Perform Network-Wide Path Insight Tracing

Perform Network-Wide Path Insight Tracing

Table 1: 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.

3.

Field	Description
(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 3.

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 3.
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 3, 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 2: 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 3: 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 4: 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 5: 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.
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.

Field	Description
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 6: 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 7: 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 8: 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.
   - **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.