications besides google-services are consuming the bandwidth on this queue?

With the answers to these questions, you can take steps to reduce the congestion on the queue.

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Troubleshooting-Google** trace.

2. In the **Insight Summary** slide-in pane, choose the **QoS Insight** tab.
3. In the **Applications** field, choose all applications to see which applications are consuming bandwidth on which queue, then choose the **google-services** application to see which queue is used by this application.

   You can see that Google applications use queue 2, but many other applications also use this queue. These applications using the same queue are causing congestion.

Using the information that you found, you can reduce congestion and address the issues that your users experience when they visit the Google website by performing any of the following actions:

- Adjust the QoS policy for the queue,
- Move the Google application to another queue
- Move other applications to another queue

Figure 11: View QoS Information

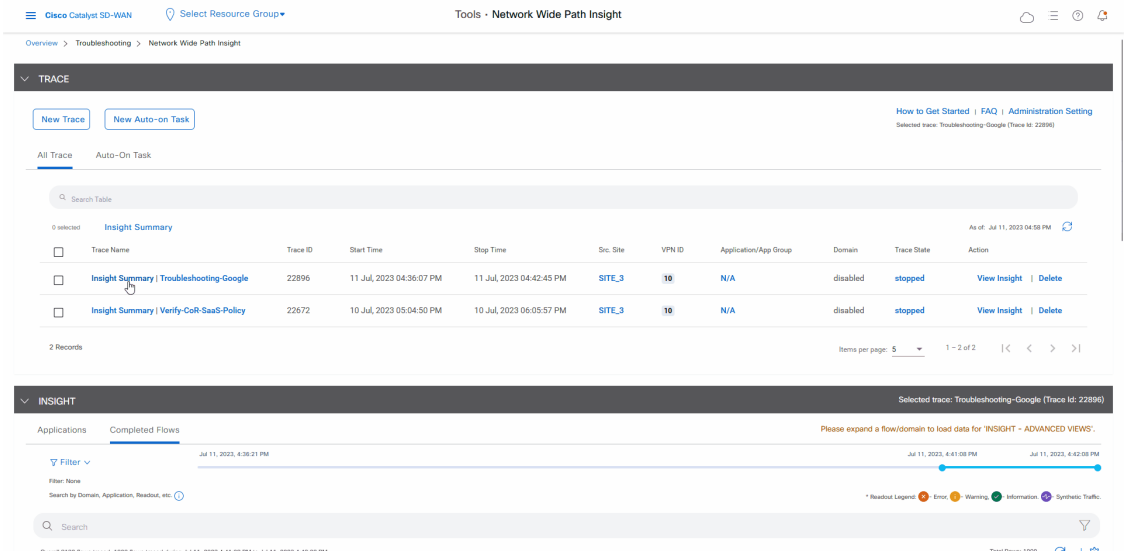


Figure 12: QoS Information for All Applications

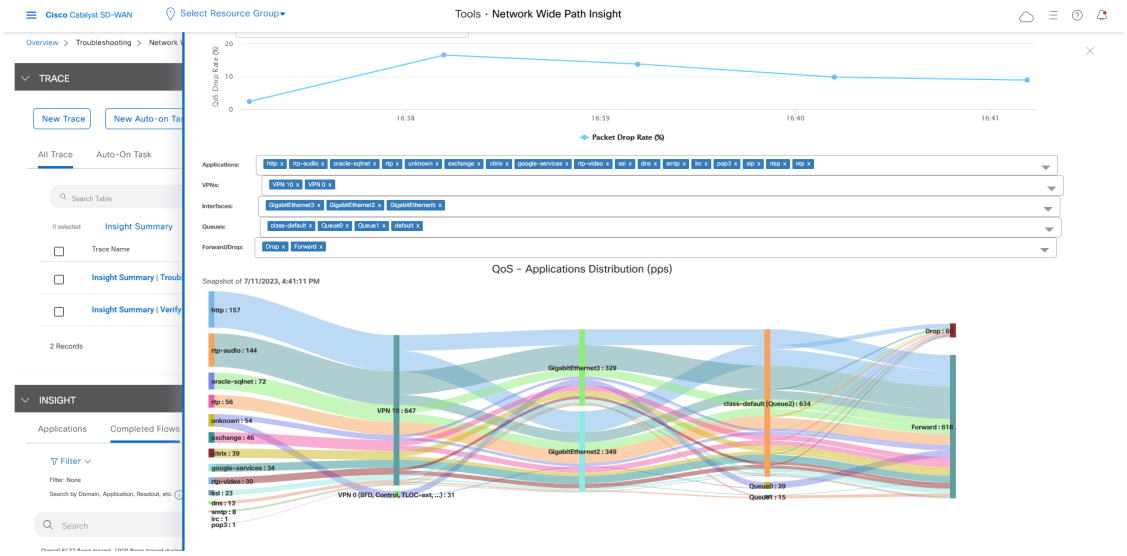
