Perform 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 a variety of options to specify the tracing that you need and view detailed information about trace flows.

To start a trace, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Network Wide Path Insight**.

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can also start a trace by choosing **Create a Trace** from the **Monitor** > **Overview** page.

   Note In Cisco vManage Release 20.6.x and earlier releases, **Network Wide Path Insight** is part of the **Monitor** menu.

2. Perform one of the following actions:

   - From Cisco vManage Release 20.6.1 through Cisco vManage 20.11.x:

     a. (Optional) In the **Trace** area, check the **Enable DNS Domain Discovery** check box to enable DNS domain discovery for network-wide path insight.

     b. Click **New Trace**.

   - From Cisco Catalyst SD-WAN Manager Release 20.12.1:

     a. Click **New Trace**.

     b. (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 **Enable DNS Domain Discovery** is enabled, DNS snooping is used to discover DNS domains and the apps that are running in the discovered domains. You can then monitor the domains under the **Application** option to obtain information about health, trends, and metrics. When this option is disabled, 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. You can check the discovered domains for information about DNS domain queries that are running, and then start a trace to probe the traffic in these domains.

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

   If you do not enter a name, the system assigns the name trace_*ID*, where *ID* is the system-generated identifier of the trace.

4. In the **Trace Duration** field, 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.

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

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

   a. In the **Site ID** field, enter the ID of the Cisco Catalyst SD-WAN network site in which to perform the trace.

   b. From the **VPN** drop-down list, 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.

   c. (Optional. This option is applicable only if DNS domain discovery is disabled.) In the **Source Address/Prefix** field, 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.

   d. (Optional. This option is applicable only if DNS domain discovery is disabled.) In the **Destination Address/Prefix** field, 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.

   e. (Optional. This option is applicable only if DNS domain discovery is enabled.) In the **Client Address/Prefix** field, 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.

   f. (Optional. The **Application** option applies only if DNS domain discovery is disabled.) Click one of the following options, then click the field under the option and use the check boxes that appear to choose the applications or application groups for the trace to monitor:

      - **Application**: Choose this option to designate specific applications for the trace to monitor.
      - **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.

For example, if you choose the application group ms-cloud-group, all the applications that this group includes are monitored. These applications are ms-office-365, ms-services, ms-teams, and more.

If you do not choose an option, the trace monitors all the applications.

To remove an application or application group from this field, click **X** adjacent to the corresponding application or application group name.

6. (Optional) If DNS domain discovery is not enabled, click the **Expand** icon to expand the **Advanced Filters** area and perform the following actions, as needed, to configure specific items for the trace to monitor.

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

a. From the **Device** drop-down list, choose one or more devices for the trace to monitor by checking the check box for each device.

If you do not choose a device, the trace monitors all devices for the site that you specified in Step 5, on page 3.

b. From the **Source Interface** drop-down list, choose the source interface of traffic for the trace to monitor.

If you do not choose a source interface, the trace monitors traffic from all source interfaces in the VPN that you specified in Step 5, on page 3.

c. In the **Source Port** field, enter the source port number of traffic that the trace should monitor. The trace monitors traffic that flows from this port number.

If you do not choose a source port, the trace monitors traffic for all source ports.

d. In the **Destination Port** field, enter the destination port number of traffic for the trace to monitor. The trace monitors traffic that flows to this port number.

If you do not choose a destination port, the trace monitors traffic for all destination ports.

e. From the **Protocol** drop-down list, choose the traffic protocol type for the trace to monitor.

If you do not choose a protocol, the trace monitors traffic for all supported protocols.

f. From the **DSCP** drop-down list, choose the DSCP type for the trace to monitor. The **DEFAULT** selection indicates **DSCP0**.

If you do not choose a DSCP type, the trace monitors traffic for all DSCP types.

g. From Cisco Catalyst SD-WAN Manager Release 20.13.1, check the **ISE Users** 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 do not choose a user, the trace monitors traffic for all users.

Note This **ISE Users** option is available only if Cisco ISE is integrated with Cisco Catalyst SD-WAN.

h. (Optional) From Cisco Catalyst SD-WAN Manager Release 20.14.1, to designate a Cisco ThousandEyes agent whose tests the trace should monitor, check the **ThousandEyes Agent** check box. Click the **ThousandEyes Agent** field and check the check box for the Cisco ThousandEyes Enterprise Agent that you want.

The agent that you choose must be one that was used as a source agent in the Cisco ThousandEyes test that is monitored.

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 other Enterprise Agents also are installed in your network, the trace monitors test from those Enterprise Agents too, but some or all test data from the Enterprise Agents might not be collected.
No	Any device	The trace monitor tests from all Enterprise Agents in your network, but some or all test date from those Enterprise Agents might not be collected.
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 any other traffic simultaneously, while monitoring a Cisco ThousandEyes agent, we recommend that you create another trace in parallel by disabling the **ThousandEyes Insight** option on the same site.