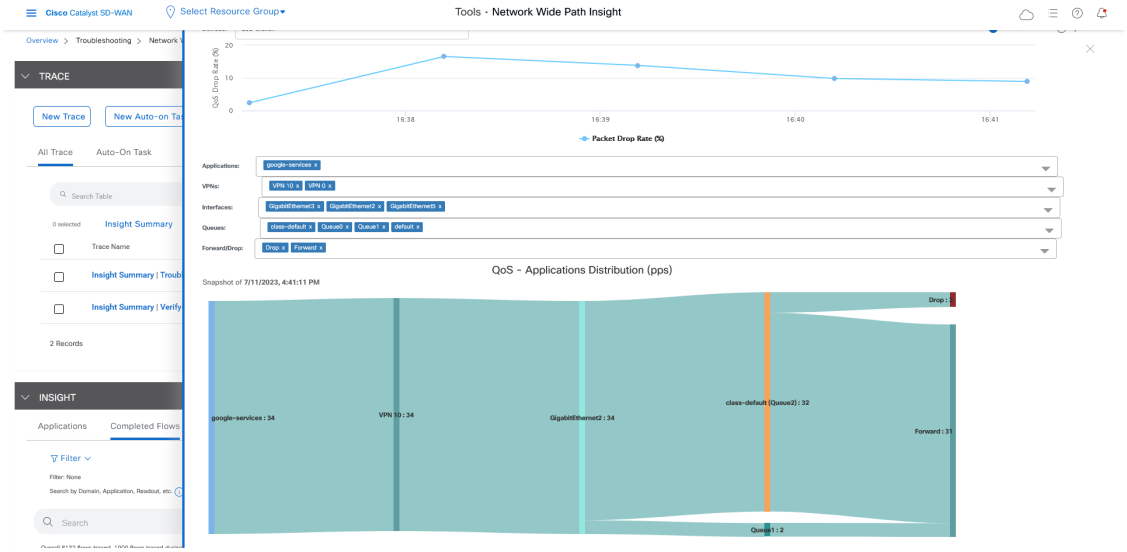
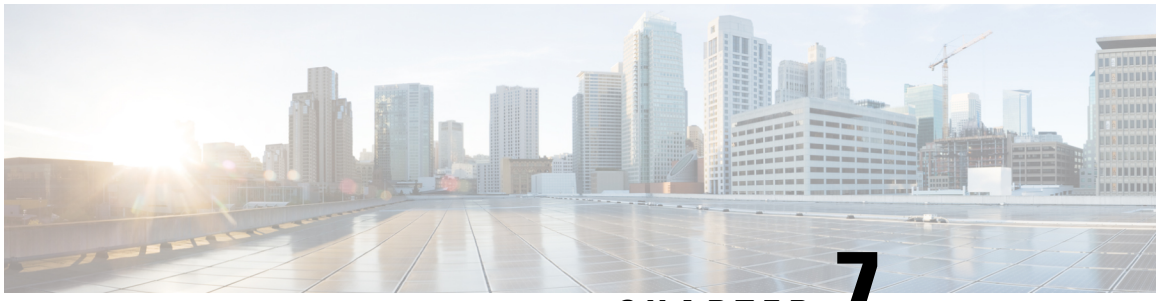


Figure 13: QoS Information for the google-services Application





CHAPTER 7

Troubleshooting

- Troubleshooting Network-Wide Path Insight, on page 65

Troubleshooting Network-Wide Path Insight

Problem

No information is displayed when you view the results of a trace.

Solution

Check the following:

- Data stream collection might not be operating properly. To resolve this issue, choose **Administration** > **Settings** > **Data stream**, click **Disabled**, then click **Save**. Click **Data stream** again, click **Enabled**, choose **System** for the IP address type, then click **Save**.
- You may have enabled DNS domain discovery for the trace, and the monitored traffic may not be from DNS domains. To resolve this issue, choose **Tools** > **Network Wide Path Insight**, uncheck the **Enable DNS Domain Discovery** check box in the **Trace** area, and run the trace again.

Problem

The location of devices does not appear in the **Geography View** section for releases before Cisco vManage Release 20.6.1 or the **Geography** tab in Cisco vManage Release 20.6.1.

Solution

Ensure that GPS is configured for the device.