7. (Optional) Click the **Expand** icon to expand the **Monitor Settings** area and perform these actions:

a. (From Cisco vManage Release 20.9.1) Click **QoS Insight** to have the trace include application, VPN, interface, and queue-level throughput and drop-rate metrics for all traffic.

This option is enabled by default.

b. Click **ART Visibility** to have the trace include the application response time (ART) metrics for TCP traffic. These metrics include client network delay (CND) and server network delay (SND) information.

   This option is enabled by default.

c. Click **App Visibility** to have the trace use the SD-WAN Application Intelligence Engine (SAIE) flow to discover applications and application groups.

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 5, on page 3, this option is enabled automatically.

   If DPI is not enabled, we recommend that you enable **App Visibility** to ensure that flows are mapped to the correct applications. Enabling this option authorizes Network-Wide Path Insight to enable DPI in the first hop router of the trace for the duration of the trace.

d. Click **DIA Visibility** to enable the viewing of downstream information from direct internet access flows, beginning with the first flow.

   This option is enabled by default if DNS domain discovery is enabled.

   This option does not affect the applications that are transported over a Cisco Catalyst SD-WAN tunnel.

   If you do not enable this option, the device discovers direct internet access traffic automatically, but it can take some time for this discovery to begin.

e. Click **Hub WAN Visibility** (or **WAN Visibility** for releases from Cisco Catalyst SD-WAN Manager Release 20.12.1.) when starting a trace to have the trace includes flows that are initiated in the WAN to LAN direction.

   By default, a trace monitors flows that are initiated in the LAN to WAN direction.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.12.1, if DNS domain discovery is enabled, this option is enabled by default and cannot be disabled. For releases from Cisco Catalyst SD-WAN Manager Release 20.12.1, this option is disabled by default in all cases and can be enabled as needed.

Note Because traffic typically flows from a spoke to a hub, we recommend that you start a trace from a spoke site.

f. From Cisco Catalyst SD-WAN Manager Release 20.14.1, click **ThousandEyes Insight** 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 check box is checked automatically. (See Configure Cisco Thousand Eyes Username and OAuth Bearer Token.)

   If your username and OAuth bearer token are not 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.

g. Click **Sampling** to enable sampling when tracing, which causes the trace to capture flows at the specified interval.

   In the **Sampling Interval** field that appears, enter the time interval, in seconds, between samples. For example, if you enter 100, one flow will be 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 help extend the monitoring period of a trace by increasing the time that it takes it to reach the maximum number of flows in a trace.

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 a new site is onboarded or an existing site configuration is changed, it is important to validate whether applications work as designed and as intended. Enabling synthetic traffic generates sample user traffic that you can evaluate with other network-wide path insight features to check whether applications are working as expected.

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

   a. In the **URL** field, enter the URL to which a router should send synthetic traffic, for example, https://www.cisco.com.

   b. In the **VPN** field, 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.

   c. In the **DNS Server** field, enter the IP address of the DNS server for translating the URL.

      We recommend that you enter the IP address of your organization’s DNS server so that the synthetic traffic flows to the same destination as the actual user traffic.

   d. From the **DSCP** drop-down list, choose the DSCP to use for the synthetic traffic.

   e. In the **Interval** field, enter how often, in minutes, the synthetic traffic is sent to the URL during the duration of the trace. For example, if you enter an interval of **2**, synthetic traffic is sent every 2 minutes. The minimum value is **1**.

   f. From Cisco Catalyst SD-WAN Manager Release 20.13.1, choose one of the following options from the **ISE User/User Group** drop-down list:

      - Choose **N/A** to generate synthetic traffic that does not 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 choose the user group from the drop-down list to the right.

Note This **ISE User/User Group** option applies only if Cisco ISE is integrated with Cisco Catalyst SD-WAN.

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

h. Click **Save**.

9. (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, information on the **App Performance Insight** tab on the **Insight Summary** display is grouped 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.

- Check the **Client Prefix** check box to additionally group information by client prefix.
- Check the **Server Prefix** check box to additionally group information by server prefix.
- Check the **Source SGT** check box to additionally group information by source security group tag (SGT).
- From Cisco Catalyst SD-WAN Manager Release 20.13.1, check the **ISE User Identity** check box to additionally group information by Cisco ISE user identities.

Note This **ISE User Identity** option applies only if Cisco ISE is integrated with Cisco Catalyst SD-WAN.

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

The **Start Trace** window displays information about the trace, including the trace ID, the start time of the trace, and related details such as the IP addresses and trace status of the started devices.

11. 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.

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 either or both of the following events 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.
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.

   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**.
7. 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.
   - **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.